

**Zarządzenie Nr 22/2023
Wójta Gminy Wiśniewo
z dnia 19 czerwca 2023r.**

**w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji
w Urzędzie Gminy w Wiśniewie**

Na podstawie art. 30 ust. 1 w zw. z art. 31 i art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (tekst jednolity Dz.U. 2023 poz. 40) w zw. z art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 119.1 z 04.05.2016) oraz Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych –
zarządzam, co następuje

§ 1.

W Urzędzie Gminy w Wiśniewie wprowadza się Politykę Bezpieczeństwa Informacji, która służy zapewnieniu ochrony przetwarzania danych osobowych.

§ 2.

Polityka Bezpieczeństwa Informacji ma zastosowanie do wszystkich stanowisk pracy, gdzie przetwarzane są dane osobowe.

§ 3.

Zobowiązuje się pracowników Urzędu Gminy w Wiśniewie do zapoznania się z Polityką Bezpieczeństwa Informacji oraz przestrzegania zasad w niej zawartych.

§ 4.

Załączniki do niniejszego Zarządzenia stanowią dokumentację wewnętrzną Urzędu w Wiśniewie .

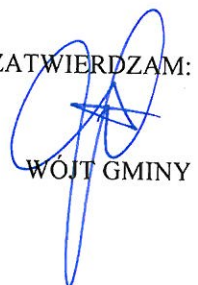
§ 5.

Zarządzenie wchodzi w życie z dniem podjęcia.

Wójt Gminy
Grzegorz Woźniak

POLITYKA BEZPIECZEŃSTWA INFORMACJI
w Urzędzie Gminy Wiśniewo

ZATWIERDZAM:

A handwritten signature in blue ink, consisting of a large, stylized 'W' followed by a horizontal line and a vertical line.

WOJT GMINY

Wiśniewo 2023

Spis treści

1.	Wprowadzenie	3
2.	Słowniczek	3
3.	Postanowienia ogólne	5
4.	Deklaracja stosowania Polityki.....	7
5.	Ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie.....	9
6.	Komunikacja.....	9
7.	Role i odpowiedzialności w Systemie Zarządzania Bezpieczeństwem Informacji.....	11
8.	Istota zarządzania bezpieczeństwem informacji.....	13
9.	Mechanizmy doskonalenia	14
10.	Informacje przetwarzane w Urzędzie.....	14
11.	Sposoby zapewnienia bezpieczeństwa informacjom chronionym	15
12.	Podstawowe zasady bezpieczeństwa informacji	16
13.	Ewidencja sprzętu i oprogramowania	18
14.	Kryteria zaklasyfikowania informacji jako chronionej	19
15.	Ochrona danych osobowych.....	19
16.	Ochrona informacji niejawnych	19
17.	Audyty wewnętrzne SZBI	19
18.	Analiza ryzyka.....	20
19.	Zarządzanie incydentami związanymi z bezpieczeństwem informacji.....	20
20.	Nadzorowanie odstępstw od zasad bezpieczeństwa	22
21.	Przegląd i aktualizacja zapisów PBI.....	24
22.	Załączniki	25

1. Wprowadzenie

Niniejszy dokument stanowi realizację wprowadzenia przez kierownictwo **Urzędu Gminy Wiśniewo** Systemu Zarządzania Bezpieczeństwem Informacji wytwarzanych i przetwarzanych przez **Urząd** jak i powierzanych przez interesariuszy. Udokumentowanie zasad bezpiecznego przetwarzania informacji w **Urzędzie** ma zapewnić możliwość realizacji zadań publicznych zgodnie z obowiązującym prawem i oczekiwaniami interesariuszy.

Wójt Gminy Wiśniewo, mając na uwadze wymaganie zapewnienia interoperacyjności **Urzędu Gminy Wiśniewo**, zlecił publikację niniejszej Polityki Bezpieczeństwa Informacji dla wszystkich ról i stron zaangażowanych w zapewnienie zdolności systemów informacyjnych, w tym teleinformatycznych **Urzędu Gminy Wiśniewo** wykorzystywanych do wspierania procesów wymiany danych z upoważnionymi stronami zgodnie z obowiązującym prawem.

2. Słowniczek

Niniejszy słownik obowiązuje dla całego dokumentu Polityki Bezpieczeństwa Informacji wraz z jej załącznikami.

Administrator Danych Osobowych (ADO) – administrator w rozumieniu art. 4 pkt. 7 RODO.

Administrator systemu – osoba zarządzająca Systemem informatycznym, odpowiedzialna za jego eksploatację, konserwację i działanie, bezpieczeństwo przechowywanych w systemie Danych osobowych oraz realizację przypisanych użytkownikom uprawnień, Administrator systemu jest powoływany zgodnie z wymaganiami Polityki Bezpieczeństwa Informacji.

Audyt wewnętrzny SZBI – audyt wewnętrzny z zakresu bezpieczeństwa informacji sprawdzający funkcjonowanie Systemu Zarządzania Bezpieczeństwem Informacji.

Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji. Dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Dostępność – atrybut informacji polegający na tym, że informacja może być wykorzystana

przez upoważnioną osobę na uzasadnione żądanie w ustalonym czasie.

Inspektor Ochrony Danych (IOD) – wyznaczona (na podstawie art. 37 ust 1 RODO) osoba pełniąca nadzór nad ochroną danych osobowych, oraz monitorujący wypełnienie mających zastosowanie obowiązków wynikających z regulacji prawnych w obszarze danych osobowych.

Integralność – atrybut informacji polegający na tym, że informacja nie uległa zmianie od ostatniej autoryzowanej modyfikacji lub nie została usunięta w niekontrolowany sposób.

Interesariusz – osoba lub organizacja, która może wpływać, na którą można wpływać lub która postrzega siebie samą jako zależną od podejmowanych decyzji lub działań.

Komórka organizacyjna Urzędu – referat, samodzielne stanowisko pracy.

Miejsce przetwarzania – system teleinformatyczny lub pomieszczenie, w którym przetwarzane są informacje.

Podatność - słabość miejsca przetwarzania, która może być wykorzystana przez zagrożenie.

Polityka Bezpieczeństwa Informacji / PBI – niniejsza Polityka Bezpieczeństwa Informacji w Urzędzie **Gminy Wiśniewo**.

Poufność – atrybut informacji polegający na tym, że informacja jest dostępna wyłącznie dla osób, które zostały upoważnione do korzystania z danej informacji.

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

Wójt – Wójt **Gminy Wiśniewo**.

Urząd – Urząd **Gminy Wiśniewo**.

System Zarządzania Bezpieczeństwem Informacji / SZBI - ustanowiony w **Urzędzie Gminy Wiśniewo** w sposób formalny w oparciu o wymagania normy ISO/IEC 27001, zbiór skoordynowanych procesów, procedur, zasobów, sposobów organizacji, planowanych działań itp. mający na celu zapewnienie skutecznego zarządzania bezpieczeństwem informacji.

3. Postanowienia ogólne

31. Celem wprowadzenia do stosowania niniejszej Polityki Bezpieczeństwa Informacji (PBI) jest zapewnienie spójności kierunków działania i wsparcia **Wójta Gminy Wiśniewo** w zakresie planowania, ustanowienia, wdrożenia, wprowadzenia, utrzymywania, monitorowania, przeglądania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w **Urzędzie**.
32. Podstawowym celem funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji jest właściwe zabezpieczenie przetwarzanych informacji przed istniejącymi zagrożeniami oraz zapewnienie zgodności prowadzonych działań z przepisami prawnymi i innymi wymaganiami obowiązującymi **Urzędzie**.
33. Dla każdego celu, jeżeli to możliwe, związanego z zapewnieniem ochrony podstawowych atrybutów bezpieczeństwa informacji, tj. poufności, integralności, dostępności należy zapewnić i udokumentować zestaw informacji dotyczących:
 - a) Osoby odpowiedzialnej za realizację celu, w tym monitorowanie;
 - b) Niezbędnych zasobów do realizacji celu (zasoby osobowe, finansowe, infrastruktura, wiedza, kompetencje);
 - c) Okresowego monitoringu spełnienia cel (metoda, narzędzia, okres);
 - d) Terminu realizacji zaplanowanego celu, jeżeli to możliwe (umiejscowienie w czasie);
 - e) Dokumentowania wyników w postaci zapisów stanowiących dowód, że to co zaplanowano przebiega zgodnie z planem.
34. Nadzór nad przestrzeganiem PBI sprawuje Administrator Systemów Informatycznych.
35. Administrator Systemów Informatycznych odpowiada za przegląd niniejszej Polityki oraz monitoring spełnienia celów SZBI nie rzadziej niż raz do roku. Przegląd ma na celu ocenę adekwatności zapisów, spójność z obowiązującym prawem oraz oczekiwaniami interesariuszy dotyczącymi bezpieczeństwa informacji przetwarzanych w **Urzędzie Gminy Wiśniewo**.
36. Zobowiązanymi do stosowania niniejszej Polityki Bezpieczeństwa Informacji są wszystkie osoby zatrudnione/podejmujące inną formę współpracy z **Urzędem**

Gminy Wiśniewo, mające dostęp do informacji, będących własnością lub powierzonych do przetwarzania Urzędowi.

- 3.7. PBI gwarantuje informacjom przetwarzanym w **Urzędzie Gminy Wiśniewo**:
 - poufność, tj. zapewnienie, że informacja jest dostępna wyłącznie dla osób, które zostały upoważnione do korzystania z danej informacji,
 - integralność, tj. zapewnienie, że informacja nie uległa zmianie od ostatniej autoryzowanej modyfikacji lub nie została usunięta w niekontrolowany sposób,
 - dostępność, tj. zapewnienie możliwości wykorzystania zasobu przez upoważnioną osobę na uzasadnione żądanie w ustalonym czasie.
- 3.8. PBI zakłada ochronę informacji przetwarzanych w **Urzędzie** przed nieautoryzowanym dostępem, ujawnieniem, powieleniem, modyfikacją, zniszczeniem, utratą, nieprawidłowym wykorzystaniem lub kradzieżą.
- 3.9. Wdrożenie oraz eksploatacja PBI na podstawie praktyk zawartych w normie ISO/IEC 27002 jest związana z potrzebą wykorzystania uznanego na świecie modelu zarządzania bezpieczeństwem informacji, bazując na modelu zapisanym w standardzie, deklarując ponadto wykorzystywanie informacji pozyskanych w ramach audytów wewnętrznych, przeglądów zarządzania oraz informacji pozyskiwanych bezpośrednio od interesariuszy.
- 3.10. Zapewnienie bezpieczeństwa informacji realizowane jest m.in. poprzez wsparcie **Urzędu** w zakresie:
 - wyznaczenia celów, kierunków rozwoju i zasad działania dla ustanowienia, wdrożenia i utrzymywania SZBI w **Urzędzie Gminy Wiśniewo**.
 - wskazania, że bezpieczeństwo informacji stanowi część strategii funkcjonowania i rozwoju **Urzędu**,
 - wskazania na obowiązującą metodę analizy ryzyka zawierającą kryteria oceny ryzyk i obowiązkowe planowanie działań powiązanych ze zidentyfikowanymi słabościami (rejestrwanie, analiza, podejmowania decyzji, zabezpieczenie zasobów, nadzór nad realizacją).
- 3.11. Wszystkie zasady związane z ochroną informacji są tworzone i wdrażane przy uwzględnieniu charakteru prowadzonych przez **Urząd** zadań, wymagań

wewnętrznych oraz wymagań zewnętrznych dotyczących bezpieczeństwa informacji.

- 3.12. PBI obejmuje swym zakresem komórki organizacyjne znajdujące się w strukturze organizacyjnej, która jest zamieszczona w Regulaminie Organizacyjnym **Urzędu Gminy Wiśniewo**.
- 3.13. PBI jest nadrzędnym dokumentem SZBI. Żaden inny dokument nie może pozostać w sprzeczności z ustalonymi w PBI zasadami.
- 3.14. PBI uszczegóławiają następujące dokumenty:
- Regulamin Zarządzania Bezpieczeństwem Teleinformatycznym - **załącznik nr 1 do PBI**;
 - Regulamin Zarządzania Bezpieczeństwem Fizycznym - **załącznik nr 2 do PBI**;
 - Regulamin Zarządzania Bezpieczeństwem Osobowym - **załącznik nr 3 do PBI**;
 - Procedura Szacowania i Zarządzania Ryzykiem Bezpieczeństwa Informacji - **załącznik nr 4 do PBI**;
 - Procedura Audytu Wewnętrznego SZBI - **załącznik nr 5 do PBI**;
 - Regulamin Zarządzania Informacjami - **załącznik nr 6 do PBI**;
 - Plan ciągłości działania - **załącznik nr 7 do PBI**;

4. Deklaracja stosowania Polityki

Bezpieczeństwo Informacji wpisuje się w podstawowe zadania publiczne Urzędu z uwagi na konieczność zapewnienia poufności, integralności i dostępności informacji związanej z realizacją zadań przewidzianych przez prawo. Polityka Bezpieczeństwa Informacji stanowi potwierdzenie wsparcia i zaangażowania **Wójta Gminy Wiśniewo** w proces planowania, ustanowienia, wdrożenia, wprowadzenia, utrzymywania, monitorowania, przeglądania i doskonalenia systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami normy ISO/IEC 27001.

Wójt, doceniając znaczenie procesu zarządzania bezpieczeństwem informacji, ustanawia PBI w celu wyznaczenia kierunku działań zmierzających do realizacji i utrzymywania SZBI.

SZBI, zapewniając bezpieczeństwo informacjom przetwarzanym w **Urzędzie Gminy**

Wiśniewo, ma na celu zagwarantowanie zgodności postępowania w zakresie ochrony informacji z obowiązującym aktami prawnymi oraz z regulacjami wewnętrznymi, w tym z **Polityką Bezpieczeństwa Przetwarzanych Danych Osobowych**.

SZBI obejmuje zakresem obowiązywania wszystkie komórki organizacyjne **Urzędu Gminy Wiśniewo**.

Celem SZBI jest osiągnięcie poziomu organizacyjnego i technicznego, który:

- a) będzie gwarantował skuteczną ochronę informacji przetwarzanych w **Urzędzie** oraz zapewni ciągłość procesu ich przetwarzania,
- b) zapewni zachowanie poufności, integralności i dostępności informacji,
- c) zagwarantuje planowany poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach jej przetwarzania,
- d) ograniczy liczbę incydentów związanych z bezpieczeństwem informacji,
- e) zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów teleinformatycznych wykorzystywanych do przetwarzania informacji,
- f) zapewni gotowość do podjęcia działań w sytuacjach kryzysowych oraz awaryjnych, zmniejszając wpływ na interesariuszy wynikający z zakłócenia,
- g) zapewnienie kontroli i poprawy bezpieczeństwa w sytuacjach związanych z cyberatakami.

Powyższe cele realizowane są poprzez:

- a) wyznaczenie ról i odpowiedzialności w zakresie utrzymania SZBI,
- b) stosowanie przez użytkowników polityk, instrukcji oraz procedur określających sposób ochrony informacji w **Urzędzie Gminy Wiśniewo**,
- c) przegląd i aktualizację polityk, instrukcji oraz procedur, zasad bezpiecznego postępowania z informacjami i środkami do przetwarzania informacji,
- d) podnoszenie świadomości użytkowników w zakresie bezpieczeństwa informacji przetwarzanych w **Urzędzie** oraz ich roli w tym procesie,
- e) ciągłe doskonalenie systemu bezpieczeństwa informacji w **Urzędzie Gminy Wiśniewo** w oparciu o wytyczne normy ISO/IEC 27001,
- f) identyfikację zmian w otoczeniu prawnym, dostosowanie zabezpieczeń adekwatnie

do oczekiwań.

Szczególną rolę w SZBI odgrywa ciągły proces kształtowania świadomości pracowników, współpracowników w zakresie zagrożeń dotyczących bezpieczeństwa informacji.

5. Ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie

51. **Wójt** ustanawia we wszystkich komórkach organizacyjnych **Urzędu** System Zarządzania Bezpieczeństwem Informacji (SZBI).
52. System Zarządzania Bezpieczeństwem Informacji ma za zadanie zapewnić adekwatne i proporcjonalne do występujących ryzyk zabezpieczenia, które zagwarantują odpowiednią ochronę informacji należących do **Urzędu** oraz umożliwią wzrost zaufania zainteresowanych stron.
53. System Zarządzania Bezpieczeństwem Informacji zapewnia realizację celów, kierunków i zasad działania wskazanych w Polityce Bezpieczeństwa Informacji **Urzędu** uwzględniając jednocześnie specyfikę zadań realizowanych przez **Urząd**.
54. SZBI obejmuje następujące etapy:
 - ustanowienie,
 - wdrożenie i eksploatację,
 - monitorowanie i przeglądy,
 - utrzymywanie i doskonalenie.

6. Komunikacja

61. **Wójt** ustanawia proces komunikacji w zakresie istotnych informacji dotyczących przetwarzania informacji, w tym danych osobowych. Zobowiązuje kluczowe role oraz wszystkich pracowników do wymiany informacji na temat zdarzeń mających wpływ na bezpieczeństwo informacji oraz możliwość realizacji obowiązków wynikających z RODO wobec osób, do których należą dane osobowe.
62. Przed rozpoczęciem Audytu wewnętrznego SZBI Sekretarz **Urzędu**, drogą mailową, wysyła powiadomienie do kluczowych pracowników **Urzędu** w celu zapewnienia dostępności kluczowych zasobów, nadania odpowiednich uprawnień dla zespołu audytowego do pozyskiwania wiedzy na temat skuteczności SZBI.

63. Każde zdarzenie mające wpływ na bezpieczeństwo informacji powinno zostać przeanalizowane pod kątem potrzeby poinformowania pracowników o źródle i sposobie zapobiegania. Za realizację powyższego zadania odpowiada Administrator Systemów Informatycznych.
64. Każde zdarzenie mogące skutkować naruszeniem ochrony danych osobowych lub praw osób, których dotyczą dane powinno zostać przeanalizowane pod kątem potrzeby poinformowania pracowników o źródle i sposobie zapobiegania. Za realizację powyższego zadania odpowiada Inspektor Ochrony Danych.
65. Komunikacja powinna się odbywać ścieżką zapewniającą skuteczny proces informowania pracowników z wykorzystaniem: korespondencji tradycyjnej (papierowej), **elektronicznego systemu obiegu dokumentów**, poczty elektronicznej. W przypadku powtarzających się zdarzeń, incydentów bezpieczeństwa lub naruszeń należy rozważyć potrzebę uzupełnienia materiałów szkoleniowych w celu budowania świadomości pracowników podczas szkoleń.
66. Komunikaty w zakresie incydentów należy pozbawić danych osobowych oraz wskazówek, które mogłyby stanowić zagrożenie dla zabezpieczeń organizacyjnych oraz technicznych.
67. W przypadku zmian w dokumentacji SZBI lub ODO należy powiadomić kluczowe osoby o obowiązku zapoznania się ze zmianą.
68. Dla systemów informatycznych utrzymywanych przez zewnętrzne podmioty należy ustanowić rolę Opiekun Umowy (osoba odpowiedzialna za realizację umowy) po stronie **Urzędu** oraz adekwatną rolę po stronie dostawcy. W przypadku utraty ciągłości działania, zdarzeń związanych z bezpieczeństwem informacji należy zapewnić krótką ścieżkę komunikacyjną pomiędzy osobami. Minimalnym zestawem informacji jest:
 - a) Imię i nazwisko
 - b) Numer telefonu
 - c) Adres mailowy
 - d) Godziny pracy
 - e) Osoba zastępująca

7. Role i odpowiedzialności w Systemie Zarządzania Bezpieczeństwem Informacji

7.1. Administrator Systemów Informatycznych odpowiada za:

- nadzór nad przestrzeganiem Polityki Bezpieczeństwa Informacji,
- koordynowanie bezpieczeństwa informacji we wszystkich lokalizacjach organizacji,
- nadzór nad opracowaniem, aktualizacją i wdrożeniem dokumentacji związanej z bezpieczeństwem informacji,
- zapewnienie utworzenia i utrzymywania wykazu zatwierdzonych odstępstw i wyjątków od obowiązujących przepisów dotyczących bezpieczeństwa informacji, w szczególności dotyczących stosowanych zabezpieczeń,
- rozstrzyganie problemów dotyczących wątpliwości w stosowaniu PBI,
- nadzór nad zapewnieniem znajomości procedur bezpieczeństwa przez wszystkich pracowników, współpracowników uczestniczących w przetwarzaniu informacji,
- przygotowywanie i przedkładanie Sekretarzowi **Urzędu** okresowych informacji o funkcjonowaniu systemu zarządzania bezpieczeństwem informacji,
- organizowanie przeglądów systemu zarządzania bezpieczeństwem informacji i sporządzanie z nich raportów,
- planowanie, organizowanie i koordynowanie wszystkich działań związanych z przeglądami oraz audytami wewnętrznymi,
- uzgadnianie i nadzorowanie niezgodności oraz działań korygujących oraz dokonywanie oceny ich skuteczności,
- uzgadnianie metodyki i procesów związanych z bezpieczeństwem informacji, np. oceny ryzyka, systemu klasyfikacji informacji, monitorowania oraz oceny skuteczności dla potrzeb bezpieczeństwa informacji,
- Zapewnienie monitorowania funkcjonowania systemu zarządzania bezpieczeństwem informacji,
- dokonywanie przeglądu i monitorowanie incydentów, słabości oraz trendów

naruszeń bezpieczeństwa informacji,

- inicjowanie oraz opiniowanie ważniejszych przedsięwzięć zmierzających do podniesienia poziomu bezpieczeństwa informacji,
- opiniowanie wyników monitorowania, przeglądów oraz oceny skuteczności stosowanych zabezpieczeń,
- nawiązywanie i utrzymywanie kontaktów ze stronami zainteresowanymi w sprawach dotyczących SZBI.

72. **Inspektor Ochrony Danych**

Status Inspektora Ochrony Danych określa art. 38 RODO, zakres obowiązków i uprawnień art. 39 RODO oraz Zarządzenie **Wójta Gminy Wiśniewo** w sprawie wyznaczenia Inspektora ochrony danych.

Inspektor jest odpowiedzialny za nadzorowanie Polityki ochrony danych osobowych zgodnie z obowiązującym prawem oraz w zgodzie z niemniejszą Polityką. Wszystkie odstępstwa wymagają formalnej akceptacji Administratora Danych Osobowych.

73. **Pracownik, współpracownik.**

Odpowiada za realizację zapisów niniejszej Polityki bezpieczeństwa informacji, w tym propagowanie zasad bezpiecznego przetwarzania informacji pośród podległych pracowników, współpracowników, w uzasadnionych przypadkach interesariuszy **Urzędu**. W przypadku zaistnienia zdarzenia mającego potencjalny wpływ na bezpieczeństwo informacji odpowiada za udzielenie wsparcia rolaom wyznaczonym w SZBI do obsługi tego typu zdarzeń oraz zabezpieczenie dowodów należytej staranności **Urzędu** w przedmiotowej sprawie. Bierze udział oraz wspiera SZBI w zakresie utrzymywania w aktualności ewidencji grup informacji oraz okresowej oceny wartości oraz analizie ryzyka dotyczącej utraty podstawowych atrybutów ochrony informacji.

74. **Właściciel Zasobu (Zasoby IT)**

Odpowiada za bezpieczeństwo informacji przetwarzanych w powierzonych do nadzorowania systemach teleinformatycznych, nadawania dostępów i uprawnień w systemach teleinformatycznych. Opracowanie wytycznych do polityki kopii zapasowych oraz ścieżki postępowania na wypadek niedostępności systemu teleinformatycznego. Inicjowania przeglądu uprawnień oraz testów skuteczności stosowanych zabezpieczeń.

75. Właściciel Zasobu (Pomieszczenia)

Odpowiada za bezpieczeństwo informacji przetwarzanych w pomieszczeniu, za które ponosi odpowiedzialność. Kreowanie polityki dostępu do kluczy do nadzorowanych pomieszczeń, przeglądów okresowych stosowanych zabezpieczeń fizycznych. Raportowania wszelakich nieprawidłowości w tym obszarze do Administratora Systemów Informatycznych i IOD. Egzekwowanie zasady czystego biurka od podległych pracowników.

76. Administrator Systemów Informatycznych / Zasobu (Zasoby IT)

Odpowiada za prawidłowe funkcjonowanie systemu teleinformatycznego, bieżący monitoring stanu systemu. Analizę podatności i wdrażanie stosowanych aktualizacji. Wykonywanie i nadzorowanie skuteczności tworzonych kopii zapasowych. Zapewnienie dokumentacji systemu pozwalającej odtworzyć usługę w przypadku awarii. Wspieranie innych ról w zakresie realizacji zabezpieczeń w systemach teleinformatycznych.

8. Istota zarządzania bezpieczeństwem informacji

8.1. W celu zapewnienia odpowiedniego poziomu bezpieczeństwa informacji w Urzędzie Gminy Wiśniewo:

- wskazuje się informacje najbardziej istotne dla funkcjonowania **Urzędu Gminy Wiśniewo** i określa się ich właścicieli - Właścicieli Informacji,
- określa się miejsca przetwarzania poszczególnych informacji,
- definiuje się zagrożenia, na które mogą być narażone informacje oraz miejsca, w których informacje są przetwarzane,
- określa się podatności, które mogą być wykorzystane przez zagrożenia,
- przy uwzględnieniu specyfiki **Urzędu Gminy Wiśniewo** - wskazuje się na skutki utraty poufności, integralności i dostępności informacji.

82. Na podstawie działań wskazanych w pkt. 8.1 wyznacza się poziomy ryzyk i w przypadku ryzyk nieakceptowanych – wdraża się określony wariant postępowania z ryzykiem.

83. W przypadku podjęcia decyzji o zastosowaniu zabezpieczeń jako środka postępowania z ryzykiem – wdraża się takie zabezpieczenia, których cel stosowania jest adekwatny do wyników szacowania ryzyka i odzwierciedla rzeczywiste

potrzeby **Urzędu Gminy Wiśniewo**.

- 8.4. Cele stosowania zabezpieczeń są osiągane poprzez wdrożenia planu postępowania z ryzykiem oraz adekwatnych i skutecznych zabezpieczeń, zapewniających odpowiedni poziom bezpieczeństwa informacji i dążenia do osiągnięcia zaplanowanego poziomu ryzyka szkodliwego.

9. Mechanizmy doskonalenia

- 9.1. Mechanizmy doskonalenia wykorzystywane w ramach SZBI obejmują:

- Audyt wewnętrzny SZBI,
- Analizę ryzyka,
- Zarządzanie incydentami bezpieczeństwa,
- Okresowe przeglądy dokumentacji dotyczącej zarządzania bezpieczeństwem informacji w **Urzędzie Gminy Wiśniewo** (w szczególności PBI).

10. Informacje przetwarzane w Urzędzie

- 10.1. W **Urzędzie Gminy Wiśniewo** przetwarzane są następujące rodzaje informacji:

- Informacje publicznie dostępne tj. informacje podane przez uprawnione do tego podmioty/osoby do publicznej wiadomości,
- Informacje wewnętrzne tj. informacje przeznaczone do użytku służbowego wszystkich pracowników **Urzędu Gminy Wiśniewo**, nie będące informacjami szczególnie chronionymi,
- Informacje szczególnie chronione tj. informacje przetwarzane przez uprawnione osoby, podlegające szczególnej ochronie ze względu na ich poufność, a w szczególności:
 - Informacje niejawne w rozumieniu ustawy z dnia 5 sierpnia 2010 o ochronie informacji niejawnych,
 - Dane osobowe w rozumieniu RODO,
 - Dane osobowe w rozumieniu Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych,
 - Informacje wynikające z Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu

nieuczciwej konkurencji,

- Informacje wynikające z Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną,
- Informacje wynikające z Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

102. Regulamin Zarządzania Informacjami stanowiący **załącznik nr 6** do niniejszej Polityki określa metodę ochrony informacji i postępowania z informacjami w zależności od wartości informacji oszacowanej w procesie klasyfikacji informacji w **Urzędzie Gminy Wiśniewo**.

11. Sposoby zapewnienia bezpieczeństwa informacjom chronionym

11.1. Wszystkie informacje należące do **Urzędu Gminy Wiśniewo** podlegają ochronie przynajmniej na poziomie zgodnym z zasadami opisanymi w punkcie 12 „Podstawowe zasady bezpieczeństwa informacji”.

11.2. W celu zabezpieczenia bezpieczeństwa informacji w **Urzędzie Gminy Wiśniewo** realizuje się następujące procedury:

- Procedura „Przeglądy i konserwacje systemów” - **załącznik nr 8 do PBI**;
- Procedura "Zgłaszanie, realizacja i testowanie nowych rozwiązań informatycznych" - **załącznik nr 9 do PBI**;
- Procedura „Postępowanie w zakresie wykonywania i obsługi kopii zapasowych oraz okresowego badania nośników służących do przechowywania informacji” - **załącznik nr 10 do PBI**;
- Procedura „Postępowanie w przypadku wystąpienia awarii systemu informatycznego oraz zasady ich zgłaszania” - **załącznik nr 11 do PBI**;

11.3. W celu umożliwienia upoważnionym zewnętrznym instytucjom i organizacjom dostępu do informacji oraz kompetentnym pracownikom dostępu do przetwarzania, właściwych ze względu na zajmowane stanowisko, informacji wprowadzony jest:

- Rejestr dostępu do dokumentacji systemu informacyjnego - **załącznik nr 12 do PBI**;
- Regulamin zarządzania pracą użytkownika w systemach teleinformatycznych

stanowi **załącznik nr 13 do PBI**;

114. Dostęp do informacji nie będących informacjami publicznie dostępnymi, nadawany jest z uwzględnieniem „zasady wiedzy koniecznej”. Poziom uprawnień i dostęp do informacji przydzielany jest w zakresie niezbędnym do realizowania zadań służbowych na danym stanowisku pracy.

12. Podstawowe zasady bezpieczeństwa informacji

121. Zasada odpowiedzialności za zasoby - każdy pracownik odpowiada za udostępnione mu zasoby Urzędu (dokumenty, sprzęt, urządzenia, infrastrukturę teleinformatyczną, dostęp do systemów, konta itp.). Zasoby te przeznaczone są do realizacji celów służbowych i w takim zakresie powinny być wykorzystywane.
122. Zasada użytkowania osobistego - użytkowanie zasobów **Urzędu** do celów osobistych jest zabroniona.
123. Zasada ograniczonej prywatności - użytkownik nie powinien oczekiwać, że korzystanie z zasobów **Urzędu Gminy Wiśniewo** jest prywatne. Informacje, środki wykorzystywane w procesie przetwarzania mogą podlegać w każdym czasie audytowi osób upoważnionych przez wewnętrzne procedury **Urzędu Gminy Wiśniewo** lub obowiązujące prawo.
124. Zasada ochrony informacji – wszystkie informacje, w tym jawne, chronione są ze względu na ich integralność (wiarygodność) oraz dostępność. Informacje szczególnie chronione, zabezpieczane są w celu wyeliminowania możliwości nieautoryzowanego dostępu, nieplanowanej zmiany, utraty kompletności lub braku dostępności do informacji. Przekazywanie informacji do publicznej wiadomości dokonuje wyłącznie Sekretarz **Urzędu** lub upoważnione przez niego osoby, zgodnie z procedurami określonymi przepisami wewnętrznymi **Urzędu**.
125. Zasada poufności haseł i kodów dostępu – każdy zobowiązany jest do zachowania poufności i nieprzekazywania osobom nieuprawnionym haseł i kodów, związanych z przydzielonymi mu uprawnieniami, w szczególności dotyczy to haseł dostępu do systemów teleinformatycznych i stref chronionych. Każdy użytkownik ponosi odpowiedzialność za działania związane z ich wykorzystaniem.
126. Zasada nadzorowania dokumentów (Zasada czystego biurka) – należy unikać pozostawiania bez nadzoru dokumentów oraz innych nośników informacji. Po

zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych oraz nośników danych (płyty CD, DVD, pendrive, pieczętek, itp.). Wszystkie dokumenty należy złożyć w szafach lub szufladach, zabezpieczonych przed dostępem osób nieuprawnionych. Zasada dotyczy również miejsc spotkań, po zakończonym spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić urządzenia audiowizualne (tablice, flipchart, itp.). Przekazywanie nośników powinno być wykonywane przy uwzględnieniu zasad bezpieczeństwa informacji, celem zapewnienia odpowiedniej ochrony utrwalonych informacji.

127. Zasada nadzorowanego ekranu – każdy komputer musi mieć ustawiony, włączający się automatycznie po 10 minutach bezczynności użytkownika, wygaszacz ekranu. Dostęp do komputera powinien być możliwy po uwierzytelnieniu się hasłem. Przy każdym opuszczeniu stanowiska użytkownik powinien zablokować komputer lub wylogować się z systemu.
128. Zasada czystych drukarek – dokumenty powinny być zabierane z drukarek natychmiast po ich wydrukowaniu. W przypadku nieudanej próby wydrukowania użytkownik powinien skontaktować się z osobą odpowiedzialną za konserwację urządzenia.
129. Zasada czystego kosza – dokumenty papierowe oraz nośniki danych (płyty CD, DVD, itp.) z wyjątkiem materiałów promocyjnych, marketingowych i informacyjnych powinny być niszczone w sposób uniemożliwiający ich odczytanie (w niszczarce, umieszczane w specjalnie przeznaczonych do tego celu pojemnikach, itp.). Każde stanowisko pracy na którym przetwarzane są informacje szczególnie chronione, musi posiadać dostęp do niszczenia dokumentów.
1210. Zasada zamkniętego pomieszczenia – niedopuszczalne jest pozostawienie niezabezpieczonego pomieszczenia, zarówno w godzinach pracy, jak i po jej zakończeniu, jeśli nie pozostaje w nim osoba uprawniona. Zasada nie dotyczy pomieszczeń ogólnie dostępnych. Na zakończenie dnia pracy, ostatnia wychodząca z pomieszczenia osoba, jest zobowiązana zamknąć wszystkie okna i drzwi oraz zabezpieczyć pomieszczenie przed dostępem osób nieuprawnionych.
1211. W przypadku wystąpienia konieczności pracy poza miejscem zatrudnienia procedury, zasady i warunki pracy zdalnej określa „Regulamin przetwarzania i ochrony danych osobowych w pracy zdalnej”, który stanowi **załącznik nr 14 do**

PBI (wraz z załącznikiem nr 14a).

13. Ewidencja sprzętu i oprogramowania

- 13.1. W celu zagwarantowania prawidłowej realizacji powierzonych **Urzędowi Gminy Wiśniewo** zadań, w tym zabezpieczenia ciągłości działania systemów informatycznych, ADO prowadzi ewidencję sprzętu informatycznego oraz oprogramowania wykorzystywanego w procesie przetwarzania danych oraz wspomagającego funkcjonowanie infrastruktury informatycznej.
- 13.2. Ewidencja służy następującym celom:
- zagwarantowaniu kompletności sprzętu niezbędnego do realizacji zadań powierzonych **Urzędowi**,
 - monitorowaniu stanu technicznego sprzętu eksploatowanego w **Urzędzie** oraz podzespołów niezbędnych do prawidłowego przepływu informacji w infrastrukturze informatycznej,
 - ustalenia lokalizacji usytuowania sprzętu oraz poszczególnych elementów infrastruktury informatycznej,
 - monitorowania legalności użytkowanego oprogramowania, poprzez sprawdzanie stanu ilościowego oraz ważności licencji oprogramowania,
 - zdjęcia ze stanu posiadania programów/aplikacji, których użytkowanie w **Urzędzie** zakończono, jak też eliminowanie zainstalowanych programów/aplikacji, których posiadanie jest nieuzasadnione (instalacje aplikacji w wersjach demo na potrzeby ich przetestowania, programy narzędziowe do diagnostyki sprzętu, oprogramowania, lub inne które nie są już wykorzystywane).
- 13.3. ADO zleca Administratorowi Systemów Informatycznych co najmniej raz w roku przeprowadzenie inwentaryzacji sprzętu informatycznego oraz oprogramowania użytkowanego w **Urzędzie** według ustalonego formularza ewidencyjnego.
- 13.4. Wzór formularza ewidencji sprzętu i oprogramowania stanowi **załącznik nr 15 do PBI**.

14. Kryteria zaklasyfikowania informacji jako chronionej

- 14.1. Wszystkie informacje przetwarzane w **Urzędzie Gminy Wiśniewo** podlegają ochronie pod kątem zachowania atrybutu poufności, integralności, dostępności. Wyłączeniu mogą podlegać informacje wytwarzane przez inne podmioty oraz upubliczniane przez inne podmioty, przy braku wpływu **Urzędu Gminy Wiśniewo** na ich sposób publikacji, nadzorowania aktualności, dostępności oraz kompletności.

15. Ochrona danych osobowych

- 15.1. Dane osobowe przetwarzane w **Urzędzie Gminy Wiśniewo** są przetwarzane zgodnie z obowiązującymi przepisami prawa Unii Europejskiej (w szczególności z RODO) i przepisami krajowymi z zakresu ochrony danych osobowych.
- 15.2. Administratorem Danych Osobowych jest **Gmina Wiśniewo** z siedzibą w **06-521 Wiśniewo, Wiśniewo 86**.

16. Ochrona informacji niejawnych

- 16.1. Zasady ochrony informacji niejawnych reguluje ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych oraz opracowane na jej podstawie regulacje wewnętrzne w **Urzędzie Gminy Wiśniewo**, tj. Plan ochrony informacji niejawnych **Urzędu Gminy Wiśniewo**.
- 16.2. W **Urzędzie Gminy Wiśniewo** został powołany Pion Ochrony Informacji Niejawnych oraz Pełnomocnik ds. Ochrony Informacji Niejawnych, który odpowiada za zapewnienie przestrzegania w **Urzędzie Gminy Wiśniewo** przepisów o ochronie informacji niejawnych.

17. Audyty wewnętrzne SZBI

- 17.1. **Urząd Gminy Wiśniewo** planuje i realizuje audyty wewnętrzne w obszarze bezpieczeństwa informacji zgodnie z procedurą: Procedura Audytu Wewnętrznego SZBI stanowiącą **załącznik nr 5 do PBI**. **Wójt Gminy Wiśniewo** zobowiązuje i upoważnia niezależnego audytora do przeprowadzenia okresowych audytów wewnętrznych w celu zbadania stopnia spełnienia zapisów niniejszej polityki, powiązanych regulacji prawnych, potrzeb w zakresie doskonalenia systemu SZBI. Audyt wewnętrzny powinien odbywać się nie rzadziej niż raz do roku, powinien obejmować wszystkie obszary istotne z punktu widzenia skuteczności

eksploatowanego systemu zarządzania bezpieczeństwem informacji.

18. Analiza ryzyka

- 18.1. Polityka bezpieczeństwa zobowiązuje właścicieli grup informacji do cyklicznej analizy ryzyka w zakresie zagrożeń dla podstawowych atrybutów bezpieczeństwa informacji tj. poufności, integralności i dostępności. Analiza ryzyka ma dać pewność **Wójtowi Gminy Wiśniewo**, że stosowane zabezpieczenia organizacyjne i techniczne są adekwatne dla zidentyfikowanych zagrożeń. W celu prawidłowej identyfikacji zmian w obszarze zagrożeń **Sekretarz Gminy** zobowiązuje właścicieli grup informacji do przeprowadzenia analizy ryzyka nie rzadziej niż raz do roku. **Sekretarz Gminy** dokonuje również wyznaczenia osób odpowiedzialnych za wdrożenie działań doskonalących oraz rozlicza z tych zadań. Proces analizy ryzyka w **Urzędzie Gminy Wiśniewo** został uregulowany procedurą: Procedura Szacowania i Zarządzania Ryzykiem Bezpieczeństwa Informacji stanowiąca **załącznik nr 4 do PBI**.

19. Zarządzanie incydentami związanymi z bezpieczeństwem informacji

- 19.1. **Wójt Gminy Wiśniewo** ustanawia proces zarządzania incydentami bezpieczeństwa oraz słabościami w celu zapewnienia spójnego i skutecznego podejścia do sposobu zgłaszania, rejestracji, dokumentowania oraz obsługi incyduentu.
- 19.2. **Wójt Gminy Wiśniewo** zobowiązuje wszystkich pracowników oraz współpracowników do zgłaszania zdarzeń mających potencjalny lub realny wpływ na bezpieczeństwo informacji oraz prawa osób, których informacje dotyczą.
- 19.3. Zgłoszenia należy dokonać ścieżką zapewniającą sprawne przekazanie kompletu informacji do ról w organizacji odpowiedzialnych za zatrzymanie i obsługę incydentów.
- 19.4. Procedura postępowania z incydentami bezpieczeństwa informacji i naruszeniami ochrony danych osobowych stanowi **załącznik nr 16 do PBI**;
- 19.5. W związku z realizacją wytycznych ustawy z dnia 5 lipca 2018 roku (Dz.U 2022 poz. 1863) o krajowym systemie cyberbezpieczeństwa w **Urzędzie Gminy Wiśniewo** wprowadzona zostaje Procedura zarządzania incydentami

cyberbezpieczeństwa stanowiąca **załącznik nr 17 do PBI**, mająca na celu prawidłowe wywiązanie się z nałożonych obowiązków w zakresie cyberbezpieczeństwa w **Urzędzie Gminy Wiśniewo**, określająca zasady postępowania w chwili wystąpienia zagrożenia lub ataku.

196. **Urząd Gminy Wiśniewo** wyznacza Administratora Systemów Informatycznych do monitorowania przypadków mogących mieć negatywny wpływ na cyberbezpieczeństwo.

197. **Urząd Gminy Wiśniewo** zobowiązany jest do zgłoszenia Administratora Systemów Informatycznych jako osobę kontaktową do CSIRT NASK. Zgłoszenie osób kontaktowych do CSIRT NASK realizowane jest na stronie internetowej:

<https://incydent.cert.pl/osoba-kontaktowa#!/lang=pl,entityType=publicInstitution>

198. W celu sprawnej obsługi incydentów **Wójt Gminy Wiśniewo** wyznacza odpowiednie role w **Urzędzie Gminy Wiśniewo**:

- **Administrator Systemów Informatycznych** - w zakresie zdarzeń, słabości dotyczących bezpieczeństwa informacji.
- **Inspektor Ochrony Danych** – w zakresie naruszeń ochrony danych osobowych lub praw osób, których dane dotyczą.

199. Kierownictwo mając na uwadze potencjalne dochodzenie swoich praw na drodze sądowej, zobowiązuje pracowników do zabezpieczenia materiału dowodowego.

20. Nadzorowanie odstępstw od zasad bezpieczeństwa

- 20.1. Odstępstwa od wymagań bezpieczeństwa zawartych w regulacjach wewnętrznych dot. SZBI nie mogą prowadzić do zakłócenia możliwości realizacji zdefiniowanych celów bezpieczeństwa informacji.
- 20.2. Odstępstwa mogą być stosowane wyłącznie, gdy są one podyktowane względami:
- technicznymi – nie jest możliwe zastosowanie zabezpieczenia z przyczyn technicznych,
 - ekonomicznymi – nie można zastosować zabezpieczenia z uwagi na zbyt wysoki koszt jego wdrożenia,
 - organizacyjnymi – nie można zastosować zabezpieczenia z uwagi na potrzebę zbyt dużych zmian organizacyjnych w **Urzędzie Gminy Wiśniewo**.
- 20.3. Odstępstwa muszą wynikać z konieczności realizacji istotnych zadań nałożonych na **Urząd Gminy Wiśniewo**.
- 20.4. Odstępstwa mogą być stosowane wyłącznie po ich zatwierdzeniu przez **Wójta Gminy Wiśniewo** na podstawie przeprowadzonej analizy ryzyka, udokumentowanych skutków i oceny prawnej. Do czasu zatwierdzenia traktowane są jako incydent bezpieczeństwa informacji.
- 20.5. Wniosek o usankcjonowanie odstępstwa zgłaszany jest przez kierownika komórki organizacyjnej.
- 20.6. Wniosek musi zawierać:
- wskazanie na wymaganie, które nie jest spełnione – np. punkt polityki,
 - opis odstępstwa – krótki opis wnioskowanego odstępstwa,
 - zakres stosowania – np. nazwy systemów, komórek organizacyjnych, lokalizacji, w których będzie obowiązywało,
 - wskazanie przyczyny stosowania odstępstwa - techniczne, organizacyjne lub ekonomiczne - wraz z krótkim uzasadnieniem,
 - wskazanie na sposoby osiągnięcia celów dla bezpieczeństwa informacji pomimo zastosowania odstępstwa – opis innych środków, które zostaną wdrożone w celu osiągnięcia celu bezpieczeństwa informacji jaki przyświecał

utworzeniu danego zabezpieczenia.

- 20.7. Wniosek składany jest do Administratora Systemów Informatycznych.
- 20.8. Administrator Systemów Informatycznych wskazuje na zagrożenia, które mogą zaistnieć w związku z zastosowaniem odstępstwa.
- 20.9. Administrator Systemów Informatycznych ocenia odstępstwo pod względem jego zasadności i przedstawia wniosek do zaopiniowania **Sekretarzowi Gminy Wiśniewo**.
- 20.10. Decyzję o zastosowaniu odstępstwa podejmuje **Wójt Gminy Wiśniewo**.
- 20.11. W przypadku powiązania odstępstwa z procesem przetwarzania danych osobowych, w roli konsultującego występuje IOD.
- 20.12. Jeżeli odstępstwo ma powodować wysokie ryzyko dla czynności przetwarzania danych osobowych, w proces konsultacji zostanie włączony Prezes Urzędu Ochrony Danych Osobowych.
- 20.13. Zastosowanie odstępstwa może być czasowe lub bezterminowe.
- 20.14. Odstępstwo czasowe stosuje się w sytuacji, gdy możliwe jest podjęcie działań doskonalących eliminujących przyczynę zastosowania odstępstwa i jest stosowane równoległe z rozpoczęciem realizacji takiego działania w postaci zgłoszenia działania korygującego/zapobiegawczego.
- 20.15. Administrator Systemów Informatycznych informuje o podjętej decyzji wnioskodawcę niezwłocznie po jej podjęciu przez **Wójta Gminy Wiśniewo**.
- 20.16. Każdy wniosek o odstępstwo wraz z analizami i decyzją o odstępstwie lub odrzuceniu wniosku przechowywane są przez Informatyka.

21. Przegląd i aktualizacja zapisów PBI

- 21.1. Polityka Bezpieczeństwa Informacji wymaga okresowego przeglądu nie rzadziej niż raz w roku. W przypadku zmian regulacji prawnych mających wpływ na proces przetwarzania informacji w **Urzędzie Gminy Wiśniewo** przegląd należy w tym zakresie przeprowadzić niezwłocznie (tj. nie później niż w terminie miesiąca) po opublikowaniu nowej regulacji.
- 21.2. Za przegląd Polityki Bezpieczeństwa **Informacji odpowiadają wspólnie Administrator Systemów Informatycznych i Inspektor Ochrony Danych.**
- 21.3. W ramach przeglądu Polityki należy ocenić zasadność stosowanych odstępstw, jeżeli występują.
- 21.4. W ramach przeglądu PBI Kierownicy komórek organizacyjnych **Urzędu Gminy Wiśniewo** **zobowiązani są do cyklicznego co najmniej raz w roku przeglądu PBI. jeśli jest taka potrzeba składają wnioski o aktualizację zapisów PBI oraz oświadczenie o dokonaniu przeglądu PBI w ramach kompetencji** Komórki organizacyjnej **Urzędu.**

22. Załączniki

- 221. Regulamin Zarządzania Bezpieczeństwem Teleinformatycznym - **załącznik nr 1 do PBI**;
- 222. Regulamin Zarządzania Bezpieczeństwem Fizycznym - **załącznik nr 2 do PBI**;
- 223. Regulamin Zarządzania Bezpieczeństwem Osobowym - **załącznik nr 3 do PBI**;
- 224. Procedura Szacowania i Zarządzania Ryzykiem Bezpieczeństwa Informacji - **załącznik nr 4 do PBI**;
- 225. Procedura Audytu Wewnętrznego SZBI - **załącznik nr 5 do PBI**;
- 226. Regulamin Zarządzania Informacjami - **załącznik nr 6 do PBI**;
- 227. Plan ciągłości działania - **załącznik nr 7 do PBI**;
- 228. Procedura „Przeglądy i konserwacje systemów” - **załącznik nr 8 do PBI**;
- 229. Procedura "Zgłaszanie, realizacja i testowanie nowych rozwiązań informatycznych” - **załącznik nr 9 do PBI**;
- 2210. Procedura „Postępowanie w zakresie wykonywania i obsługi kopii zapasowych oraz okresowego badania nośników służących do przechowywania informacji” - **załącznik nr 10 do PBI**;
- 2211. Procedura „Postępowanie w przypadku wystąpienia awarii systemu informatycznego oraz zasady ich zgłaszania” - **załącznik nr 11 do PBI**;
- 2212. Rejestr dostępu do dokumentacji systemu informacyjnego - **załącznik nr 12 do PBI**;
- 2213. Regulamin zarządzania pracą użytkownika w systemach teleinformatycznych - **załącznik nr 13 do PBI**;
- 2214. Regulamin przetwarzania i ochrony danych osobowych w pracy zdalnej - **załącznik nr 14 do PBI (wraz z załącznikiem nr 14a)**;
- 2215. Formularz ewidencji sprzętu i oprogramowania - **załącznik nr 15 do PBI**;
- 2216. Procedura postępowania z incydentami bezpieczeństwa informacji i naruszeniami ochrony danych osobowych - **załącznik nr 16 do PBI**;
- 2217. Procedura zarządzania incydentami cyberbezpieczeństwa - **załącznik nr 17 do PBI**.

REGULAMIN ZARZĄDZANIA BEZPIECZEŃSTWEM TELEINFORMATYCZNYM

Spis treści

1. Wprowadzenie	3
2. Słowniczek uzupełniający	3
3. Osoba odpowiedzialna za dokument	3
4. Role w zarządzaniu systemami teleinformatycznymi	3
5. Role w zarządzaniu zasobami	4
6. Zarządzanie licencjami oprogramowania	4
7. Zarządzanie uprawnieniami	5
8. Dostęp do poczty elektronicznej	6
9. Dzienniki administracyjne	6
10. Monitorowanie działań użytkowników	7
11. Uwierzytelnianie użytkowników	8
12. Hasła Administracyjne	8
13. Zarządzanie zmianą	10
14. Aktualizacja bezpieczeństwa	10
15. Zarządzanie kopiami bezpieczeństwa	11
16. Zabezpieczenie sieci	12
17. Bezpieczeństwo urządzeń mobilnych	13
18. Audyty infrastruktury teleinformatycznej	15
19. Dostęp zdalny (spoza infrastruktury Urzędu)	15
20. Zarządzanie nośnikami danych	16
21. Wytyczne i klauzule obowiązkowe w umowach serwisowych	17
22. Procedury eksploatacyjne	18
23. Rozwój i utrzymanie systemów informacyjnych	19
24. Odpowiedzialność	20
Załącznik nr 1	21

1. Wprowadzenie

Celem Regulaminu Zarządzania Bezpieczeństwem Informacji jest przedstawienie wytycznych w zakresie zapewnienia bezpieczeństwa teleinformatycznego systemów wykorzystywanych przez **Urząd Gminy Wiśniewo** oraz wskazanie innych regulacji, które mają zastosowanie w ww. zakresie.

SZBI dotyczy wszystkich Pracowników i współpracowników **Urzędu**. Wszyscy pracownicy i współpracownicy **Urzędu** zobowiązani są znać i przestrzegać wymagania niniejszego dokumentu oraz dokumentów powiązanych zgodnie z zakresem wynikającym ze stanowiska i realizowanych obowiązków służbowych.

2. Słowniczek uzupełniający

System teleinformatyczny – system operacyjny, aplikacja, baza danych przetwarzająca informacje w postaci elektronicznej.

Właściciel zasobu - kierownik komórki organizacyjnej odpowiedzialny za dostarczenie lub utrzymanie zasobu.

Zasób – pomieszczenie lub urządzenie nie będące systemem teleinformatycznym, w którym przetwarzane są informacje.

3. Osoba odpowiedzialna za dokument

Za aktualność treści zawartej w tym dokumencie odpowiedzialny jest: Administrator Systemów Informatycznych.

4. Role w zarządzaniu systemami teleinformatycznymi

- 4.1. W odniesieniu do każdego systemu teleinformatycznego muszą istnieć zdefiniowane role:
 - Administrator systemu.
 - Właściciel zasobu (systemu lub urządzenia teleinformatycznego).
 - Użytkownik.
- 4.2. Użytkownik realizuje operacyjnie zadania Właściciela Zasobu. Podlega bezpośredniemu nadzorowi przez Właściciela Zasobu. Rola daje możliwość Właścicielowi Zasobu scedowanie części obowiązków na podległego pracownika, przy czym odpowiedzialność za prawidłowe funkcjonowanie procesu, realizację zadań nadal pozostaje na Właścicielu Zasobu.
- 4.3. Każda z osób pełniąca role, o których mowa w pkt 4.1 musi posiadać swojego stałego lub czasowego (na czas nieobecności) zastępcę.

- 4.4. W przypadku powołania wielu osób pełniących tę samą rolę spośród wymienionych w punkcie 4.1, należy wyznaczyć osobę, która będzie odpowiedzialna za nadzorowanie pracy pozostałych osób.
- 4.5. Osoby pełniące funkcję administratorów systemu wskazuje Właściciel Zasobu (kierownik jednostki organizacyjnej odpowiedzialny za utrzymanie systemu).

5. Role w zarządzaniu zasobami

- 5.1. W odniesieniu do każdego zasobu (miejsce przetwarzania informacji nie będące systemem teleinformatycznym – np. przenośny dysk twardy, pendrive, pomieszczenie), do którego można uzyskać uprawnienia muszą istnieć zdefiniowane role:
 - Administrator zasobu,
 - Właściciela Zasobu,
 - Nadzorujący.
- 5.2. Każda z osób pełniących role wskazane w punkcie 5.1 musi posiadać swojego stałego lub czasowego (na czas nieobecności) zastępcę.
- 5.3. Osoby pełniące rolę administratorów zasobu wskazuje Właściciel Zasobu (Kierownik komórki organizacyjnej odpowiedzialny za dostarczenie lub utrzymanie zasobu).

6. Zarządzanie licencjami oprogramowania

- 6.1. Dopuszcza się wykorzystywanie oprogramowania, co do którego **Urząd** posiada stosowne licencje, prawa.
- 6.2. Oprogramowanie darmowe jest dopuszczone do użytkowania pod warunkiem wydania pozytywnej opinii Administratora Systemów Informatycznych, co do zgodności zapisów darmowej licencji i sposobu wykorzystania w **Urzędzie**.
- 6.3. Sposób ewidencji licencji zainstalowanego oprogramowania musi umożliwiać wykonanie audytu faktycznie zainstalowanego oprogramowania.
- 6.4. Ewidencja **licencji i oprogramowania wykorzystywanego przez Gminę prowadzony** jest przez Administratora Systemów Informatycznych zgodnie nr z **załącznikiem nr 15 do PBI** - Ewidencji sprzętu i oprogramowania w formie papierowej (Excel).
- 6.5. Eksploatowane oprogramowanie powinno być chronione przed jakąkolwiek niekontrolowaną modyfikacją, nieautoryzowanym usunięciem oraz kopiowaniem.
- 6.6. Każdy użytkownik odpowiada za eksploatację udostępnionego mu sprzętu stanowiskowego, w tym zainstalowanego na nim oprogramowania (wykorzystywania tylko do celów służbowych, zgodnie z warunkami licencji, nieudostępniania kopii, itd.)

- 6.7. Administrator Systemów Informatycznych jest zobowiązany do inicjowania okresowych kontroli zgodności w zakresie wykorzystywanego oprogramowania w **Urzędzie Gminy Wiśniewo**. Wszelkie niezgodności w zakresie licencji, treści plików należy traktować jak incydent bezpieczeństwa informacji i obsługiwać zgodnie z wdrożoną procedurą w tym zakresie.

7. Zarządzanie uprawnieniami

- 7.1. Dostęp do Systemów i Zasobów oraz uprawnienia do korzystania z nich nadawane są jedynie w zakresie wiedzy koniecznej, tj. niezbędnym do wykonywania aktualnie powierzonych danej osobie zadań i obowiązków na wniosek Sekretarza **Gminy**.
- 7.2. Należy zapewnić w procedurach taki obieg informacji pomiędzy Sekretarzem **Gminy**, Administratorem systemów Informatycznych i Inspektorem Ochrony Danych oraz osobami odpowiedzialnymi za sprawy kadrowe w **Urzędzie**, który umożliwi podjęcie odpowiednich kroków w przypadku zatrudnienia bądź zwolnienia pracownika w celu niezwłocznej wymiany informacji o zatrudnieniu bądź zwolnieniu pracownika.
- 7.3. Nadawanie uprawnień odbywa się na podstawie uprawnień do pracy w Systemie Informatycznym **Urzędu** oraz upoważnień do przetwarzania danych osobowych, zgodnie z **załącznikiem nr 12 do PBI** - Rejestr dostępu do dokumentacji systemu informacyjnego oraz z **załącznikiem nr 13 do PBI** - Rejestr upoważnień do systemów informatycznych.
- 7.4. Dla wszystkich systemów umożliwiających dostęp zdalny do zasobów (np. VPN) Właścicielem Systemu akceptującym wnioski jest Administrator Systemów Informatycznych.
- 7.5. Niezależnie od zleconych przez Sekretarza **Gminy** weryfikacji uprawnień, przynajmniej raz do roku Administrator Systemów Informatycznych/Zasobu dokonuje weryfikacji rzeczywistych uprawnień.
- 7.6. Weryfikacja uprawnień przeprowadzana jest na wybranej losowo próbce użytkowników nie mniejszej niż 10% wszystkich aktywnych kont lub przydzielonych Systemów/Zasobów.
- 7.7. Porównywane są uprawnienia faktycznie posiadane z obowiązującymi upoważnieniami.
- 7.8. Z każdej weryfikacji dokonywana jest notatka służbowa lub raport.
- 7.9. W przypadku wykrycia niezgodności pomiędzy rzeczywistymi uprawnieniami, a uprawnieniami, które powinny zostać nadane, zgłaszany jest incydent związany z bezpieczeństwem informacji. Jeśli stwierdzone uprawnienia są wyższe od wnioskowanych, to po określeniu przyczyn niezgodności uprawnienia są

administracyjnie: korygowane lub odbierane.

- 7.10. W przypadku dłuższej nieobecności w pracy tzn. przekraczającej 3 miesiące (np. urlop bezpłatny, urlop macierzyński, urlop wychowawczy, zwolnienie lekarskie), uprawnienia do Systemów/Zasobów są odbierane, ze szczególnym uwzględnieniem potrzeby wyłącznie zablokowania kont w systemach teleinformatycznych i nieusuwania danych użytkownika. Za poinformowanie Administratora Systemów Informatycznych o wyżej wymienionej nieobecności użytkownika odpowiada Sekretarz **Gminy**.

8. Dostęp do poczty elektronicznej

- 8.1. W **Urzędzie Gminy Wiśniewo** obowiązuje zakaz stosowania służbowej poczty elektronicznej do celów prywatnych/osobistych.
- 8.2. W **Urzędzie Gminy Wiśniewo** obowiązuje zakaz stosowania prywatnej poczty elektronicznej do celów służbowych.
- 8.3. Wiadomości służbowe na skrytkach służbowej poczty elektronicznej stanowią własność Pracodawcy.
- 8.4. Dostęp do służbowej poczty elektronicznej mają osoby uprawnione, osoby je zastępujące i ich przełożeni celem realizacji obowiązków służbowych.
- 8.5. Dostęp do służbowej poczty elektronicznej ma Administrator Systemów Informatycznych w celach realizacji obowiązków służbowych tj. archiwizacji i odzyskiwania danych, zapewnienia ochrony antywirusowej oraz dokumentowania incydentów bezpieczeństwa i naruszeń ochrony danych osobowych.
- 8.6. Dostęp do służbowej poczty elektronicznej nie może naruszać tajemnicy korespondencji. Pracownik, który podczas wykonywania obowiązków służbowych uzyskał dostęp do prywatnej korespondencji innej osoby, jak tylko się zorientuje, iż jest to korespondencja prywatna winien przerwać zapoznavanie się z tą korespondencją i winien zachować jej treść w tajemnicy.

9. Dzienniki administracyjne

- 9.1. W odniesieniu do każdego Systemu Teleinformatycznego prowadzony jest dziennik administracyjny. Dzienniki administracyjne mogą być prowadzone w narzędziach informatycznych.
- 9.2. Dziennik administracyjny uzupełniany jest automatycznie przez oprogramowanie lub uzupełniany jest na bieżąco przez Administratora systemów Informatycznych i zawiera co najmniej następujące informacje:

- identyfikator systemu teleinformatycznego,
 - numer kolejnego wpisu,
 - datę i godzinę dokonania wpisu,
 - imię i nazwisko Administratora Systemów Informatycznych dokonującego wpisu,
 - opis czynności.
- 9.3. Dziennik administracyjny może być prowadzony w dowolnej formie, przy zapewnieniu dostępu i możliwości dokonywania wpisów jedynie przez upoważnionego Administratora Systemów Informatycznych lub autoryzowane oprogramowanie oraz przy zapewnieniu wiarygodności zapisów.
- 9.4. Administrator Systemów Informatycznych jest zobowiązany do okresowego przeglądu logów systemowych. Przegląd logów ma na celu identyfikację wszystkich niepożądanych działań, usterek, ostrzeżeń, które mogą wskazywać na utratę poufności informacji lub dostępności systemu teleinformatycznego.
- 9.5. Logi należy objąć ochroną kopii archiwalnej i utrzymywać w dostępności nie krócej niż przez 2 lata od zarejestrowania zdarzenia. Logi systemowe należy replikować na **centralny serwer logów** oraz zapewnić dostępność narzędzi wspomagających ich przegląd.
- 9.6. W przypadku identyfikacji incydentu bezpieczeństwa informacji należy logi zabezpieczyć na płycie DVD-R w celu przedstawienia dowodów odpowiednim służbom.

10. Monitorowanie działań użytkowników

- 10.1. Działania użytkowników w systemach można monitorować wyłącznie za zgodą **Wójta Gminy Wiśniewo**:
- w ramach wyjaśniania incydentów lub przeprowadzania audytów teleinformatycznych
 - celem spełnienia obowiązków wynikających z przepisów prawa.
- 10.2. Administratorzy systemów mogą monitorować wyłącznie logi, zdarzenia, dzienniki zdarzeń, które są niezbędne do zapewnienia odpowiedniego poziomu usług, a nie śledzeniu treści informacji przetwarzanych przez użytkownika.
- 10.3. W przypadku uzasadnionej potrzeby weryfikacji działań pracownika, dostęp do przetwarzanych treści musi zostać udzielony zgodnie z przepisami prawa oraz przepisami wewnętrznymi oraz musi zostać poprzedzony formalną zgodą **Wójta Gminy Wiśniewo**.
- 10.4. Dostęp do danych z monitorowania użytkowników mają wyłącznie pisemnie upoważnione do tego osoby. Zabrania się udostępniania tych danych celem analizy czasu

i jakości pracy użytkowników.

11. Uwierzytelnianie użytkowników

- 11.1. W systemach IT należy stosować indywidualne konta umożliwiające rozliczalność działań użytkowników.
- 11.2. W systemach IT zabrania się stosowania kont niezabezpieczonych procedurą uwierzytelnienia (identyfikacji i autoryzacji), np. identyfikator i hasło lub certyfikat i pin.
- 11.3. W systemach teleinformatycznych należy zapewnić funkcjonalność:
 - wpisywania haseł bez jawnego ich pokazywania na ekranie logowania;
 - przechowywania haseł w systemie w postaci kryptograficznych skrótów wygenerowanych za pomocą funkcji jednokierunkowych;
 - wymuszania złożoności i okresowej zmiany hasła;
 - możliwość zmiany hasła przez użytkownika.
- 11.4. Hasło użytkownika może być znane wyłącznie użytkownikowi.
- 11.5. W przypadku zaistnienia podejrzenia utraty poufności jak również w przypadku zmiany hasła przez administratora, hasło powinno być niezwłocznie zmienione przez użytkownika.
- 11.6. Zapomniane przez użytkownika hasło, administrator zmienia na hasło tymczasowe, po czym przekazuje go użytkownikowi osobiście, telefonicznie lub za pomocą SMS.
- 11.7. Wszystkie dostarczone hasła standardowe należy bezwzględnie zmienić, niezwłocznie po zainstalowaniu systemu lub aplikacji.
- 11.8. Hasła użytkownika dla każdego systemu teleinformatycznego muszą spełniać przynajmniej:
 - Złożoność – minimum 8 znaków składających się z trzech grup znaków (duże i małe litery, znaki specjalne, cyfry).
 - Okresową zmianę – wszystkie hasła muszą być cyklicznie zmieniane.

12. Hasła Administracyjne

- 12.1. Hasła imienne administratora dla każdego systemu teleinformatycznego muszą spełniać przynajmniej:
 - długość – minimum 12 znaków;
 - złożoność – minimum trzy z czterech grup znaków (małe litery, duże litery, cyfry, znaki specjalne);
 - maksymalny okres ważności haseł – 6 miesięcy.
- 12.2. Dla aplikacji wykorzystujących konta w innych systemach IT (np. bazy danych) definiuje

się następujące minimalne wymagania dotyczące haseł:

- długość – minimum 12 znaków;
- złożoność – minimum trzy z czterech grup znaków (małe litery, duże litery, cyfry, znaki specjalne);
- zalecany maksymalny okres ważności hasła 3 miesiące.

- 12.3. Dla każdego systemu informatycznego administrator systemu zapewnia istnienie loginu i hasła administracyjnego jako administracyjnego konta zapasowego. Konto to powinno być dedykowanym administratorskim kontem zapasowym, niewykorzystywanym w codziennej pracy przez administratorów.
- 12.4. W przypadku braku możliwości technicznej wdrożenia powyższych zasad dotyczących haseł, dopuszczalne jest obszarowe wyłączenie zasady, tzw. odstępstwo. Warunkiem koniecznym do zastosowania odstępstwa jest analiza ryzyka pod kątem zagrożeń wynikających z zastosowania odstępstwa i jeżeli to możliwe, wdrożenie zastępczych środków. Systemy niewspierające interaktywnego mechanizmu nadzorowania jakości haseł mają być separowane od Internetu. Dostęp do nich może być zapewniony przez kanał VPN lub mechanizm reverse proxy, gdzie wymagania odnośnie haseł będą spełnione.
- 12.5. Administrator Systemów Informatycznych zapewnia przechowywanie w formie pisemnej identyfikatora (loginu) i hasła do administracyjnego konta zapasowego, o którym mowa w punkcie 12.3 gwarantującego ciągłość działania usług realizowanych przez administrowane systemy.
- 12.6. Hasło konta zapasowego ma złożoność i długość taką jak hasła imienne administratora oraz jest aktualizowane okresowo zgodnie zapisami punktu 12.2.
- 12.7. Hasło konta zapasowego stanowi tajemnicę **Urzędu** i jest przechowywane w sposób zapewniający ich poufność (zalakowana nieprzejrzysta koperta, zaplombowany pojemnik itp.) także w innej lokalizacji niż administrowane systemy.
- 12.8. Dostęp do hasła administracyjnego konta zapasowego możliwy jest w sytuacji, gdy niezbędny jest dostęp do konta administracyjnego i nie jest możliwe zapewnienie tego dostępu w inny sposób.
- 12.9. Wykorzystanie hasła administracyjnego konta zapasowego jest możliwe w uzasadnionym przypadku przy zapewnieniu poinformowania Administratora Systemów Informatycznych o tym fakcie oraz odpowiedniego udokumentowania użycia hasła.
- 12.10. Po uzyskaniu dostępu do hasła konta zapasowego wymagana jest jego zmiana zgodnie zapisami punktów 12.1 i 12.2.

13. Zarządzanie zmianą

13.1. Przeprowadzanie zmian w systemach IT należy wykonać przy spełnieniu następujących minimalnych wymagań:

- planowanie modyfikacji stosownie do potrzeb powinno obejmować uzgodnienie parametrów modyfikacji (tj. czasu, zakresu) z osobami zainteresowanymi (np. Właścicielem Systemu, Administratorem Systemów Informatycznych, aplikacji, baz danych, osobami odpowiedzialnymi za bezpieczeństwo itp.) oraz analizą wpływu na systemy powiązane;
- przed dokonaniem modyfikacji, w miarę możliwości, należy wykonać kopię zapasową środowiska systemu – oprogramowania, konfiguracji i danych – celem umożliwienia, w przypadku wystąpienia problemów, powrotu do pierwotnego stanu systemu.
- wszystkie modyfikacje powinny być przetestowane w środowisku testowym, w przypadku jego braku osoba odpowiedzialna za utrzymanie systemu zobowiązana jest do podjęcia wszelkich możliwych kroków pozwalających zapewnić bezawaryjną pracę systemu;
- weryfikacja modyfikacji obejmuje sprawdzenie poprawności działania systemu, aktualizację dokumentacji oraz zabezpieczenie nowej (zmienionej) wersji środowiska teleinformatycznego.

13.2. Nie jest wymagane spełnienie wszystkich powyższych punktów w przypadku zmian wprowadzanych do systemów w celu usunięcia awarii.

13.3. Każda informacja o wdrożeniu zmiany w systemie IT wpisywana jest do dziennika administracyjnego tego systemu.

13.4. W przypadku projektów rozwojowych, w miarę możliwości, należy personalnie rozdzielać odpowiedzialności związane z rozwojem i bieżącym utrzymaniem systemu.

13.5. Administrator Systemów Informatycznych zobowiązany jest zapewnić istnienie procedury zarządzania zmianą określającej szczegółowy sposób postępowania w przypadku wprowadzania zmian do systemów. Niniejsza procedura powinna być konsultowana z Sekretarzem **Gminy**.

13.6. Administrator Systemów Informatycznych uczestniczy w planowaniu i realizacji zmian pod kątem oceny wpływu zmiany na bezpieczeństwo teleinformatyczne. Ocena wpływu zmiany na bezpieczeństwo teleinformatyczne odbywa się w formie pisemnej.

14. Aktualizacja bezpieczeństwa

14.1. W przypadku nadesłania lub opublikowania poprawki, jeżeli nie ma pewności, że poprawka pochodzi od producenta lub autoryzowanego przez niego dostawcy, poprawka

jest odrzucana.

- 14.2. Administrator Systemów Informatycznych zobowiązany jest do wyszukiwania i oceny informacji o poprawce i jej wpływie na funkcjonowanie systemu informatycznego. W przypadku gdy w oparciu o pozyskane informacje Administrator Systemów Informatycznych stwierdzi, że poprawka może wywrzeć negatywny wpływ na pracę systemu, nanoszona jest ona (jeśli są możliwości techniczne) w środowisku testowym i weryfikowany jest jej wpływ na działanie systemu.

15. Zarządzanie kopiami bezpieczeństwa

- 15.1. Administrator Systemów Informatycznych zobowiązany jest do opracowania dla każdego systemu IT lub grupy systemów szczegółowej instrukcji wykonywania kopii bezpieczeństwa, ich testowania oraz odtwarzania z nich systemu. W szczególności instrukcja zawiera metodę, zakres, częstotliwość i harmonogram wykonywania kopii systemu, metodę sprawdzania ich poprawności oraz okres ich przechowywania.
- 15.2. Każde testowe odtworzenie danych powinno być odnotowywane w dzienniku administracyjnym systemu. Minimalna zawartość informacyjna testu, zgodnie ze wzorem przedstawionym w **załączniku nr 1** do niniejszego Regulaminu to:
- a) Data testu;
 - b) Wynik: pozytywny, negatywny;
 - c) Czas przywrócenia odtwarzanego systemu lub informacji;
 - d) Opis wskaźnika RPO (Recovery Point Objective) – utraty danych, jeżeli zasadne;
 - e) Opis wszelkich okoliczności, które mają wpływ na skuteczności tworzonych kopii zapasowych oraz archiwalnych.
- 15.3. Każde odtworzenie zasobu, informacji wykonywane na polecenie użytkownika, uprawnionej osoby może zostać potraktowane jako test pod warunkiem spełnienia punktu 15.2.
- 15.4. Kopie zapasowe należy przechowywać poza miejscem przetwarzania informacji celem zabezpieczenia danych na wypadek utraty lokalizacji, pożaru lub innego zdarzenia mającego wpływ na zniszczenie danych w pierwotnym miejscu przetwarzania.
- 15.5. Kopie zapasowe oraz archiwalne wynoszone poza obszar serwerowni **Urzędu Gminy Wiśniewo** muszą być szyfrowane w celu zabezpieczenia istotnych informacji organizacji.
- 15.6. Retencja i zakres kopii zapasowych oraz archiwalnych powinna być konsultowana z właścicielami aktywów oraz zasobów nie rzadziej niż raz w roku.
- 15.7. O każdej nieudanej kopii zapasowej lub archiwalnej należy powiadomić Właściciela

informacji lub Właściciela zasobu. Jeżeli dotyczy to również danych osobowych, należy powiadomić o tym fakcie IOD. **Załącznik nr 10 do PBI** - Procedura „Postępowanie w zakresie wykonywania i obsługi kopii zapasowych oraz okresowego badania nośników służących do przechowywania informacji”.

16. Zabezpieczenie sieci

16.1. Każdy styk sieci LAN z Internetem jest chroniony przed nieuprawnionym dostępem do zasobów Urzędu z wykorzystaniem:

- systemów firewall;
- IDS, IPS;
- ochrony antywirusowej w tym ochrony antywirusowej elektronicznej poczty przychodzącej;
- filtrowanie ruchu WWW pod kątem złośliwego kodu.

16.2. Każda reguła filtrowania tworzona w systemie zabezpieczeń jest udokumentowana przez Administratora Systemów Informatycznych w postaci tabeli ruchu lub archiwizacji kolejnej wersji plików konfiguracyjnych.

16.3. Stosowany system zabezpieczeń gromadzi informacje o naruszeniach lub próbach naruszenia zasad dostępu.

16.4. W celu skutecznej ochrony sieci teleinformatycznej stosowany jest jej podział (segmentacja) oraz ochrona zasobów serwerowych za pomocą systemu firewall.

16.5. Odseparowane są od sieci biurowej zgodnie z najlepszymi praktykami segmenty sieci, w których znajdują się systemy sterowania i nadzoru obiektów technicznych.

Odseparowane sieci mają na celu minimalizacji ryzyk związanych z atakami na infrastrukturę teleinformatyczną **Urzędu Gminy Wiśniewo**. Dozwolone metody separacji: fizyczna – odrębna sieć, logiczna – wydzielone dedykowane VLAN-y. Rekomendowanym rozwiązaniem jest stworzenie co najmniej VLAN-ów:

- a) LAN_biura;
- b) LAN_drukarki;
- c) LAN_WIFI;
- d) LAN_serwery.

16.6. W celu ochrony wewnętrznej sieci LAN serwery usług teleinformatycznych świadczonych na zewnątrz muszą znajdować się w wydzielonym segmencie sieci – strefie DMZ.

16.7. Zaleca się, aby krytyczne systemy IT działały w wydzielonym, o ograniczonym do niezbędnego minimum dostępie, segmencie sieci teleinformatycznej (patrz punkt 17.6).

- 16.8. Kontrola routingu oraz monitorowanie stanu bezpieczeństwa poszczególnych segmentów sieci powinna uwzględniać krytyczność systemów IT działających w danym segmencie.
- 16.9. W celu ochrony poszczególnych segmentów sieci w **Urzędzie Gminy Wiśniewo** wykorzystywano technikę pozwalających na skuteczną ochronę zasobów (np. IDS, IPS).

17. Bezpieczeństwo urządzeń mobilnych

- 17.1. W przypadku gdy w urządzeniach mobilnych (telefonach, tabletach lub urządzeniach o podobnej funkcjonalności) przetwarzane są istotne informacje Urzędu należy zapewnić odpowiednie ich bezpieczeństwo.
- 17.2. Osoby realizujące zakupy urządzeń mobilnych powinny przeprowadzić konsultacje z Administratorem Systemów Informatycznych w celu weryfikacji kompatybilności urządzenia z infrastrukturą **Urzędu** oraz wymagań w zakresie bezpieczeństwa informacji. Wynikiem konsultacji powinno być ustalenie:
- sposobu wykorzystania urządzenia w pracy (wymaganie podłączenie do infrastruktury, zakres informacji przetwarzanych na urządzeniu, w tym informacja czy będą to dane osobowe);
 - możliwość zastosowania minimalnych zabezpieczeń dla urządzenia mobilnego wykorzystywanego poza terenem **Urzędu Gminy Wiśniewo**:
 - szyfrowanie nośników danych;
 - blokada PIN-em, hasłem;
 - instalacja oprogramowania antywirusowego, jeżeli zasadne (wynika z planowanego sposobu korzystania z urządzenia);
 - weryfikacja systemu operacyjnego pod kątem występujących podatności i możliwości ich eliminacji (wynika z planowanego sposobu korzystania z urządzenia).
- 17.3. Zaleca się ograniczenie liczby systemów operacyjnych działających na urządzeniach mobilnych w celu sprawniejszego zarządzania całością infrastruktury.
- 17.4. Administrator Systemów Informatycznych odpowiada za wdrożenie stosownych zabezpieczeń dla urządzeń mobilnych, monitoring skuteczności stosowanych zabezpieczeń.
- 17.5. Administrator Systemów Informatycznych jest zobowiązany do okresowego przeglądu urządzeń mobilnych w zakresie stosowanych zabezpieczeń ich skuteczności. Audyt wewnętrzny SZBI musi obejmować weryfikację bezpieczeństwa informacji przetwarzanych na platformie mobilnej.
- 17.6. Użytkowanie urządzenia mobilnego jest dozwolone:

- w celach związanych z realizacją zadań o charakterze służbowym,
 - w zakresie przyznanych uprawnień.
- 17.7. Użytkownik jest odpowiedzialny za zapewnienie bezpieczeństwa powierzonych mu urządzeń mobilnych w szczególności zapewnienia odpowiedniej ochrony fizycznej urządzenia przed zagubieniem lub kradzieżą.
- 17.8. Użytkownikom zabrania się:
- a) wyłączania lub przełamывania jakichkolwiek zabezpieczeń, które zostały wdrożone na urządzeniu mobilnym,
 - b) kopiowania danych z poczty elektronicznej, kalendarza i kontaktów do innych aplikacji na urządzeniu mobilnym i na urządzenia prywatne,
 - c) dokonywania prób obejścia zabezpieczeń narzucanych przez systemy informatyczne,
 - d) samodzielnej instalacji oprogramowania systemowego i aplikacji,
 - e) innych działań naruszających bezpieczeństwo informacji.
- 17.9. Bezpieczeństwo i monitorowanie urządzeń mobilnych.
- Urządzenia mobilne oraz inne, które umożliwiają dostęp do informacji chronionych **Urzędu Gminy Wiśniewo**, muszą być zabezpieczone. Urządzenia takie muszą spełniać poniższe wymagania.

Dla tabletów, smartphone:

- a) posiadają usunięte lub zmienione domyślne hasła dostępowe,
- b) zostały przetestowane pod względem bezpieczeństwa,
- c) posiadają zainstalowany system antywirusowy,
- d) nośniki danych zostały zaszyfrowane (jeśli są takie możliwości techniczne),
- e) posiadają blokadę ekranu,
- f) są zabezpieczone PIN-em, hasłem lub innym równoważnym zabezpieczeniem,
- g) posiadają skonfigurowaną kopię danych w chmurze (jeśli jest to możliwe).

Dla notebooków:

- a) hasła lokalne spełniają wymagania niniejszego SZBI,
- b) konto gość zostało zdezaktywowane,
- c) zablokowano możliwość uruchamiania notebooka z innego nośnika niż wbudowany dysk,
- d) zabezpieczono dostęp do BIOS-u poprzez ustawienie hasła, zarządzanie hasłami do BIOS,
- e) skonfigurowano szyfrowanie nośników danych, zarządza się kluczem szyfrowania,
- f) zainstalowano nadzorowane oprogramowanie antywirusowe,
- g) wdrożono niezbędne poprawki w systemie operacyjnym i aplikacjach

zainstalowanych na komputerze.

- Urządzenia mobilne oraz inne, które umożliwiają dostęp do informacji chronionych **Urzędu Gminy Wiśniewo**, muszą być zarządzane, to znaczy powinna istnieć możliwość:
 - zdalnego dostępu,
 - monitorowania zdarzeń (np. w event logu),
 - zarządzanie dostępem do sieci LAN **Urzędu** poprzez przypisanie adresu IP.
- Administrator Systemów Informatycznych może w miarę możliwości zdalnie zarządzać urządzeniami mobilnymi, w szczególności blokować, modyfikować, usuwać dane oraz aplikacje lub modyfikować ustawienia urządzenia.

17.10. Incydenty związane z urządzeniami mobilnymi. W przypadku utraty urządzenia fakt ten należy niezwłocznie zgłosić jako incydent bezpieczeństwa informacji zgodnie z obowiązującymi zasadami.

18. Audyty infrastruktury teleinformatycznej

- 18.1. Audyty teleinformatyczne realizowane są zgodnie z obowiązującą procedurą wykonywania audytów wewnętrznych.
- 18.2. Wyniki audytów wewnętrznych mogą zawierać informacje wrażliwe. Jeżeli osoba realizująca audyt uzna to za stosowne, należy zapewnić dostęp do wyników z audytu osobom upoważnionym. Raport z audytu nie może zawierać danych wrażliwych – dane te muszą zostać poddane pseudonimizacji.
- 18.3. Automatyczne narzędzia skanujące sieć lub systemy teleinformatyczne pod kątem istnienia podatności mogą być używane wyłącznie przez upoważnione do tego osoby podczas realizacji audytów wewnętrznych.
- 18.4. Istnieje możliwość korzystania z tego rodzaju narzędzi do wspomagania pracy administratorów sieci lub systemów po uprzedniej pisemnej akceptacji Sekretarza **Gminy**. Przy wyrażaniu zgody bierze pod uwagę możliwość wystąpienia naruszeń bezpieczeństwa w związku z korzystaniem z tego typu narzędzi.

19. Dostęp zdalny (spoza infrastruktury Urzędu)

- 19.1. Dostęp zdalny pracowników **Urzędu Gminy Wiśniewo** jest możliwy na wniosek Sekretarza **Gminy** za pisemną zgodą **Wójta Gminy Wiśniewo**, z zastrzeżeniem punkt 20.2. Dostęp do zasobów **Urzędu** wymaga skonfigurowania na sprzęcie służbowym pracownika **Urzędu Gminy Wiśniewo** klienta VPN i nadania odpowiednich uprawnień oraz ruchu sieciowego w kanale VPN przez Administratora Systemów

- Informatycznych. Dostęp może być czasowy lub jeżeli to zasadne, bezterminowy.
- 19.2. Pracownik pełniący obowiązki Administratora Systemów, ma cały czas możliwość uzyskiwania zdalnego dostępu do systemów teleinformatycznych.
- 19.3. Za terminowe informowanie Administratora Systemów Informatycznych o nadaniu, zmianie i odebraniu uprawnień do pracy zdalnej odpowiada Sekretarz **Gminy**.
- 19.4. W przypadku dopuszczenia do pracy zdalnej podmiotu, osoby trzeciej spoza **Urzędu Gminy Wiśniewo** wymagane jest podpisanie oświadczenia o poufności, stworzenie wymagań w zakresie ruchu sieciowego, akceptacja wniosku o nadanie dostępu przez Informatyka.
- 19.5. Za terminowe informowanie Administratora Systemów Informatycznych o nadaniu, zmianie i odebraniu uprawnień do pracy zdalnej dla zewnętrznego podmiotu odpowiada Sekretarz **Gminy**.
- 19.6. Administrator Systemów Informatycznych zobowiązany do kwartalnych przeglądów dostępu osób z zewnątrz pod kątem zasadności uprawnienia.
- 19.7. Osobie otrzymującej dostęp do infrastruktury **Urzędu Gminy Wiśniewo** należy przedstawić minimalne wymagania w zakresie komputera, z którego korzysta podczas pracy: bezwzględnie zainstalowany aktualny program antywirusowy, wdrożone wszystkie krytyczne poprawki w systemie operacyjnym i aplikacjach wykorzystywanych podczas procesu świadczenia usługi dla **Urzędu**.
- 19.8. W przypadku wystąpienia konieczności pracy poza miejscem zatrudnienia procedury, zasady i warunki pracy zdalnej określa **załącznik nr 14 do PBI** – „Regulamin przetwarzania i ochrony danych osobowych w pracy zdalnej”.

20. Zarządzanie nośnikami danych

- 20.1. Każdy nośnik danych użytkowany służbowo na terenie **Urzędu** wymaga autoryzacji przez Administratora Systemów Informatycznych.
- 20.2. W przypadku przekazywania urządzenia z nośnikiem danych, nośnika wcześniej użytkowanego przez innego użytkownika należy zadbać o skuteczne usunięcie danych. Akceptowalne jest nadpisanie zawartości nośnika ciągiem 0 lub 1 dedykowanym oprogramowaniem do nadpisywania nośników danych.
- 20.3. Urządzenia z nośnikami danych należy przed przekazaniem do serwisu pozbawić nośnika danych, chyba, że z serwisem zawarto umowę o poufności.
- 20.4. Wszystkie nośniki, które są wykorzystywane poza obszarem **Urzędu Gminy Wiśniewo** lub te, dla których prawdopodobieństwo utraty jest wyższe, muszą być zaszyfrowane.
- 20.5. Nośniki danych z serwerów przekazywanych do serwisu, przed przekazaniem do serwisu

należy pozbawić danych.

- 20.6. Tablety, smartphone przekazywane do serwisu należy pozbawić danych, kart pamięci, jeżeli to jest możliwe. W przypadku braku możliwości należy zadbać o wybór serwisów, z którymi można podpisać umowę o zachowaniu poufności lub serwisów, które posiadają certyfikowany system zarządzania bezpieczeństwem informacji na zgodność z ISO/IEC 27001.
- 20.7. Sprzęt podlegający utylizacji należy pozbawić nośników danych, te należy oddać do profesjonalnej firmy gwarantującej trwałe zniszczenie danych.
- 20.8. Urządzenia, w których nie jest możliwe wymontowanie nośnika danych, należy zniszczyć mechanicznie przed przekazaniem do utylizacji. Zniszczeniu muszą podlegać wszystkie nośniki danych, w tym pamięci RAM, dyski elektroniczne.

21. Wytyczne i klauzule obowiązkowe w umowach serwisowych

- 21.1. Informacje niezbędne do realizacji umowy podmiot zewnętrzny udostępnia wyłącznie tym swoim pracownikom, którym są one niezbędne do wykonywania powierzonych zadań.
- 21.2. Powielanie oraz kopiowanie dokumentów, zawierających informacje związane z realizacją umowy wymaga zgody osoby sprawującej nadzór nad realizacją umowy w **Urzędzie Gminy Wiśniewo**.
- 21.3. Powielanie oraz kopiowanie dokumentów zawierających dane techniczne związane z utrzymaniem/wdrożeniem systemów/sieci teleinformatycznych wymaga uzyskania zgody Administratora Systemów Informatycznych.
- 21.4. Przesyłanie drogą elektroniczną dokumentów, o których mowa w powyższych punktach, wymaga zastosowania szyfrowania i przesłania klucza odrębnym kanałem.
- 21.5. Powyższe zapisy nie dotyczą informacji, które:
 - znajdowały się w nieograniczonym posiadaniu podmiotu zewnętrznego przed ich otrzymaniem,
 - są powszechnie znane.
- 21.6. Po zakończeniu realizacji umowy podmiot zewnętrzny zobowiązuje się do niezwłocznego trwałego usunięcia informacji przetwarzanych w formie elektronicznej (usunięcie, zniszczenie nośników itp.), chyba że umowa stanowi inaczej.
- 21.7. Podmiot zewnętrzny podczas wykonywania umowy zobowiązuje się do przestrzegania zasad ochrony informacji obowiązujących w **Urzędzie Gminy Wiśniewo**.
- 21.8. Pracownicy podmiotów zewnętrznych zobligowani są do przestrzegania zasad zawartych w PBI, a dotyczących podstawowych zasad bezpieczeństwa.

- 21.9. W umowach serwisowych należy zapewnić możliwość audytu drugiej strony w zakresie oceny bezpieczeństwa przetwarzania informacji, w tym danych osobowych, powierzanych podmiotowi w ramach współpracy.
- 21.10. Umowa serwisowa musi zawierać informacje na temat zabezpieczania danych przekazywanych na nośnikach w procedurach serwisowych lub reklamacyjnych. Ma zobowiązać wykonawcę do zabezpieczenia własności **Urzędu Gminy Wiśniewo** poprzez usunięcie danych, zaszyfrowanie lub nieprzekazywanie nośników do zewnętrznych organizacji.
- 21.11. Umowy, w których następuje przetwarzanie danych osobowych muszą zawierać klauzule powierzenia przetwarzania danych osobowych według wzoru określonego przez Inspektora Ochrony Danych.

22. Procedury eksploatacyjne

- 22.1. Celem opracowania procedur eksploatacyjnych jest ujednolicenie działań odnoszących się do środków przetwarzania informacji lub przesyłania informacji, takich jak procedury uruchamiania i zatrzymywania serwerów, w tym systemów, tworzenia i testowania kopii zapasowych, konserwacji urządzeń i systemów, obsługi nośników danych, procedur odtworzeniowych na wypadek rozległej awarii, opisów czynności dla pracowników, które dotyczą dużej liczby pracowników (ponad 30, np. stosowanie pola UDW w mailu).
- 22.2. Procedury eksploatacyjne muszą zabezpieczać **Urząd Gminy Wiśniewo** na wypadek utraty kompetencji pracowników **Urzędu** spowodowanych fluktuacją pracowników. Każdą unikalną wiedzę na temat uruchamiania, odtwarzania systemu IT istotnego dla **Urzędu Gminy Wiśniewo** należy udokumentować w sposób umożliwiający nowemu Administratorowi Systemów Informatycznych przeprowadzenie tej procedury.
- 22.3. Procedury eksploatacyjne należy traktować jako element planów ciągłości działania.
- 22.4. Procedury należy przeglądać pod kątem aktualności nie rzadziej niż raz w roku. Za nadzór tego procesu odpowiada Administrator Systemów Informatycznych, za realizację autor procedury eksploatacyjnej.
- 22.5. Procedury powinny zostać udostępnione wszystkim pracownikom, którzy mogą potrzebować ich w sytuacji awaryjnej. Należy rozważyć możliwość alternatywnego udostępniania procedur eksploatacyjnych na wypadek awarii podstawowego systemu informowania.
- 22.6. Dostępność i przegląd procedur eksploatacyjnych powinien być punktem stałym audytu wewnętrznego systemu SZBI.
- 22.7. Za aktualność i przegląd procedur eksploatacyjnych odpowiada Administrator systemów

Informatycznych.

23. Rozwój i utrzymanie systemów informacyjnych

- 23.1. Dla każdego nowego systemu, który będzie przetwarzał informacje w **Urzędzie Gminy Wiśniewo**, w tym dane osobowe, należy opracować wytyczne w zakresie bezpieczeństwa informacji. Wytyczne powinny uwzględniać informacje dotyczące:
- wymagany poziom zaufania wobec podawanej tożsamości użytkowników, w celu zastosowania odpowiednich wymagań dotyczących uwierzytelniania użytkowników;
 - procesy przydzielania dostępu i autoryzacji dla użytkowników biznesowych, jak również dla użytkowników uprzywilejowanych lub technicznych;
 - informowanie użytkowników i operatorów o ich obowiązkach i odpowiedzialności;
 - wymagane potrzeby ochrony zaangażowanych aktywów, w szczególności w zakresie dostępności, poufności i integralności;
 - wymagania wynikające z procesów biznesowych, takich jak rejestrowanie i monitorowanie transakcji oraz wymagania niezaprzeczalności;
 - wymagania narzucane przez inne zabezpieczenia, np. interfejsy do logowania i monitorowania lub systemy wykrywania wycieków danych;
 - obowiązek szyfrowania komunikacji w sieciach publicznych;
 - zalecenie do szyfrowania danych na nośnikach.
- 23.2. Podczas wdrażania nowych rozwiązań należy zadbać o wiedzę w zakresie sposobu licencjonowania oprogramowania, zwłaszcza w przypadku oprogramowania open source. Za ustalenie warunków licencjonowania odpowiada zamawiający system po stronie **Urzędu Gminy Wiśniewo**. Należy ustalić czasokres ważności licencji i zabezpieczyć odpowiednie środki finansowe na przedłużenie licencji zgodnie z potrzebami **Urzędu**. W przypadku tworzenia oprogramowania na zamówienie **Urzędu** przedstawienie stosownych licencji powinno zostać narzucone w umowie z wykonawcą.
- 23.3. Przed podpisaniem protokołu odbioru system produkcyjnie musi mieć wdrożone wszystkie mechanizmy bezpieczeństwa przekazane przez **Urząd Gminy Wiśniewo**. Niedopuszczalne jest uruchamianie systemu i dopracowywanie zabezpieczeń w trakcie życia produkcyjnego systemu.
- 23.4. Przed podpisaniem protokołu odbioru wykonawca musi przekazać informację w zakresie:
- Karty instalacji – zawiera informacje o architekturze systemu, hasłach administracyjnych, wersjach użytych komponentów,
 - Instrukcję odtworzenia danych z kopii zapasowej,
 - Instrukcję odtworzenia całego systemu z kopii zapasowej – na wypadek rozległej

awarii,

- Instrukcje eksploatacyjne dotyczące kopii zapasowych, monitorowania pojemności, dostępności systemu, zarządzania uprawnieniami.

23.5. Dla każdej usługi świadczonej przez zewnętrzne podmioty rekomendowane jest zapisanie w umowie warunków SLA określających:

- Poziom dostępności usługi/systemu w godzinach roboczych **Urzędu Gminy Wiśniewo**,
- Okna serwisowe,
- Czas reakcji na zgłoszenie serwisowe zwykłe (nie dotyczy utraty dostępności systemu),
- Czas reakcji na zgłoszenie serwisowe w trybie pilnym (awaria systemu brak dostępności systemu lub kluczowej funkcjonalności),
- Osobę kontaktową – krótka ścieżka komunikacji na wypadek awarii,
- Osobę kontaktową, opiekuna umowy/kontraktu, umowy SLA,
- Wymagania w zakresie raportowania stanu usługi,
- Definicję niedostępności systemu,
- Definicję zakłócenia pracy systemu,
- Definicję zmiany pilnej,
- Metodę powrotu do wersji systemu po nieudanej zmianie.

23.6. Umowy SLA należy przeglądać w cyklu nie rzadziej niż raz na rok. Odpowiada za to po stronie **Urzędu Gminy Wiśniewo** Administrator Systemów Informatycznych, po stronie dostawcy opiekun kontraktu SLA.

23.7. W umowie wdrożeniowej należy zabezpieczyć możliwość audytu drugiej strony wdrażanego rozwiązania przez **Urząd Gminy Wiśniewo** lub wyznaczony podmiot przed podpisaniem protokołu odbioru. Wynikiem audytu będzie potwierdzenie zamówionych funkcjonalności, zgodności z przepisami prawa, zbadanie bezpieczeństwa systemu w ustalonym zakresie.

24. Odpowiedzialność

Za zarządzanie bezpieczeństwem teleinformatycznym odpowiada Administrator Systemów Informatycznych oraz wszyscy użytkownicy systemów teleinformatycznych **Urzędu Gminy Wiśniewo**.

Załącznik nr 1

**Dziennik administracyjny systemu.
Testowe odtworzenie danych
W Urzędzie Gminy Wiśniewo**

Lp.	Data testu	Wynik Pozytywny / negatywny	Czas przywrócenia odtworzonego systemu lub informacji	Opis wskaźnika RPO (Recovery Point Objective) – utraty danych, jeżeli zasadne	Opis wszelkich okoliczności, które mają wpływ na skuteczności tworzonych kopii zapasowych oraz archiwalnych
1	2	3	4	5	6
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

REGULAMIN ZARZĄDZANIA BEZPIECZEŃSTWEM
FIZYCZNYM

Spis treści

1. Wprowadzenie	3
2. Obszary bezpieczne.....	3
3. Zarządzanie kontrolą dostępu	6
4. Ochrona fizyczna	7
5. Komunikacja	8
6. Odpowiedzialność	9
Załącznik nr 1	10
Załącznik nr 2	11

1. Wprowadzenie

Niniejszy Regulamin zawiera wymagania dotyczące zapewnienia bezpieczeństwa fizycznego we wszystkich lokalizacjach **Urzędu Gminy Wiśniewo**.

2. Obszary bezpieczne

- 2.1. Ze względu na bezpieczeństwo informacji oraz osób i mienia w **Urzędzie Gminy Wiśniewo** wdraża się 3 strefy ochrony fizycznej, odpowiednio strefa I – strefa ogólna, strefa II – strefa administracyjna, strefa III – strefa specjalna.
- 2.2. **Strefa I** ogólna (korytarze, sale spotkań, pomieszczenia sanitarne) - obszar, w którym bez kontroli może przebywać pracownik, współpracownik, interesariusz. Stosuje się podstawowe techniki zabezpieczeń: zamykane drzwi po godzinach pracy **Urzędu**, instalacje alarmowe, wideo monitoring. W godzinach urzędowania w tej strefie może przebywać dowolna osoba.
- 2.3. **Strefa II** administracyjna (Biura) - obszar, do którego dostęp powinien być ograniczany i kontrolowany. Do strefy administracyjnej należą wszystkie obszary związane z działalnością **Urzędu**, które nie mają charakteru obszarów ogólnodostępnych. Wymagają zapewnienia podstawowych wymagań bezpieczeństwa w zakresie kontroli dostępu: zamykane drzwi, instalacja alarmowa, możliwość przebywania w strefie II tylko i wyłącznie w obecności pracownika **Urzędu**.
- 2.4. **Strefa III** bezpieczeństwa (składnice akt, archiwa, kancelaria materiałów niejawnych, serwerownie, punkty dystrybucyjne) - obszar, do którego dostęp jest ograniczony i ściśle nadzorowany. Oprócz zabezpieczeń wymaganych w strefie I i II powinny tutaj zostać zastosowane dodatkowe zabezpieczenia, np. antywłamaniowe drzwi, okna, czujki alarmu, instalacja ppoż. z powiadamianiem o podejrzeniu pożaru odpowiednich osób. Przebywanie w strefie III wymaga rejestrowania osób, które w tej strefie przebywają z podaniem imienia, nazwiska, daty, celu wizyty. W strefie III powinno się również instalować czujniki wilgoci i temperatury w przypadku przechowania, archiwizowania informacji w postaci papierowej i na nośnikach elektronicznych. Przebywanie osoby postronnej w strefie III wymaga akceptacji Administratora Danych Osobowych lub IOD oraz stałej obecności osoby nadzorującej, odpowiedzialnej za bezpieczeństwo danych ze strony **Urzędu Gminy Wiśniewo**.

- 2.5. W każdej lokalizacji należy stosować wytyczne w zakresie nadzoru ruchu osobowego adekwatnie do wrażliwości strefy.

Strefa I.

Brak wytycznych w zakresie nadzoru ruchu osobowego.

Strefa II.

W trakcie pobytu osoby trzeciej w strefie II należy zadbać o ciągły nadzór pracownika **Urzędu** w trakcie całej wizyty w strefie. W przypadku zdarzenia związanego z przebywaniem osoby trzeciej w strefie II bez nadzoru pracownika **Urzędu Gminy Wiśniewo** należy niezwłocznie zgłosić incydent bezpieczeństwa informacji do Administratora Systemów Informatycznych, a osobę zatrzymać do wyjaśnienia.

Podczas pobytu osoby trzeciej w II strefie należy w taki sposób przyjmować interesanta, aby uniemożliwić naruszenie praw innych osób do prywatności, przeciwdziałać możliwości kradzieży dokumentów, informacji.

Należy zadbać o bezpieczeństwo wydruków w taki sposób, aby osoby postronne nie mogły zabrać lub pozyskać informacji utrwalonych w ten sposób.

Niedopuszczalne jest pozostawienie niezabezpieczonych urządzeń do przetwarzania informacji, w tym nośników danych. Komputer należy blokować po utracie kontaktu wzrokowego z urządzeniem.

Wszystkie dokumenty po pracy należy zabezpieczać w zamykanych szafach, biurkach, szufladach, kontenerach. Klucze należy zabezpieczyć przed dostępem osób postronnych.

Inspektor Ochrony Danych jest uprawniony do kontroli zasady czystego biurka po zakończeniu pracy przez pracowników **Urzędu Gminy Wiśniewo**.

Strefa III.

Pracownik **Urzędu Gminy Wiśniewo** przed wejściem do strefy III musi odnotować taki fakt w rejestrze (dopuszczony rejestr w formie papierowej lub elektronicznej, minimalny czas przechowania 2 lata). Tylko osoby uprawnione mogą przebywać i pozyskiwać klucze do pomieszczeń z tej strefy.

W trakcie pobytu osoby trzeciej w strefie III należy zadbać o formalną zgodę na taki dostęp i zapewnić ciągły nadzór. Sprzątanie w tym obszarze może się odbywać

jedynie w obecności uprawnionego pracownika **Urzędu Gminy Wiśniewo**. Nie wolno wносить urządzeń do przetwarzania informacji do strefy III bez wyraźnej potrzeby. W przypadku podmiotów trzecich należy pozyskać formalną zgodę kierownika komórki organizacyjnej odpowiedzialnej za pomieszczenie strefy III. W przypadku zdarzenia związanego z przebywaniem osoby trzeciej w strefie III bez nadzoru pracownika **Urzędzie Gminy Wiśniewo** należy niezwłocznie zgłosić incydent bezpieczeństwa informacji do Administratora Systemów Informatycznych, a osobę zatrzymać do wyjaśnienia i wezwać ochronę, jeżeli zasadne policję (podejrzenie o nieuprawniony dostęp do informacji, kradzież, wandalizm). Osoby nie przetwarzające danych osobowych, a upoważnione ze względu na obowiązki służbowe do przebywania w tej strefie otrzymują właściwe upoważnienie (**Załącznik nr 1** do niniejszego Regulaminu). Wykaz osób upoważnionych do przebywania w tej strefie zawiera **załącznik nr 2** do niniejszego Regulaminu.

Zakaz wnoszenia nośników informacji bez autoryzacji właściwej jednostki merytorycznej.

W przypadku organizowania kolejnych stref ochrony należy opisać strefę w zakresie:

- zasad postępowania pracowników i osób trzecich w strefie;
- opisu stosowanych zabezpieczeń;
- postępowania w sytuacjach awaryjnych;
- osób odpowiedzialnych za bezpieczeństwo, w tym zarządzanie uprawnieniami do stref.

2.6. Jako strefę bezpieczeństwa (strefa III), należy uznać:

- pomieszczenia mające istotne znaczenie dla funkcjonowania **Urzędu**;
- pomieszczenia, w których znajdują się newralgiczne urządzenia systemów IT np. serwerownie, punkty dystrybucyjne, węzły łączności;
- pomieszczenia istotne z punktu widzenia ochrony informacji np. kancelarie materiałów niejawnych, archiwa i składnice dokumentów.

2.7. Wszystkie strefy powinny być zorganizowane tak, aby przepływ osób odbywał się przez przeznaczone do tego przejścia, umożliwiając identyfikację osób i skutecznie oddzielając strefy o podwyższonym stopniu bezpieczeństwa.

2.8. Dostęp do stref administracyjnych przydzielany jest pracownikom **Urzędu** według przydzielonego/wskazanego miejsca pracy i uprawnień. Dostęp współpracownikom **Urzędu Gminy Wiśniewo** przydzielają osoby upoważnione zgodnie z zasadami zarządzania uprawnieniami do zasobów obowiązującymi w **Urzędzie Gminy Wiśniewo**.

2.9. Dostęp do poszczególnych stref bezpieczeństwa przydzielają osoby upoważnione zgodnie z zasadami zarządzania uprawnieniami do zasobów obowiązującymi w **Urzędzie Gminy Wiśniewo**.

3. Zarządzanie kontrolą dostępu

3.1. W każdej lokalizacji należy uniemożliwić dostęp do pomieszczeń osobom nieuprawnionym przez zapewnienie:

- bezpiecznego przechowywania kluczy do pomieszczeń,
- pobrania i zdawania kluczy jedynie przez osoby uprawnione, w tym rejestrowanie tych czynności,
- nadawania uprawnień do pobrania kluczy jedynie osobom, którym dostęp do pomieszczenia jest niezbędny do wykonania zadań służbowych,
- przechowywanie kluczy zapasowych, zabezpieczonych przed nieuprawnionym użyciem.

3.2. Należy sporządzić rejestr kluczy zapasowych oraz określić, kto i w jakich okolicznościach ma prawo do ich pobrania. Każde pobranie klucza zapasowego powinno być odnotowywane wraz z odpowiednią adnotacją.

3.3. W przypadku zgubienia klucza, dysponent pomieszczenia oraz pracownik **Urzędu** odpowiedzialny za bezpieczeństwo podejmują decyzje o niezbędnych krokach zmierzających do skutecznego zabezpieczenia pomieszczenia, w tym wymiany zamka. Zgubienie klucza w każdej sytuacji stanowi incydent bezpieczeństwa informacji.

3.4. Dla wszystkich pomieszczeń w strefach bezpieczeństwa po zgubieniu klucza należy bezwarunkowo zadbać o wymianę zamka.

3.5. Powyższe wymagania dotyczące nadawania uprawnień dotyczą również elektronicznych systemów kontroli dostępu. Należy zadbać, aby istniały

udokumentowane prawa dostępu do danej strefy oraz w przypadku zgubienia/kradzieży klucza elektronicznego (identyfikatora), zostało dokonane odebranie uprawnień tego klucza.

4. Ochrona fizyczna

4.1. Organizując fizyczną ochronę obiektu należy zapewnić:

- przekazanie ochronie w formie regulaminu ochrony fizycznej zasad ochrony obiektu i odpowiedzialności pracowników ochrony;
- okresową (przynajmniej raz na pół roku) oraz doraźną, jeżeli istnieje taka potrzeba, kontrolę przez pracowników **Urzędu** odpowiedzialnych za bezpieczeństwo spełnienia zasad ochrony obiektu;
- zdefiniowanie zasad dokonywania zmian w składzie osobowym pracowników ochrony;
- ustalenie zasad postępowania w przypadku wystąpienia nieprawidłowości w stosunku do przekazanych zasad ochrony obiektu.

4.2. W przypadku powierzenia ochrony obiektu specjalistycznej firmie zewnętrznej należy również zapewnić:

- zamieszczenie w umowie zobowiązania do zachowania poufności informacji w trakcie wykonywania usługi oraz po jej zakończeniu,
- zapoznanie z podstawowymi wymaganiami bezpieczeństwa każdego pracownika ochrony – obowiązek pracodawcy,
- zapisy w umowie odnośnie zgody na okresowe audyty wewnętrzne w zakresie jakości powierzonych zadań związanych z ochroną,
- przeszkolenie przez pracodawcę każdego pracownika z procedury zgłaszania incydentów bezpieczeństwa informacji.

4.3. **Urząd Gminy Wiśniewo** dopuszcza wdrożenie monitoringu wizyjnego na terenie **Urzędu Gminy Wiśniewo** w celu zapewnienia bezpieczeństwa pracowników oraz ochrony mienia. Monitoring nie może być instalowany w pomieszczeniach sanitarnych, szatniach, stołówkach, palarni.

4.4. Każdy pracownik mający dostęp do wideo monitoringu lub utrwalonego materiału

powinien posiadać stosowane uprawnienia oraz upoważnienie do przetwarzania danych osobowych. W przypadku realizacji usługi przez podmiot zewnętrzny należy podpisać stosowną umowę powierzenia i zobowiązać pracodawcę podwykonawcy do upoważnienia swoich pracowników.

4.5. **Urząd** może przechowywać nagrania z video monitoringu przez okres nieprzekraczający 3 miesiące od chwili utrwalenia nagrania. W przypadku, kiedy nagranie stanowi dowód w sprawie dotyczącej przestępstwa okres retencji może zostać przedłużony o czas trwania postępowania oraz możliwości odwołania się od decyzji organu.

4.6. Wszystkie miejsca zarówno wewnątrz budynku oraz na zewnątrz budynku przy wejściach powinny zostać oznaczone tabliczkami oznaczeniem monitoringu, np. „Uwaga obiekt monitorowany” zawierającym również obowiązkowo piktogram kamery oraz klauzulę informacyjną wynikającą z RODO.

4.7. Zgodnie z wymaganiami rozporządzenia RODO należy spełnić obowiązek informacyjny wobec kategorii osób, które zostaną utrwalone na wideo monitoringu.

4.8. W przypadku zgłoszenia z zewnątrz dotyczącego dostępu do utrwalonego materiału, należy przekazać materiał w sposób zapewniający ochronę wizerunku pozostałych osób utrwalonych na materiale. Zasadność, zakres ustala Inspektor Ochrony Danych i to on odpowiada finalnie za zgodę na wydanie materiału. Powyższa zasada nie dotyczy uprawnionych służb.

5. Komunikacja

5.1. Należy zapewnić, przez odpowiednie zapisy w umowach, należytą komunikację na wypadek zdarzenia mającego wpływ na bezpieczeństwo aktywów informacyjnych **Urzędu**, w tym danych osobowych.

5.2. Należy uregulować ścieżkę komunikacji na wypadek zdarzenia mogącego wpłynąć na bezpieczeństwo przetwarzanych informacji.

5.3. W przypadku naruszeń ochrony fizycznej, ataku na chronione obiekty, po zabezpieczeniu mienia **Urzędu Gminy Wiśniewo**, służby są zobowiązane do zaraportowania sytuacji do Informatyka oraz IOD.

6. Odpowiedzialność

- 6.1. Za zarządzanie bezpieczeństwem fizycznym odpowiada Sekretarz **Gminy Wiśniewo**.
- 6.2. Za zarządzanie bezpieczeństwem fizycznym w zakresie zadań wynikających z ustawy o ochronie informacji niejawnych odpowiada Pełnomocnik ds. Ochrony Informacji Niejawnych.

Załącznik nr 1

**UPOWAŻNIENIE DO
PRZEBYWANIA W OBSZARZE PRZETWARZANIA DANYCH**

Data wydania upoważnienia:

ADMINISTRATOR:

w osobie:

WYRAŻA ZGODĘ PANI/PANU:

Imię i nazwisko;

stanowisko służbowe;

czas trwania zgody:

*DO USTANIA STOSUNKU PRACY LUB UMOWY
CYWILNOPRAWNEJ (w zależności od formy zatrudnienia)*

NA PRZEBYWANIE W POMIESZCZENIACH, w których przetwarzane są dane osobowe w zakresie niezbędnym do wykonywania obowiązków służbowych. Jednocześnie zobowiązuje się ww. osobę do zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w pomieszczeniach, co do których uzyskał (a) zgodę na przebywanie.

Zobowiązuję się do zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w pomieszczeniach, w których zachodzi proces przetwarzania niniejszych danych, w oparciu o przedmiotowe upoważnienie. W przypadku wystąpienia naruszenia/incydentu w zakresie przetwarzania danych osobowych jako osoba upoważniona do przebywania w obszarach przetwarzania zobowiązuję się do powiadomienia Administratora o zaistniałym naruszeniu/incydencie bez zbędnej zwłoki od chwili, kiedy zidentyfikowałam(em) naruszenie/incydent bądź dowiedziałam(am) się o wystąpieniu naruszenia/incydentu.

.....
(data i podpis osoby upoważnionej do
przebywania w obszarze przetwarzania
danych)

.....
(data, podpis i pieczęć Administratora)

Załącznik nr 2

**EWIDENCJA OSÓB UPOWAŻNIONYCH DO
PRZEBYWANIA W OBSZARZE PRZETWARZANIA**

Administrator: **Gmina Wiśniewo, Wiśniewo 86, 06-521 Wiśniewo**

LP	IMIĘ I NAZWISKO	STANOWISKO	DATA WYDANIA UPOWAŻNIENIA	DATA USTANIA UPOWAŻNIENIA	ZAKRES UPOWAŻNIENIA	UWAGI
1.				zakończenie stosunku pracy/zakończenie trwania umowy cywilnoprawnej	przebywanie w obszarze przetwarzania	brak
2.				zakończenie stosunku pracy/zakończenie trwania umowy cywilnoprawnej	przebywanie w obszarze przetwarzania	brak
3.				zakończenie stosunku pracy/zakończenie trwania umowy cywilnoprawnej	przebywanie w obszarze przetwarzania	brak
4.				zakończenie stosunku pracy/zakończenie trwania umowy cywilnoprawnej	przebywanie w obszarze przetwarzania	brak
5.				zakończenie stosunku pracy/zakończenie trwania umowy cywilnoprawnej	przebywanie w obszarze przetwarzania	brak
6.				zakończenie stosunku pracy/zakończenie trwania umowy cywilnoprawnej	przebywanie w obszarze przetwarzania	brak

REGULAMIN ZARZĄDZANIA BEZPIECZEŃSTWEM
OSOBOWYM

Spis treści

1. Wprowadzenie.....	3
2. Rekrutacja	3
3. Zatrudnienie w formie umowy o pracę	3
4. Inne formy zatrudnienia	4
5. Zmiana zatrudnienia.....	5
6. Szkolenia okresowe w zakresie bezpieczeństwa informacji	6
7. Zakończenie zatrudnienia.....	7
8. Odpowiedzialność	8
Załącznik nr 1	9

1. Wprowadzenie

Niniejszy dokument przedstawia wewnętrzne regulacje **Urzędu Gminy Wiśniewo**, mające na celu zapewnienie właściwego poziomu bezpieczeństwa osobowego związanego z procesem rekrutacji, szkoleń wstępnych i okresowych, a także przebiegu procesu zmiany i zakończenia zatrudnienia lub współpracy.

2. Rekrutacja

2.1. Proces rekrutacji w **Urzędzie** odbywa się zgodnie z wymaganiami Ustawy o pracownikach samorządowych oraz przepisami wewnętrznymi **Urzędu Gminy Wiśniewo**.

3. Zatrudnienie w formie umowy o pracę

3.1. Przełożony nowozatrudnionego pracownika jest zobowiązany do określenia wymagań, w zakresie dostępu do informacji oraz uprawnień do zasobów (systemów teleinformatycznych, stref dostępu itp.) niezbędnych do wykonania powierzonych pracownikowi obowiązków lub zadań.

Nadanie uprawnień do zasobów odbywa się zgodnie z procedurą zarządzania uprawnieniami w **Urzędzie Gminy Wiśniewo** zawartą w **załączniku nr 13 do PBI**.

3.2. Udostępnienie zasobów informacyjnych **Urzędu Gminy Wiśniewo** (dokumentów, nośników z danymi, systemów teleinformatycznych, stref dostępu itp.) w tym również urządzeń (komputerów, telefonów itp.) musi być poprzedzone szkoleniem wstępnym z zakresu ochrony informacji i zapisów **Polityki Bezpieczeństwa Informacji**, w tym danych osobowych oraz wydaniem stosownych upoważnień (upoważnienie do przetwarzania danych osobowych i upoważnienie do pracy w Systemie Informatycznym **Urzędu**). Szkolenie może zostać przeprowadzone na platformie e-Learningowej, obowiązkowym wymaganiem jest przeprowadzenie oceny skuteczności szkolenia.

3.3. W związku z powyższym, przełożony jest zobowiązany do poinformowania nowozatrudnionego pracownika o konieczności odbycia szkolenia w zakresie ochrony informacji prowadzonego przez Inspektora Ochrony Danych, szkolenie musi obejmować zapoznanie się z:

- obowiązującymi w **Urzędzie Gminy Wiśniewo** zasadami ochrony informacji,

- wskazaniem miejsca, w którym można znaleźć aktualne wymagania dotyczące ochrony informacji,
- wymaganiami obecnie obowiązujących regulacji w obszarze ochrony danych osobowych,
- zasadami ochrony tajemnicy **Urzędu**,
- podstawowymi zasadami bezpieczeństwa informacji,
- zaleceniami dotyczącymi postępowań gwarantujących przestrzeganie obowiązujących w **Urzędzie** instrukcji i procedur dotyczących bezpieczeństwa informacji.

Skuteczność powyższych działań należy ocenić podczas Audytu wewnętrznego SZBI. Wyniki oceny stanowią potencjalny wkład do doskonalenia procesu szkoleń z zakresu SZBI.

3.4. Fakt odbycia szkolenia jest dokumentowany w aktach personalnych pracownika w formie zobowiązania do zachowania poufności stanowiącego **Załącznik nr 1** do niniejszego Regulaminu, jeżeli możliwe na dedykowanej platformie elektronicznej.

3.5. Przed podjęciem zadań lub obowiązków wymagających dostępu do danych osobowych, osobie zatrudnionej nadaje się upoważnienie do przetwarzania danych osobowych w zakresie zgodnym z zasadą wiedzy koniecznej. Przed rozpoczęciem przetwarzania osoba musi przejść szkolenie z ochrony danych osobowych i istniejących wymagań prawnych w tym zakresie. Każda osoba zatrudniona w **Urzędzie Gminy Wiśniewo** powinna mieć świadomość swoich praw i obowiązków w tym zakresie.

3.6. Przed podjęciem zadań lub obowiązków wymagających dostępu do informacji niejawnych konieczne jest ukończenie szkolenia związanego z przetwarzaniem informacji niejawnych realizowanego przez Pełnomocnika ds. Ochrony Informacji Niejawnych oraz uzyskanie pisemnego upoważnienia do dostępu do informacji niejawnych.

4. Inne formy zatrudnienia

4.1. W przypadku podejmowania jakiejkolwiek formy współpracy innej niż umowa o pracę (tj. praktyka, staż, umowa zlecenia, umowa o dzieło itp.) wymagane jest jednoznaczne zdefiniowanie pracownika odpowiedzialnego za realizację współpracy i zabezpieczenie interesów **Urzędu Gminy Wiśniewo** – Opiekuna Umowy.

4.2. Opiekun Umowy jest zobowiązany do określenia wymagań, w zakresie dostępu do informacji oraz uprawnień do zasobów (systemów teleinformatycznych, stref dostępu itp.) niezbędnych do wykonania powierzonych pracownikowi obowiązków lub zadań. Nadanie uprawnień do zasobów odbywa się zgodnie z procedurą zarządzania uprawnieniami w **Urzędzie Gminy Wiśniewo**.

4.3. Udostępnienie zasobów informacyjnych **Urzędu Gminy Wiśniewo** (dokumentów, nośników z danymi, systemów teleinformatycznych, stref dostępu itp.) w tym również urządzeń (komputerów, telefonów itp.) musi być poprzedzone szkoleniem wstępnym z zakresu ochrony informacji.

4.4. W przypadku współpracowników zatrudnionych w formie innej niż umowa o pracę konieczne jest:

- w przypadku praktyki lub stażu wydanie upoważnień do przetwarzania danych osobowych w zakresie zgodnym z zasadą wiedzy koniecznej;
- w przypadku umowy zlecenia lub umowy o dzieło powierzenia przetwarzania danych osobowych.

Przed rozpoczęciem przetwarzania osoba musi przejść szkolenie z ochrony danych osobowych i istniejących wymagań prawnych w tym zakresie. Powinna mieć świadomość swoich praw i obowiązków w tym zakresie.

4.5. Przed podjęciem zadań lub obowiązków wymagających dostępu do informacji niejawnych konieczne jest ukończenie szkolenia związanego z przetwarzaniem informacji niejawnych realizowanego przez Pełnomocnika ds. Ochrony Informacji Niejawnych oraz uzyskanie pisemnego upoważnienia do dostępu do informacji niejawnych.

5. Zmiana zatrudnienia

5.1. W przypadku zmiany powierzonych obowiązków lub wykonywanych zadań, przełożony - w przypadku pracownika lub Opiekun Umowy - w przypadku współpracownika, musi zapewnić:

- przejęcie akt powierzonych spraw,
- odebranie uprawnień do zasobów, do których nie jest wymagany dalszy dostęp (przekazanie informacji do Administratora Systemów Informatycznych),

- przekazanie wszystkich aktywów związanych z informacjami (np. folderów sieciowych),
- nadanie uprawnień do zasobów, do których dostęp jest niezbędny,
- jeżeli z uwagi na zmieniony zakres obowiązków jest to wymagane, przeprowadzenie odpowiedniego szkolenia adekwatnego do rodzaju wykonywanych zadań i przetwarzanych danych.

5.2. W przypadku zmiany warunków zatrudnienia (np. zmiany komórki organizacyjnej, stanowiska) uprawnienia do systemów teleinformatycznych i pozostałych zasobów muszą zostać całkowicie odebrane, a nowe nadane w nowej komórce organizacyjnej. Zasada ta nie obejmuje podstawowych uprawnień, jak np. dostęp do konta domenowego, poczty elektronicznej, dostępu do pomieszczeń, pod warunkiem, że zakres dostępu nie uległ zmianie.

5.3. W przypadku zidentyfikowania niestosowania się do przyjętych w **Urzędzie Gminy Wiśniewo** zasad bezpieczeństwa informacji, wszyscy pracownicy są zobowiązani do zgłoszenia tego faktu zgodnie z przyjętą procedurą zarządzania incydentami oraz poinformowania kierownika komórki organizacyjnej, w której są zatrudnieni.

5.4. W przypadku wszczęcia postępowania dyscyplinarnego, Sekretarz **Gminy** niezwłocznie informuje **Administradora Systemów Informatycznych** o konieczności odebrania uprawnień i udostępnionego sprzętu (w tym również jego zabezpieczenia w celach dowodowych).

5.5. Dopuszcza się stosowanie dowolnych kanałów komunikacji pomiędzy Sekretarzem **Gminy** i **Administratorem Systemów Informatycznych**. W przypadku kontaktu telefonicznego lub osobistego przekazania informacji należy ponownie przekazać tę informację w formie pisemnej w celu zachowania materiału dowodowego (np. wiadomość e-mail).

6. Szkolenia okresowe w zakresie bezpieczeństwa informacji

6.1. W celu utrwalania właściwych zachowań dotyczących zasad bezpieczeństwa informacji, niezbędne jest cykliczne przeprowadzanie szkoleń wśród pracowników i współpracowników. Szkolenia mogą odbywać się w dowolnej formie tj. wykładów, warsztatów, akcji informacyjnych, e-learningu, gier edukacyjnych, newsletterów itp.

6.2. Za zapewnienie cyklicznych szkoleń w obszarze bezpieczeństwa informacji odpowiada

Inspektor Ochrony Danych. W obowiązkowym szkoleniu w obszarze bezpieczeństwa informacji musi uczestniczyć każdy pracownik i współpracownik nie rzadziej niż raz na rok.

- 6.3. W przypadku istotnych zmian w dokumentacji SZBI lub obowiązujących zasadach bezpieczeństwa, Inspektor Ochrony Danych zobowiązany jest zapewnić szkolenie z zasad bezpieczeństwa dla wybranej grupy lub wszystkich pracowników i współpracowników w formie i treści dostosowanej do sytuacji i potrzeb.
- 6.4. Przyjęta forma szkolenia powinna gwarantować jego skuteczność. Niezależnie od przyjętej formy, fakt przeprowadzenia szkolenia powinien być udokumentowany.
- 6.5. Podczas realizacji wszelkich szkoleń wewnętrznych w obszarze bezpieczeństwa informacji, konieczne jest zapewnienie dowodu audytowego odbycia szkolenia. Konieczne jest prowadzenie list obecności zawierających datę szkolenia, tytuł szkolenia oraz listę uczestników. Zasady dokumentowania odbycia szkolenia mogą różnić się w zależności od jego formy. Dokumentacja potwierdzająca odbycie szkoleń przechowywana jest przez Inspektora Ochrony Danych.

7. Zakończenie zatrudnienia

7.1. W przypadku zakończenia lub przewidywanego zakończenia zatrudnienia lub świadczenia pracy na innej podstawie niż umowa o pracę, przełożony lub Opiekun Umowy zobowiązani są do:

- poinformowania osób odpowiedzialnych za odebranie uprawnień do zasobów (systemów teleinformatycznych, stref dostępu itp.) o konieczności ich odebrania w określonym terminie. Dotyczy to wszystkich udzielonych uprawnień;
- poinformowania osób odpowiedzialnych za odebranie udostępnionego wyposażenia związanego z przetwarzaniem informacji (komputerów, telefonów, pamięci Flash-USB itp.) o konieczności ich odebrania w określonym terminie; Potwierdzenie oddania wszystkich zasobów za pomocą karty obiegowej, druków zmiany miejsca użytkowania lub/i protokołów przekazania.
- Niezwłoczne odebranie przez właścicieli zasobów uprawnień wskazanej osobie.

7.2. Proces informowania o konieczności odebrania uprawnień do zasobów oraz odebrania udostępnionego wyposażenia związanego z przetwarzaniem informacji odbywa się zgodnie z funkcjonującą procedurą zarządzania uprawnieniami zawartą w **załączniku**

nr 1 do PBI - Regulamin Zarządzania Bezpieczeństwem Teleinformatycznym.

8. Odpowiedzialność

8.1. Za zarządzanie bezpieczeństwem osobowym odpowiada **Administrator Systemów Informatycznych** oraz **Sekretarz Gminy Wiśniewo**.

Załącznik nr 1

Wiśniewo, dd.mm.rrrr.

Zobowiązanie do zachowania poufności

Ja,, w związku z realizacją na rzecz **Urzędu Gminy Wiśniewo** zadań wynikających z wiążącej mnie z **Urzędem** umowy:

- oświadczam, iż odbyłem szkolenie dotyczące zasad zapewnienia bezpieczeństwa informacji w **Urzędzie**, w tym zasad ochrony danych osobowych,
- zapoznałem/am się z dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji, a także Polityką bezpieczeństwa danych osobowych w **Urzędzie Gminy Wiśniewo**,
- zobowiązuję się do przestrzegania zasad i reguł wynikających z Systemu Zarządzania Bezpieczeństwem Informacji oraz zasad ochrony danych osobowych opisanych w w/w dokumentach,
- zobowiązuję się do zachowania w tajemnicy informacji należących do **Urzędu Gminy Wiśniewo** oraz powierzonych do przetwarzania **Urzędowi Gminy Wiśniewo** przez podmioty zewnętrzne, do których będę miał dostęp w związku z wykonywanymi obowiązkami,
- zobowiązuję się do wykorzystywania w/w informacji wyłącznie w zakresie niezbędnym do realizacji zadań wynikających z wiążącej mnie umowy i niewykorzystywania tych informacji w żadnym innym celu.

Oświadczam, że jestem świadomy/świadoma odpowiedzialności wynikającej z niespełnienia wymagań Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), a także art. 266 Kodeksu karnego.

Niniejsze zobowiązanie do zachowania poufności obowiązuje również po ustaniu stosunku wynikającego z umowy.

.....
Data i podpis składającego
oświadczenie

PROCEDURA
SZACOWANIA I ZARZĄDZANIA RYZYKIEM
BEZPIECZEŃSTWA INFORMACJI
w Urzędzie Gminy Wiśniewo

Spis treści

1.	Definicje	3
2.	Wstęp.....	3
3.	Postępowanie.....	3
4.	Analiza ryzyka bezpieczeństwa informacji:	4
5.	Etapy oceny i postępowania z ryzykiem bezpieczeństwa informacji.....	5
6.	Plan postępowania z ryzykiem	6
7.	Raport z szacowania ryzyka bezpieczeństwa informacji	6
8.	Załączniki:	6

1. Definicje

Ryzyko – potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów powodując w ten sposób szkodę dla **Urzędu Gminy Wiśniewo**.

Zagrożenie – to wydarzenie, które powoduje, że ryzyko materializuje się w postaci wymiernej straty poprzez wystawienie aktywów na utratę, ujawnienie, zniszczenie lub zmianę.

Podatność – to słabość aktywów, która jest wykorzystywana przez zagrożenie w celu spowodowania strat w aktywach.

Szacowanie ryzyka – proces analizy i identyfikowania ryzyka oraz jego ocena.

SZBI – System Zarządzania Bezpieczeństwem Informacji.

BI – Bezpieczeństwo Informacji.

2. Wstęp

Niniejsza metoda analizy ryzyka opracowana została w oparciu o wymagania normy ISO 27001 oraz wytyczne zawarte w normie ISO 27005.

3. Postępowanie

3.1 Klasyfikacja informacji

3.1.1 Wyznaczyć klasy informacji zgodnie z **załącznikiem nr 1** do niniejszej procedury (**tabela nr 1.1**) funkcjonujące w **Urzędzie Gminy Wiśniewo** wraz ze wskazaniem ich wrażliwości.

3.1.2 Wrażliwość Klasy (**WG**) informacji jest wyznaczana, jako funkcja atrybutów poufności, integralności i dostępności danych.

$$\mathbf{WG = P + I + D}$$

Skala atrybutów bezpieczeństwa (P - poufności, I - integralności, D - dostępności) jest umieszczona w **załączniku nr 2** do niniejszej procedury (w **tabeli nr 2.1**).

3.2 Inwentaryzacja aktywów (zasobów).

3.2.1 Zinwentaryzować aktywa wchodzące w skład SZBI. Należy rozważyć takie kategorie aktywów, jak sieć LAN, sieć WAN, protokoły sieciowe, aplikacje, bazy

danych i oprogramowanie informatyczne, sprzęt komputerowy, serwery, sprzęt i nośniki danych, pliki elektroniczne i dokumenty papierowe, lokalizacja i pomieszczenia, personel.

3.2.2 Wskazać osoby odpowiedzialne za nadzorowanie, utrzymanie, korzystanie i bezpieczeństwo grup zasobów w SZBI.

3.2.3 Określić, jakie klasy informacji przetwarzane są przez poszczególne grupy zasobów.

4. Analiza ryzyka bezpieczeństwa informacji:

4.1 Określić zagrożenia, które mogą dotyczyć danej grupy zasobów (przykłady zagrożeń przedstawiono **załączniku nr 3** do niniejszej procedury (w **tabeli nr 3.2**).

4.2 Określić podatności związane z daną grupą (przykłady podatności przedstawiono w **załączniku nr 3** do niniejszej procedury (w **tabeli nr 3.1**).

4.3 Określić zabezpieczenia związane z danym ryzykiem (przykłady zabezpieczeń przedstawiono w **załączniku nr 3** do niniejszej procedury (w **tabeli nr 3.3**).

4.4 Określić wskaźnik efektywności zabezpieczenia (WEZ).

$$WEZ = SZ \times SWZ$$

gdzie:

SZ – skuteczność zabezpieczenia,

SWZ – stopień wdrożenia zabezpieczenia.

Skuteczność zabezpieczenia (SZ) i stopień wdrożenia zabezpieczenia (SWZ) ustalany jest wg skal przedstawionych w **załączniku nr 2** do niniejszej procedury (w **tabeli nr 2.4**).

4.5 Określić prawdopodobieństwo (PR) wystąpienia zagrożenia zgodnie z skalą (**załączniku nr 2** do niniejszej procedury (w **tabeli nr 2.2**).

4.6 Oszacować skutki (S) (zgodnie ze skalą zawartą w **załączniku nr 2** do niniejszej procedury (w **tabeli nr 2.3**)) jakie mogą wynikać na skutek naruszenia bezpieczeństwa (atrybutów poufności, integralności i dostępności) dla **Urzędu**

Gminy Wiśniewo biorąc pod uwagę, aktualnie wdrożone zabezpieczenia.

- 4.7 Wyliczyć wartość ryzyka (**WR**) związanego z danym zagrożeniem, określona wzorem:

$$WR = (WA \times PR \times S) / (WEZ)$$

5. Etapy oceny i postępowania z ryzykiem bezpieczeństwa informacji

- 5.1 Uszeregować ryzyka (stworzyć ranking ryzyk) oraz wskazać ryzyka nieakceptowane.
- 5.2 Ocena ryzyka polega na porównaniu wyznaczonych poziomów ryzyka z ustalonymi wstępnie kryteriami akceptowania ryzyka i umożliwia ustalenie priorytetów w zarządzaniu ryzykiem.
- 5.3 Otrzymany wynik w skali od 1 do 25 przekłada się na ocenę wagi ryzyka.
- 5.4 Ogólne zasady postępowania ze zidentyfikowanym ryzykiem opisane są w tabeli ogólnych zasad wyznaczania ryzyka.

			SKUTEK				
			Bardzo niski	Niski	Średni	Wysoki	Bardzo wysoki
			1	2	3	4	5
PRAWDOPODOBIEŃSTWO	Prawie pewne	5	Ś	W	K	K	K
	Prawdopodobne	4	Ś	W	W	K	K
	Możliwe	3	N	Ś	W	W	K
	Mało prawdopodobne	2	N	Ś	Ś	W	W
	Rzadkie	1	N	N	N	W	W

Wartość	Poziom ryzyka	Opis działania
1-3	Niski (N)	Poziom ryzyka akceptowany – działania podejmowane w zależności od wymaganych nakładów
4-7	Średni (Ś)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
8- 14	Wysoki (W)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania
15-25	Krytyczny (K)	Poziom ryzyka nietolerowany – wymaga natychmiastowego działania

6. Plan postępowania z ryzykiem

- 6.1. Określić warianty postępowania z ryzykiem.
- 6.2. Wyniki analizy ryzyka bezpieczeństwa informacji dla każdego z ryzyk (punktów krytycznych) podlegają ocenie przez Kierownictwo **Urzędu**, które decyduje o podjęciu działań mających na celu minimalizację ryzyk związanych z każdym z ryzyk (punktów krytycznych).
- 6.3. Opracować Plan Postępowania z ryzykiem bezpieczeństwa informacji zgodny z szablonem w **punkcie 4 w załączniku nr 4** do niniejszej procedury.
- 6.4. Dla każdego z wyznaczonych działań minimalizujących ryzyko określa się termin realizacji oraz osobę odpowiedzialną za jego ukończenie.
- 6.5. Postępowanie z ryzykiem może polegać na:
 - 1) zmianie poziomu ryzyka poprzez zastosowanie zabezpieczenia,
 - 2) unikaniu ryzyka,
 - 3) przeniesieniu ryzyka,
 - 4) akceptacji ryzyka.

7. Raport z szacowania ryzyka bezpieczeństwa informacji

Wyniki analizy i oceny ryzyka – w tym informacja na temat poziomu ryzyka akceptowalnego w **Urzędzie Gminy Wiśniewo** – a także decyzje w zakresie podjęcia działań minimalizujących ryzyko, zamieszczone są w formalnym raporcie akceptowanym przez Kierownictwo **Urzędu**. Zakres informacji zawartych w raporcie obejmuje co najmniej dane wskazane w **Załączniku 4** do niniejszej procedury.

8. Załączniki:

Załącznik nr 1 –Klasy informacji

Tabela nr 1.1. Klasy informacji

Załącznik nr 2 – Skale

Tabela nr 2.1. Atrybuty bezpieczeństwa

Tabela nr 2.2. Prawdopodobieństwo

Tabela nr 2.3. Szacowanie skutków

Tabela nr 2.4. Wskaźnik efektywności zabezpieczenia (WEZ)

Załącznik nr 3 – Przykłady zagrożeń, podatności i zabezpieczeń

Tabela nr 3.1. Przykładowe podatności

Tabela nr 3.2. Przykładowe zagrożenia

Tabela nr 3.3. Przykładowe zabezpieczenia

Załącznik nr 4 - Raport z analizy ryzyka bezpieczeństwa informacji

Załącznik nr 1 –Klasy informacji

KLASA INFORMACJI – mówi o stopniu ochrony, jaki informacja powinna mieć zapewniony.
Wyróżniamy następujące klasy informacji:

Tabela nr 1.1. Klasy informacji

<i>Grupa informacji</i>	<i>Opis</i>
Informacja publiczna	Informacje, których obowiązek udostępniania wynika z przepisów prawa, w szczególności informacje publiczne w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Informacje udostępniane w szczególności na stronach internetowych Urzędu Gminy Wiśniewo ,.
Informacja prawnie chroniona	Informacje stanowiące dane osobowe podlegające ochronie na mocy przepisów o ochronie danych osobowych. Informacje przekazane Urzędowi Gminy Wiśniewo przez przedsiębiorcę, co do których podjął on działania w celu zachowania ich w poufności, w szczególności nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą (tajemnica przedsiębiorstwa). Informacje chronione na mocy ustawy o ochronie informacji niejawnych (uregulowane odrębnymi przepisami). Inne informacje chronione z mocy prawa.
Informacja wrażliwa	Informacje wewnętrzne Urzędu Gminy Wiśniewo , wytworzone w Urzędzie Gminy Wiśniewo lub na jego rzecz, niewchodzące w zakres informacji zaklasyfikowanych do pozostałych grup. Są to informacje ogólnie dostępne wewnątrz Urzędu Gminy Wiśniewo oraz przeznaczone do użytku wewnętrznego.
Informacja wymagająca klasyfikacji	Informacje, których ewentualne udostępnienie poza Urząd Gminy Wiśniewo wymaga złożenia stosownego wniosku oraz analizy prawnej dotyczącej możliwości udostępnienia informacji wskazanej we wniosku oraz analizy ewentualnych konsekwencji związanych z jej udostępnieniem.

Załącznik nr 2 – Skale

Tabela nr 2.1. Atrybuty bezpieczeństwa

Poufność (P)	
1	informacja jest ogólnodostępna,
2	udostępnienie informacji osobom nieupoważnionym powoduje straty, nie wiąże się z odpowiedzialnością karną organów Urzędu Gminy Wiśniewo ,
3	Udostępnienie informacji osobom nieupoważnionym powoduje straty i wiąże się z odpowiedzialnością karną organów Urzędu Gminy Wiśniewo .
Integralność (I)	
1	nieautoryzowana zmiana informacji nie wpływa na możliwość funkcjonowania Urzędu Gminy Wiśniewo ani zgodność z wymaganiami prawnymi,
2	nieautoryzowana zmiana informacji uniemożliwia poprawną pracę Urzędu Gminy Wiśniewo i nie jest związana z naruszeniem przepisów prawnych,
3	nieautoryzowana zmiana informacji uniemożliwia poprawne funkcjonowanie Urzędu Gminy Wiśniewo i powoduje naruszenie przepisów prawnych.
Dostępność (D)	
1	informacja może być dostępna z opóźnieniem powyżej 2 dni roboczych,
2	informacja musi być dostępna co najwyżej z opóźnieniem od 1 do 2 dni roboczych,
3	informacja musi być dostępna w każdej chwili.

Tabela nr 2.2. Prawdopodobieństwo

Prawdopodobieństwo (PR)	
1	Rzadkie - zagrożenie jest mało realne, aby mogło wystąpić (nie miało nigdy miejsca),
2	Mało prawdopodobne - zagrożenie nie miało miejsca w przeszłości i istnieje niewielkie prawdopodobieństwo, że wystąpi w przyszłości,
3	Możliwe - zagrożenie występuje w innych organizacjach i może wystąpić w tej organizacji jak w każdej innej o podobnym charakterze,
4	Prawdopodobne - zagrożenie może wystąpić, gdyż miało miejsce w przeszłości i należy sądzić, że wystąpi co najmniej raz w ciągu roku,
5	Prawie pewnie - zagrożenie jest bardzo realne i może wystąpić w każdej chwili lub kilkakrotnie w ciągu roku.

Tabela nr 2.3. Szacowanie skutków

Skutek (wpływ na organizację i/lub proces)	
1	Bardzo niski
2	Niski
3	Średni
4	Wysoki
5	Bardzo wysoki

Tabela nr 2.4. Wskaźnik efektywności zabezpieczenia (WEZ)

Skuteczność zabezpieczenia (SZ)	
1	zabezpieczenie organizacyjne (proceduralne),
2	zabezpieczenie techniczne obsługiwane ręcznie,
3	zabezpieczenie techniczne automatyczne.
Stopień wdrożenia zabezpieczenia (SWZ)	
1	nie stosuje się zabezpieczeń,
2	zabezpieczenie funkcjonuje nieformalnie,
3	zabezpieczenie wprowadzono formalnie, ale jest niedoskonałe,
4	zabezpieczenie wprowadzono formalnie, jest doskonałe i skuteczne.

Załącznik nr 3 – Przykłady zagrożeń, podatności i zabezpieczeń

Tabela nr 3.1. Przykładowe podatności

Grupa podatności	Podatność
Dokumentacja/procedury	brak opracowanych planów ciągłości działania
	brak aktualizacji planów ciągłości działania
	brak procedur testowania planów ciągłości działania
	brak dokumentacji systemów
	brak dokumentacji wymaganej prawem
	brak dokumentów polityki bezpieczeństwa informacji i SZBI
	brak dzienników operatorów
	brak kontroli zmian
	brak listy osób upoważnionych do dostępu do określonej informacji
	brak procedur dostępu do pomieszczeń
	brak procedur eksploatacji elektronicznych systemów zabezpieczeń
	brak procedur eksploatacyjnych
	brak procedur wymiany danych i oprogramowania
	brak procedury monitorowania użycia urządzeń do przetwarzania informacji
	brak rejestrów zdarzeń dla celów audytu
	brak ustanowionych mechanizmów monitorowania naruszeń bezpieczeństwa
	brak wymagań bezpieczeństwa w procesach rozwojowych (umowach)
	brak zabezpieczenia dokumentów przechowywanych
	niedostateczne procedury kontroli zmian
	niedostateczne procedury rekrutacji
Łączność	brak zabezpieczenia linii telekomunikacyjnych
	brak zabezpieczenia transmisji wrażliwych informacji
	transmitowanie haseł w jawnej postaci
Oprogramowanie	brak aktualizacji oprogramowania (usługi sieciowe i systemy operacyjne)
	brak autoryzacji użytkowanych kodów mobilnych
	brak kontroli pobieranego oprogramowania
	brak lub niedostateczne mechanizmy 'patch management'
	brak lub niewystarczające procedury testowania oprogramowania
	brak mechanizmów identyfikacji i uwierzytelniania
	brak mechanizmów monitorowania
	brak sformułowanych wymagań bezpieczeństwa dla tworzonych aplikacji

	niedostateczne zarządzanie hasłami (hasła łatwe do odgadnięcia, przechowywanie hasel w jawnej postaci, niedostateczna częstotliwość zmiany hasel),
	niekontrolowane kopiowanie
	niewłaściwe skonfigurowane aplikacje, usługi lub systemy operacyjne
	skomplikowany interfejs użytkownika
	użytkowanie usług powszechnie uznanych za niegwarantujące bezpieczeństwa
	znane błędy (dziury) w oprogramowaniu
	znane podatności baz danych (replikacja)
	organizacja brak regularnych audytów
Organizacja	brak testowania urządzeń zasilających
	brak wykonywania zadań wynikających z dokumentów określających politykę bezpieczeństwa informacji i ISMS
	brak wykonywanych regularnie procedur nadzoru
	brak wymagań bezpieczeństwa na stanowiskach pracy
	brak wyznaczonych osób odpowiedzialnych za aktywa
	niewłaściwy przydział uprawnień dostępu
	praca pracowników podmiotów zewnętrznych bez nadzoru
	przechowywanie kopii w miejscu wytworzenia
Personel	absencja personelu
	brak audytorów wewnętrznych w zakresie bezpieczeństwa informacji
	brak zastępstw
	brak stosowania „polityki czystego biurka i ekranu”
	brak wylogowania się przy opuszczaniu miejsca pracy
	brak szkoleń w zakresie bezpieczeństwa
Sieć	brak alternatywnych dróg połączenia
Sprzęt	brak kopii zapasowych/archiwalnych
	niewłaściwe wycofywanie nośników z użycia
	niewłaściwe zabezpieczenie okablowania
	pojedynczy punkt uszkodzenia (brak rezerwy)
Środowisko i infrastruktura	brak elektronicznej kontroli dostępu, brak fizycznej ochrony budynków, drzwi, okien
	brak gwarantowanego zasilania
	brak mechanicznych i budowlanych systemów zabezpieczeń
	brak monitorowania przez wyspecjalizowane jednostki SP
	brak planów wymiany infrastruktury
	brak systemów sygnalizacji napadu i włamania
	lokalizacja na terenie zagrożonym powodzią
	stan techniczny budynku
	stan techniczny instalacji grzewczych, systemu ogrzewania

	stan techniczny instalacji odgromowych
	stan techniczny instalacji zasilania
	usytuowanie budynku
	wrażliwość na wilgotność
	wrażliwość na zanieczyszczenie (kurz)
	wrażliwość na zmiany napięcia
	wrażliwość na zmiany temperatury

Tabela nr 3.2. Przykładowe zagrożenia

Grupa Zasobu	Zagrożenie
Bazy danych	Kradzież
	Modyfikacja lub usunięcie danych
	Nieuprawniony dostęp
	Uszkodzenie
Pliki w postaci elektronicznej	Kradzież
	Nieuprawniony dostęp
	Uszkodzenie
Dane w postaci papierowej	Kradzież
	Nieuprawniony dostęp
	Uszkodzenie lub zniszczenie
	Wyciek wrażliwych danych
	Zagubienie
Systemy wspomagające	Awaria urządzenia
	Brak klimatyzacji
	Brak zasilania
	Niedziałanie urządzenia
	Zniszczenie instalacji
Sieci	Awaria urządzenia
	Nieuprawniony dostęp fizyczny
	Niezabezpieczona sieć
	Podśluch
	Przeciążenie ruchu
	Uszkodzenie sieci
Oprogramowanie	Wadliwe działanie lub brak działania
	Rozprzestrzenianie wirusów itp.
Sprzęt i nośniki danych	Awaria sprzętu
	Awaria urządzenia lub jego podzespołów

	Awarie prądowe
	Awarie przez kurz
	Awarie ze względu na temperaturę
	Błędy działania
	Błędy konserwacji
	Błędy personelu obsługującego
	Kradzież
	Nieautoryzowane kopiowanie/zmiana/usunięcie
	Nieprawdziwa informacja lub funkcjonowanie strony intranetowej
	Niewłaściwe wykorzystanie
	Zniszczenie
	Zużycie części
	Zużycie nośników
Budynki/Pomieszczenia	Awaria ze względu na temperaturę lub wilgotność
	Kradzież lub nieupoważniony dostęp do informacji
	Pożar
	Umyślna szkoda
	Wahania napięcia prądu
	Zalanie
Personel zewnętrzny - firmy współpracujące	Błąd personelu obsługującego
	Kradzież
	Nieautoryzowany dostęp
	Niedobór (brak) personelu
	Niemożliwość respektowania swoich potrzeb
	Podśluch lub szpiegostwo
	Szkoda umyślna lub nieumyślna
	Ujawnienie informacji chronionych
	Użycie oprogramowania w niewłaściwy sposób
Personel własny (pracownicy)	Błąd personelu obsługującego
	Kradzież
	Nieautoryzowany dostęp
	Niedobór (brak) personelu
	Podśluch lub szpiegostwo
	Szkoda umyślna lub nieumyślna
	Ujawnienie informacji chronionych
	Użycie oprogramowania w niewłaściwy sposób

Tabela nr 3.3. Przykładowe zabezpieczenia

Grupa Zabezpieczeń	Zabezpieczenie
Proceduralne	Polityka Bezpieczeństwa Informacji, Dokumentacja systemu BI,
Prawne	Wymagania prawne Ustawy, rozporządzenia, uchwały, zarządzenia Zarządzenie ws. wprowadzenia w "Polityki bezpieczeństwa informacji
Techniczne	karty urządzeń
	Konfiguracja dostępu AD, Konfiguracja urządzeń, programów i wygaszacza
	Bezpieczeństwo sieci, firewall, router, VLAN Przeglądy okablowania, monitorowanie ruchu,
	Inwentaryzacja Środków trwałych i nietrwałych Telefony alarmowe,
Organizacyjne	Naczelnicy wydziałów - właściciele aktywów, Upoważnienie do przetwarzania danych osobowych Ograniczony dostęp do zasobu Internetu, umowy z firmami Telefonicznymi Regulamin pracy,
	Oświadczenie o zapoznaniu się z treścią Polityki BI oraz o sposobie postępowania z informacjami w Urzędzie Gminy Wiśniewo
	Upoważnienie do przetwarzania danych osobowych
	Karta użytkownika zasobów informatycznych, Upoważnienie do przetwarzania danych osobowych, podpis użytkownika, Unikalne identyfikatory,
	Odebranie praw administracyjnych, karty urządzeń,
	Plan ciągłości działania
	Przeglądy okablowania, monitorowanie ruchu,
	zasady zwyczajowo przyjęte
	Konfiguracja urządzeń, Monitorowanie systemów informatycznych,

Załącznik nr 4 - Raport z analizy ryzyka bezpieczeństwa informacji

**RAPORT Z ANALIZY RYZYKA BEZPIECZEŃSTWA INFORMACJI
w Urzędzie Gminy Wiśniewo z dnia dd.mm.rrrr**

- data szacowania ryzyka
- lista osób uczestnicząca w analizie ryzyka bezpieczeństwa informacji

1. Klasyfikacja informacji

ID	Nazwa grupy informacji	Przykładowe dokumenty	P	I	D	WG
G01						
...						

2. Zidentyfikowane aktywa

ID	Zidentyfikowane aktywa (zasoby)
...	
...	

3. Wyniki szacowania ryzyka bezpieczeństwa informacji

Nr ryzyka	Ryzyko	Aktywo (Zasób)	Zagrożenie	Podatność	Wartość ryzyka	Akceptacja [TAK/NIE]
R01						
...						

4. Plan postępowania z ryzykiem

Nr ryzyka	Planowane działanie	Osoba odpowiedzialna	Termin realizacji
R01			
...			

5. Uwagi

--

Kierownictwo **Urzędu** przeanalizowało wyniki analizy ryzyka bezpieczeństwa informacji, wyznaczyło kryterium akceptowalności ryzyka oraz deklaruje podjęcie działań zmierzających do minimalizacji nieakceptowanych ryzyk.

Opracował

.....

Zatwierdził

.....

**PROCEDURA AUDYTU WEWNĘTRZNEGO SYSTEMU
ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI**

1. Cel procedury i zakres stosowania

- 1.1. Celem niniejszej procedury jest zapewnienie planowego, systematycznego i niezależnego badania skuteczności Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Zgodności z celami systemu, mającymi zastosowanie wymaganiami prawnymi oraz wynikającymi z wewnętrznych regulacji.
- 1.2. Procedura określa zasady dotyczące planowania, organizowania oraz przeprowadzania audytów wewnętrznych SZBI.

2. Przebieg procedury

- 2.1. Celem audytów wewnętrznych jest ocena czy system zarządzania bezpieczeństwem informacji jest skutecznie wdrożony, funkcjonuje zgodnie z wymaganiami § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz czy występują potrzeby doskonalenia jego elementów. Audyty prowadzone są w sposób obiektywny i bezstronny.
- 2.2. Administrator Danych Osobowych jest odpowiedzialny za planowanie i wyznaczenia audytora do przeprowadzenia audytów wewnętrznych z roczną częstotliwością lub częściej.
- 2.3. Audytor opracowuje programy audytów biorąc pod uwagę ważność procesów oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. Określa on kryteria audytu, jego cel, zakres i ewentualnie terminy i metody.
- 2.4. Możliwe jest również przeprowadzenie audytów nieplanowanych, które mogą zostać zatwierdzone do realizacji przez **Wójta Gminy Wiśniewo** m.in. na podstawie:
 - zarejestrowanych incydentów,
 - wyników poprzednich audytów,
 - wyników przeglądów zarządzania,

- informacji od zainteresowanych stron.
- 2.5. Osoba wyznaczona przez **Wójta Gminy Wiśniewo**, zwana dalej audytorem, realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań ustawowych, dokonywania zapisów, nadzoru nad dokumentami.
 - 2.6. Osoba powołana na audytora nie może audytować swojej własnej pracy.
 - 2.7. W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania Systemu Zarządzania Bezpieczeństwem Informacji, audytor identyfikuje tzw. niezgodności lub spostrzeżenia. Audytor odpowiedzialny jest także za identyfikację potrzeb mających wpływ na doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji.
 - 2.8. Osoba odpowiedzialna za audytowany dział / proces / obszar oraz osoba audytowana ma obowiązek przekazywania prawdziwych, możliwie najpełniejszych informacji, udostępniania wszystkich związanych z procesem dokumentów i zapisów, o które poprosi audytor.
 - 2.9. Wynik audytu zostaje niezwłocznie udokumentowany przez audytora w wypełnionym formularzu audytu i przekazany **Wójtowi Gminy Wiśniewo** najpóźniej w ciągu dwóch dni po jego zakończeniu zgodnie z **załącznikiem nr 1** (Protokół audytu).
 - 2.10. **Wójt Gminy Wiśniewo** dokonuje przeglądu i analizy wyniku audytu oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych niezgodności. Jest to dokumentowane w Protokole audytu.
 - 2.11. Wyniki przeprowadzonego audytu uwzględniane są w szacowaniu wartości ryzyka i skutków wystąpienia naruszenia.

Załącznik nr 1

PROTOKÓŁ AUDYTU SZBI

O opracowaniu

Niniejsze opracowanie ma na celu ocenę jakości stosowanego w organizacji Systemu Zarządzania Bezpieczeństwem Informacji. W ramach prac audytowych przeprowadzonych w dniach dokonano oceny rozwiązań technicznych, informatycznych oraz organizacyjnych stosowanych w celu zapewnienia bezpieczeństwa informacji, a w szczególności spełnienia wymogów określonych w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności.

Zastosowane kryteria oceny

Niniejsze opracowanie zawiera ocenę stosowanych rozwiązań oraz sugestie dotyczące możliwości podniesienia poziomu bezpieczeństwa rozumianego jako jednoczesne spełnienie kryteriów: poufności, integralności, dostępności oraz rozliczalności. Propozycje dotyczące usprawnień przygotowane zostały w oparciu o aktualnie panujące standardy branżowe oraz tzw. „dobre praktyki”, z uwzględnieniem wysokiego poziomu bezpieczeństwa informacji jako podstawowego kryterium.

Program audytu Systemu Zarządzania Bezpieczeństwem Informacji

Przeprowadzenie audytu ma na celu ustalenie stopnia spełnienia wymogów bezpieczeństwa informacji zdefiniowanych w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności. W ramach prac audytowych dokonano oceny Systemu Zarządzania Bezpieczeństwem Informacji i poddano weryfikacji następujące jego cechy (na podstawie §20 ww. rozporządzenia):

1. Zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.
2. Utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.
3. Przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub

poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

4. Podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienia bezpieczeństwa informacji.
5. Bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.
6. Zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
 - zagrożenia bezpieczeństwa informacji,
 - skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
 - stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
7. Zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
 - monitorowanie dostępu do informacji,
 - czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
 - zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.
8. Ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.
9. Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.
10. Zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.
11. Ustalenia zasad postępowania z informacjami, zapewniających minimalizację

wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.

12. Zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
 - dbałości o aktualizację oprogramowania,
 - minimalizowaniu ryzyka utraty informacji w wyniku awarii,
 - ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
 - stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
 - zapewnieniu bezpieczeństwa plików systemowych,
 - redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
 - niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
 - kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.
13. Bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.
14. Zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Stopień spełnienia wymogów KRI dotyczących bezpieczeństwa informacji

Określone w Rozporządzeniu o KRI wymogi zakładają zaplanowanie, wdrożenie i eksploatację Systemu Zarządzania Bezpieczeństwem Informacji w rozumieniu normy ISO 27001. Jak stwierdzono w rozporządzeniu, posiadanie certyfikatu zgodności z powyższą normą jest warunkiem wystarczającym do stwierdzenia pełnego spełnienia wymogów.

REGULAMIN ZARZĄDZANIA INFORMACJAMI

1. W **Urzędzie Gminy Wiśniewo** poszczególne informacje są chronione na podstawie przepisów prawa. W oparciu o wymagania prawne, wszystkie przetwarzane w **Urzędzie Gminy Wiśniewo** informacje podzielone zostały na następujące grupy:

<i>Grupa informacji</i>	<i>Opis</i>
Informacja publiczna	Informacje, których obowiązek udostępniania wynika z przepisów prawa, w szczególności informacje publiczne w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Informacje udostępniane w szczególności na stronach internetowych Urzędu Gminy Wiśniewo .
Informacja prawnie chroniona	Informacje stanowiące dane osobowe podlegające ochronie na mocy przepisów o ochronie danych osobowych. Informacje przekazane Urzędowi Gminy Wiśniewo przez przedsiębiorcę, co do których podjął on działania w celu zachowania ich w poufności, w szczególności nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą (tajemnica przedsiębiorstwa). Informacje chronione na mocy ustawy o ochronie informacji niejawnych (uregulowane odrębnymi przepisami). Inne informacje chronione z mocy prawa.
Informacja wrażliwa	Informacje wewnętrzne Urzędu Gminy Wiśniewo , wytworzone w Urzędzie Gminy Wiśniewo lub na jego rzecz, niewchodzące w zakres informacji zaklasyfikowanych do pozostałych grup. Są to informacje ogólnie dostępne wewnątrz Urzędu Gminy Wiśniewo oraz przeznaczone do użytku wewnętrznego.
Informacja wymagająca klasyfikacji	Informacje, których ewentualne udostępnienie poza Urząd Gminy Wiśniewo wymaga złożenia stosownego wniosku oraz analizy prawnej dotyczącej możliwości udostępnienia informacji wskazanej we wniosku oraz analizy ewentualnych konsekwencji związanych z jej udostępnieniem.

2. Wprowadzenie klasyfikacji informacji, o której mowa w ust. 1 nie powoduje konieczności specjalnego fizycznego oznaczania informacji udokumentowanych, dokonuje się w nich jedynie odwzorowania literowo-cyfrowego zgodnie z Instrukcją kancelaryjną.
3. W **Urzędzie Gminy Wiśniewo** przyjmuje się następujące zasady postępowania z informacjami:

Informacja publiczna	PRZETWARZANIE, PRZECHOWYWANIE, PRZEKAZYWANIE: w sposób gwarantujący zachowanie integralności i dostępności informacji. ZMIANA KLASYFIKACJI i UDOSTĘPNIANIE: na zasadach i w trybie przewidzianym przepisami prawa. NISZCZENIE: zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Urząd Gminy Wiśniewo umowach oraz Instrukcją kancelaryjną.
Informacja prawnie chroniona	PRZETWARZANIE: w sposób gwarantujący zapewnienie bezpieczeństwa informacji ze szczególnym uwzględnieniem atrybutów integralności, dostępności i poufności oraz innych atrybutów bezpieczeństwa, które są wymagane dla danej informacji chronionej na podstawie właściwej ustawy. PRZECHOWYWANIE: w sposób gwarantujący zapewnienie bezpieczeństwa informacji. PRZEKAZYWANIE: wyłącznie osobom uprawnionym, w sposób gwarantujący zachowanie integralności i poufności oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Urząd Gminy Wiśniewo umowach. ZMIANA KLASYFIKACJI: zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Urząd Gminy Wiśniewo umowach. UDOSTĘPNIANIE: wyłącznie uprawnionym osobom lub podmiotom po uzyskaniu zgody kierownika właściwej komórki organizacyjnej Urzędu Gminy Wiśniewo. NISZCZENIE: zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Urząd Gminy Wiśniewo umowach oraz Instrukcją kancelaryjną.
Informacja wrażliwa	PRZETWARZANIE: w sposób gwarantujący zapewnienie bezpieczeństwa informacji, ze szczególnym uwzględnieniem atrybutów integralności, dostępności i poufności. PRZECHOWYWANIE: w sposób gwarantujący zapewnienie bezpieczeństwa informacji. PRZEKAZYWANIE: wyłącznie osobom uprawnionym (pracownikom Urzędu, osobom/pracownikom podmiotów, z którymi Urząd Gminy Wiśniewo zawarł stosowne umowy), w sposób gwarantujący zachowanie integralności i dostępności informacji oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Urząd Gminy Wiśniewo umowach. ZMIANA KLASYFIKACJI: możliwa po podjęciu decyzji przez uprawnione osoby oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Urząd Gminy Wiśniewo umowach. UDOSTĘPNIANIE: wyłącznie po uzyskaniu zgody Kierownika Referatu lub zastępcy Kierownika właściwej komórki organizacyjnej Urzędu Gminy Wiśniewo. NISZCZENIE: zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Urząd Gminy Wiśniewo umowach oraz Instrukcją kancelaryjną.

Informacja wymagająca klasyfikacji	PRZETWARZANIE: w sposób gwarantujący zachowanie integralności, dostępności i poufności informacji. PRZECHOWYWANIE: w sposób gwarantujący zapewnienie bezpieczeństwa informacji. PRZEKAZYWANIE: możliwe wysyłanie adresatom zewnętrznym po dokonaniu analizy prawnej dotyczącej możliwości udostępnienia informacji oraz analizy ewentualnych konsekwencji z tym związanych. Przekazywanie wewnątrz Urzędu Gminy Wiśniewo na zasadach określonych przez kierownika lub zastępcę Kierownika właściwej komórki organizacyjnej Urzędu Gminy Wiśniewo. ZMIANA KLASYFIKACJI: po dokonaniu analizy w tym zakresie. UDOSTĘPNIANIE: wyłącznie po uzyskaniu zgody kierownika lub zastępcy kierownika właściwej komórki organizacyjnej Urzędu Gminy Wiśniewo. NISZCZENIE: zgodnie z Instrukcją kancelaryjną.
---	--

PLAN CIĄGŁOŚCI DZIAŁANIA
Urzędu Gminy Wiśniewo

Spis treści

1. Cel procedury	3
2. Przedmiot	3
3. Zakres stosowania	3
4. Odpowiedzialność i uprawnienia	3
5. Warunki uruchomienia planu	3
7. Plany postępowania w przypadku awarii	4
8. Wykaz zewnętrznych usługodawców.....	5
9. Testowanie planu.....	6
10. Aktualizacja planu	6
11. Działania zapewniające przywrócenie zdolności realizacji działalności.....	7
12. Osoby krytyczne dla realizacji Planu	9

1. Cel procedury

Celem procedury jest minimalizacja zakłóceń w realizacji działalności **Urzędu Gminy Wiśniewo** oraz zapewnienie ciągłości działania **Urzędu** w sytuacji kryzysowej, gdy skutki zaistniałych incydentów zagrażają funkcjonowaniu systemów informatycznych.

2. Przedmiot

Przedmiotem procedury jest postępowanie w przypadku zaistnienia zdarzeń mających wpływ (również potencjalny) na bezpieczeństwo informacji oraz ciągłość działania **Urzędu Gminy Wiśniewo**.

3. Zakres stosowania

Zdefiniowanie działań koniecznych do podjęcia w przypadku dysfunkcji systemu informatycznego.

4. Odpowiedzialność i uprawnienia

- 4.1. Za opracowanie i utrzymanie niniejszego planu ciągłości działania odpowiedzialny jest Administrator Systemów Informatycznych.
- 4.2. Za nadzór nad realizacją działań związanych z opracowaniem i utrzymaniem niniejszego planu ciągłości działania odpowiedzialny jest Administrator Systemów Informatycznych.
- 4.3. Za realizację działań przewidzianych w niniejszym planie ciągłości działania odpowiedzialne są wskazane w nim osoby.

5. Warunki uruchomienia planu

- 5.1. Wykonanie planu rozpoczyna się na skutek zdarzenia (niezależnie od jego źródła i typu), które zaburzyło ciągłość działania lub obniżenie jakości świadczonych usług.
- 5.2. Podstawą Planu jest zapewnienie bezpieczeństwa w pierwszej kolejności ludziom, jeśli ich życie lub zdrowie są zagrożone na skutek zdarzenia.

6. Osoby oraz zasoby wymagane do realizacji planu

O uruchomieniu planu decyduje **Wójt, Zastępca Wójta lub Sekretarz Urzędu**. Do realizacji wyznaczone są osoby, których działania są konieczne do prawidłowej realizacji planu.

7. Plany postępowania w przypadku awarii

7.1. Postępowanie w przypadku awarii komputera

- 1) W przypadku awarii sprzętowej, Administrator Systemów Informatycznych powinien oddać do użytku zastępczą stację roboczą, o ile takowa istnieje, a następnie przystąpić do usunięcia usterki lub powinien wezwać serwis zewnętrzny, jeżeli komputer posiada stosowną gwarancję.
- 2) W przypadku awarii programowej, Administrator Systemów Informatycznych powinien w miarę możliwości sprawdzić co wywołało dany błąd programowy, a następnie szybko usunąć daną usterkę. Jeżeli istnieje podejrzenie o zainfekowaniu komputera, taka stacja robocza powinna zostać odłączona od sieci, a następnie sprawdzona pod kątem obecności wirusów oraz innego, tzw. Złośliwego oprogramowania.

7.2. Postępowanie w przypadku awarii serwera

- 1) W przypadku awarii serwerów, Administrator Systemów Informatycznych powinien przystąpić do rozwiązania powstałego problemu. W przypadku awarii wykraczających poza techniczne możliwości wykonawcy należy zwrócić się do odpowiedniego serwisu zewnętrznego.
- 2) W przypadku awarii sprzętowej, gdzie wymagana jest wymiana danego elementu, a nie ma on zapewnionej redundancji, należy jak najszybciej sprowadzić oraz wymienić dany element, jeżeli serwer nie posiada już gwarancji. W przypadku serwerów będących na gwarancji, należy jak najprędzej wezwać lokalny, autoryzowany serwis.
- 3) W przypadku awarii programowej, np. systemu operacyjnego, silnika baz danych lub innych, kluczowych usług, należy przejrzeć logi systemowe oraz logi danej usługi/aplikacji, celem stwierdzenia czy błąd nie jest w nich jasno określony, wraz ze wskazówkami do jego rozwiązania.

- 4) W przypadku awarii systemu bazy danych, należy ustalić, czy dane zawarte w tym momencie na serwerze są spójne oraz czy nie jest konieczne przeprowadzenie operacji odtworzenia z kopii zapasowej.
- 5) Jeżeli awaria dotyczy uszkodzonej struktury danych lub samych danych w bazie danych, przed jakąkolwiek operacją na niej, należy wykonać kopię zapasową, która umożliwi powrót do stanu przed ingerencją w bazę danych.
- 6) Jeżeli awaria dotyczy silnika bazodanowego, należy ustalić, czy nie były wykonywane jakiejkolwiek zmiany w konfiguracji, a jeżeli takowe nastąpiły, to należy sprawdzić, czy nie one były przyczyną powstałej awarii.
- 7) Jeżeli jest to konieczne, należy podczas usuwania usterki zapewnić ciągłość pracy w możliwie najdłuższym czasie, o ile nie wpływa to negatywnie na spójność systemu. W szczególności każda usterka w bazach danych wymaga wstrzymania pracy tej bazy.

7.3. Postępowanie w przypadku braku zasilania w sieci komputerowej.

- 1) W przypadku stwierdzenia braku zasilania w sieci komputerowej Administrator Systemów Informatycznych kontaktuje się z dostawcą energii elektrycznej PGE Dystrybucja SA Rejon dostępnej pod numerem telefonu +48lub Pogotowiem energetycznym nr 991.
- 2) Serwer podłączony jest do UPS wyposażony w baterie wystarczające na ok. 60 minut pracy.
- 3) Administrator Systemów Informatycznych zobowiązany jest do ukończenia wszelkich prac na serwerze i bezpiecznie wyłączyć system.

7.4. Plan awaryjny na wypadek utraty dostępu do sieci internetowej.

- 1) W przypadku utraty dostępu do sieci Internet, Administrator Systemów Informatycznych zgłasza do firmy Orange dostępnej pod numerem telefonu: +48

8. Wykaz zewnętrznych usługodawców

8.1 Usługi ślusarskie:

.....pracownik gospodarczy Urzędu Gminy Wiśniewo, nr tel.:

8.2 Usługa elektro-energetyczne:

elektryk Referatu Gospodarki Komunalnej, nr tel.:

9. Testowanie planu

- 1) **Urząd** prowadzi okresowe testy Planu zgodnie z ustalonym harmonogramem przez **Sekretarza Urzędu**.
- 2) Podczas testowania Planu sprawdza się wszystkie dane osobowe odpowiadające za realizację scenariusza oraz aktualizuje ich dane kontaktowe. Aktualizuje się także listę zasobów.

Lp.	Opis testu	Czas realizacji	Oczekiwany wynik	Osoba odpowiedzialna
1.	Symulacja wyłączenia serwera danej aplikacji, brak możliwości wykonywania usług, symulacja na podstawie scenariusza zawartego w protokole.	1 dzień	Wznowienie działania usługi, możliwie na nowej maszynie	Administrator Systemów Informatycznych

10. Aktualizacja planu

Plan aktualizowany jest każdorazowo w przypadku zmian kadrowych oraz w przypadku niepowodzenia w jego testowaniu.

11. Działania zapewniające przywrócenie zdolności realizacji działalności

L.p.	Działanie	Czynności operacyjne	Zapewnione zasoby	Odpowiedzialny
1.	Sprawdzić zasadność zgłoszenia od użytkownika	Zweryfikować, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego.	Zapewnić: dostęp do infrastruktury informatycznej na stanowisku, skąd pochodzi zgłoszenie	Administrator Systemów Informatycznych
2.	Ustalić miejsca awarii	Ustalić, co jest źródłem i przyczyną awarii: - wadliwe działanie sprzętu, - wadliwe działanie aplikacji, - wadliwe działanie systemu, na którym uruchomiona jest aplikacja. - brak połączenia z siecią Internet/WAN, - brak połączenia z siecią LAN - przerwa w zasilaniu prądem,	Zapewnić: - dostęp do przedmiotowego komputera/serwera, urządzeń sieciowych / - dostępowych/serwerowni, - kontakt z osobą, która może w porze nocnej pobrać klucze / udostępnić potrzebne pomieszczenie w Urzędzie - w przypadku blokady zamka wezwać konserwatora, - w przypadku awarii zasilania elektrycznego wezwać pogotowie energetyczne	Administrator Systemów Informatycznych
3.	Określić potencjalną skalę awarii	Ustalić, czy awaria powoduje przestój: - jednego stanowiska - wielu stanowisk - całego Urzędu	Zapewnić kontakt z kluczowymi pracownikami, lista z numerami telefonów.	Administrator Systemów Informatycznych
4.	Ustalić czy wznowianie usług może odbywać się w dotychczasowej lokalizacji	Działanie ma na celu zweryfikowanie czy wznowianie usługi uruchamiane będą w dotychczasowej lokalizacji, czy w lokalizacjach alternatywnych.	Zapewnić: - możliwość uruchomienia dowolnych usług w lokalizacji - infrastrukturę sieciową, zasilanie prądem	Administrator Systemów Informatycznych
5.	Rozpocząć procedurę zakupów niezbędnych zasobów, aby dokonać naprawy (wymiany) urządzeń, uruchomić usługi.	W przypadku braku możliwości zakupu należy rozważyć alternatywne rozwiązanie (np. relokować urządzenie z innej jednostki, uruchomić aplikację na innym komputerze/serwerze).	Zapewnić środki na zakup elementów niezbędnych do ponownego uruchomienia systemu.	Administrator Systemów Informatycznych

6.	Zweryfikować możliwość docelowego przeniesienia aplikacji na inny komputer/ serwer	Sprawdzić, czy aplikacja może być uruchomiona na którymś z działających poprawnie komputerów/serwerów. Czy jest możliwość przełączenia na alternatywne łącze / sieć.		Administrator Systemów Informatycznych
7.	Przygotować komputer/komputer y/ urządzenia/serwery zastępcze	Jako urządzenie/serwer zastępczy można wykorzystać np. komputer typu desktop, który należy odpowiednio skonfigurować. Po uruchomieniu aplikacji na komputerze/serwerze zastępczym należy przetestować jego działanie.	Zapewnić komputery/serwery/urządzenia o zbliżonych parametrach, które w podstawowym zakresie pozwolą na uruchomienie podstawowych usług.	Administrator Systemów Informatycznych
8.	Podjąć decyzję o terminie odtworzenia infrastruktury IT	W razie konieczności należy skontaktować się z właściwymi pracownikami	Zapewnić kontakt z kluczowymi pracownikami jednostki, lista z numerami telefonów.	Administrator Systemów Informatycznych
9.	Przywrócić funkcjonowanie aplikacji / systemu IT	Podjąć próbę usunięcia przyczyny nieprawidłowego działania. W razie konieczności należy odtworzyć bazy/aplikacje korzystając z kopii zapasowych.	Zapewnić: - dostęp do najbardziej aktualnej wersji aplikacji, - dostęp do aktualnej kopii bazy danych	Administrator Systemów Informatycznych
10.	Sprawdzenie aplikacji / systemu IT	Po przeniesieniu / uruchomieniu należy zweryfikować prawidłowe funkcjonowanie aplikacji / systemów / połączeń sieciowych.	Zapewnić kontakt z kluczowymi pracownikami jednostki mogącymi przetestować prawidłowość funkcjonowania systemów i aplikacji.	Administrator Systemów Informatycznych
11.	Uruchomienie usług w systemie IT	Po uruchomieniu usługi należy powiadomić właściwych pracowników o tym fakcie.	Zapewnić kontakt z kluczowymi pracownikami jednostki, lista z numerami telefonów. Przygotować wykaz zewnętrznych jednostek usługowych realizujących zadania na rzecz jednostki (przykładowo: usługi ślusarskie, elektryczne, gazownicze, dekarские, hydrauliczne)	Administrator Systemów Informatycznych

12. Osoby krytyczne dla realizacji Planu

LP	Imię i nazwisko	Stanowisko	Dane kontaktowe (tel. komórkowy firmowy/prywatny, tel. stacjonarny, komunikatory, adres email firmowy/prywatny)	Proces	Zastępuje go
1					
2					
3					
4					
5					
6					
7					

PROCEDURA
„PRZEGLĄDY I KONSERWACJE SYSTEMÓW”

Spis treści

1. Cel	3
2. Przeglądy i konserwacje systemów.....	3
3. Usługi autoryzacyjne.....	4
4. Przegląd systemów ochrony na styku z siecią publiczną.....	4
5. Przegląd serwerów	4
6. Przegląd infrastruktury sieciowej.....	5
7. Przegląd systemów zasilania.....	5
8. Przegląd konfiguracji stacji roboczych	6
Wzór: Dziennik przeglądów i konserwacji systemów	7

1. Cel

Przeprowadzanie przeglądów i konserwacji ma na celu wczesne wykrycie i usunięcie nieprawidłowości, zanim doprowadzą one do poważniejszych w skutkach awarii czy ujawnienia danych chronionych

2. Przeglądy i konserwacje systemów

2.1 Warunki ogólne

1. Przeglądy systemów przeprowadza doraźnie Administrator Systemów Informatycznych, z wyjątkiem przeglądów głównych usług autoryzacyjnych oraz systemu ochrony styku z siecią publiczną, które należy przeprowadzać co najmniej raz w roku przez wyspecjalizowane służby.
2. Przeglądom podlegają następujące elementy:
 - a. Usługi autoryzacyjne systemów.
 - b. Systemy ochrony na styku z siecią publiczną.
 - c. Serwery.
 - d. Infrastruktura sieciowa.
 - e. Systemy zasilania.
 - f. Konfiguracja stacji roboczych.
3. Przegląd systemu może być dokonany poprzez analizę danych pozyskanych przez systemy monitorowania zasobów.
4. Konserwacja wskazana jest tam, gdzie przeglądy wykażą taką konieczność oraz tam, gdzie jest zalecana przez producentów rozwiązania.

2.2 Czynności do wykonania

Przegląd działania istotnych elementów systemu powinien przebiegać według podobnego schematu, tj. należy:

- 1) tam, gdzie jest to możliwe, pozyskać systemowe dzienniki zdarzeń generowanych przez badany element w okresie od ostatniego przeglądu,
- 2) dokonać analizy pozyskanych dzienników w zakresie wystąpienia zdarzeń zdefiniowanych przez producenta rozwiązania jako błędy lub ostrzeżenia, ze szczególnym uwzględnieniem możliwości spowodowania sytuacji zagrażających

bezpieczeństwu,

- 3) przejrzeć zgłoszenia serwisowe, które zostały ocenione jako powiązane z badanym elementem systemu,
- 4) pozyskać od producentów rozwiązania, dla wszystkich zaobserwowanych nieprawidłowości, informacje dotyczące przyczyn i skutków tych sytuacji oraz sugerowanych działań naprawczych,
- 5) porównać wynik przeglądu i zapisu w dzienniku przeglądów z poprzednim wynikiem dla tego samego elementu,
- 6) przeprowadzić analizę skutków wdrożenia wszystkich działań naprawczych w odniesieniu do innych systemów,
- 7) przedstawić **Sekretarzowi Gminy** raport z przeglądu z propozycją działań naprawczych wraz z ich skutkami,
- 8) wdrożyć wskazane przez **Sekretarza Gminy** działania naprawcze,
- 9) w przypadku braku działań naprawczych raportu nie sporządza się, a fakt przeprowadzenia przeglądu odnotowuje się w dzienniku przeglądów.

3. Usługi autoryzacyjne

Należy pamiętać, że usługi autoryzacyjne świadczone są zarówno przez **Windows Active Directory** (główne usługi autoryzacyjne), jak i przez inne systemy i aplikacje, w zakresie dostępu do nich.

4. Przegląd systemów ochrony na styku z siecią publiczną

Poza pobraniem i analizą dzienników zdarzeń z tych systemów, należy:

- 1) sprawdzić reguły ustawione na systemach firewall porównując je z wymogami działania **Urzędu**,
- 2) sprawdzić z sieci publicznej usługi i porty udostępniane przez sieć **Urzędu**.

5. Przegląd serwerów

Poza pobraniem i analizą dzienników zdarzeń, działanie serwerów powinno być sprawdzone pod kątem:

- 1) aktualności poprawek systemowych (m.in. narzędzie MBSA),
- 2) poprawności konfiguracji serwerów baz danych (m.in. narzędzie MSSQL BPA),

- 3) poprawności działania podzespołów takich jak pamięci, dyski, karty sieciowe, wentylatory. Do kontroli takiej może być użyte oprogramowanie diagnostyczne, np. dostarczane z serwerem,
- 4) stopnia zajętości dysków oraz czasu ich pracy w stosunku do gwarantowanego przez producenta czasu bezawaryjnej pracy (parametr MTBF),
- 5) średniego obciążenia procesora.

6. Przegląd infrastruktury sieciowej

W przypadku infrastruktury sieciowej, pobranie dzienników zdarzeń może być niemożliwe. Tym większy nacisk należy położyć na dodatkowe źródła informacji o kondycji systemu.

W szczególności, podczas przeglądu należy:

- 1) narysować faktyczny sposób połączeń i przeanalizować pod kątem nieprawidłowości,
- 2) sprawdzić stopień wykorzystania przepustowości kluczowych połączeń,
- 3) tam, gdzie to możliwe, zbadać obciążenie (stopień wykorzystania) urządzeń,
- 4) sprawdzić częstotliwość wystąpień błędów transmisji w dostępnych źródłach,
- 5) przeprowadzić skanowanie sieci w celu wykrycia wszystkich urządzeń i sprawdzenia prawidłowości adresacji,
- 6) sprawdzić ochronę urządzeń przed nieautoryzowanym dostępem przez:
 - a. SNMP (community name public lub private),
 - b. HTTP (Web based management),
 - c. Telnet, SSH.

7. Przegląd systemów zasilania

W przypadku urządzeń zasilających, pobranie dzienników zdarzeń może być niemożliwe. Tym większy nacisk należy położyć na dodatkowe źródła informacji o kondycji systemu.

W szczególności, podczas przeglądu należy:

- 1) sprawdzić obciążenie zasilaczy awaryjnych,
- 2) sprawdzić wiek lub raportowaną przez urządzenie kondycję akumulatorów,
- 3) dla wybranych urządzeń przeliczyć, czy czas gwarantowanego podtrzymania zasilania jest wystarczający do zapewnienia bezpiecznego wyłączenia chronionych

urządzeń,

- 4) wyrywkowo sprawdzić parametry zasilania tam, gdzie zapewniane jest ono przez urządzenia typu on-line,
- 5) wyrywkowo sprawdzić czy do chronionej sieci zasilającej nie są wpięte niepożądane urządzenia,
- 6) sprawdzić ochronę przed nieautoryzowanym dostępem zarówno do centralnego UPS-a jak i do tablic rozdzielczych kluczowych elementów systemu informatycznego,
- 7) **uwaga!** Testy systemów zasilania powinny być przeprowadzane po godzinach pracy **Urzędu** (należy uwzględnić zróżnicowane godziny pracy wszystkich jednostek organizacji wewnętrznej),
- 8) **uwaga!** Nie należy przeprowadzać testów wyłączników różnicowoprądowych, do których podłączone są działające elementy systemu **Urzędu**.

8. Przegląd konfiguracji stacji roboczych

Stacje robocze pracowników stanowią istotny element infrastruktury teleinformatycznej **Urzędu**, a ze względu na potencjalnie dużą dostępność dla nieupoważnionych osób oraz z powodu różnorodnej działalności użytkowników często ich konfiguracja odbiega od wymaganej. Szczególną uwagę należy zwrócić na stacje użytkowane przez osoby o dużych uprawnieniach (Administrator Systemów Informatycznych, kierownicy wszystkich szczebli). Ze względu na dużą liczbę stacji do podstawowego przeglądu konieczne jest użycie oprogramowania narzędziowego. Należy skontrolować:

- 1) zainstalowane systemowe pakiety poprawek (service pack),
- 2) oprogramowanie zainstalowane i uruchamiane,
- 3) zgodność nazewnictwa stacji z przyjętymi regułami,
- 4) istniejące lokalne konta i grupy użytkowników,
- 5) stopień zajętości dysków.

Wzór: Dziennik przeglądów i konserwacji systemów

Lp.	Data przeglądu	Nazwa systemu	Nazwisko i imię osoby przeprowadzającej przegląd	Uwagi

PROCEDURA

"ZGŁASZANIE, REALIZACJA I TESTOWANIE NOWYCH ROZWIĄZAŃ INFORMATYCZNYCH"

Spis treści

1. Cel	3
2. Definicje	3
3. Warunki ogólne	3
4. Czynności do wykonania – zgłaszanie i realizacja nowych rozwiązań teleinformatycznych	4
5. Czynności do wykonania – testowanie nowych rozwiązań teleinformatycznych	6
6. Odbiór wdrożonej Zmiany	6
Wzór zgłoszenia zapotrzebowania na zmianę	8
Wzór arkusza testowego	11

1. Cel

Celem procedury „Zgłaszanie, realizacja i testowanie nowych rozwiązań informatycznych” jest usprawnienie wdrożenia systemów informatycznych w **Urzędzie Gminy Wiśniewo** i zapewnienia minimalizacji przerw w działaniu systemu informatycznego.

2. Definicje

- 1) **Zmiana** - wdrożenie nowego systemu teleinformatycznego, zmiana funkcjonalności lub rozbudowa istniejących systemów o nowe, nieistniejące funkcjonalności, o ile stanowią znaczącą modyfikację systemu. Zmianą nie są prace związane z bieżącą obsługą serwisową istniejących systemów. Zmiana może być realizowana „w trybie zamówień publicznych” lub „w trybie poza ustawą”, a potwierdzeniem realizacji może być umowa lub sama faktura – zgodnie z odpowiednimi przepisami;
- 2) **Wydział merytoryczny** - wydział/biuro/samodzielne stanowisko zgłaszające zapotrzebowanie na Zmianę. Zapotrzebowanie na Zmianę wydział/biuro może zgłaszać we własnym imieniu lub w imieniu wielu zainteresowanych wydziałów/biur.
- 3) **Zakres teleinformatyczny** - zakres wytycznych i założeń teleinformatycznych dotyczący komputerów, serwerów, oprogramowania systemowego, licencjonowania, integracji z istniejącymi systemami itp.
- 4) **Zakres merytoryczny** - zakres wytycznych i założeń dotyczący treści sprawy (tj. jak system ma realizować poszczególne funkcje, aby spełniać potrzeby i wymagania użytkownika), a nie jej strony teleinformatycznej.
- 5) **Wykonawca Zmiany** – firma, której zlecono realizację zmiany. W szczególnych przypadkach Wykonawcą Zmiany mogą być Administrator Systemów Informatycznych.

3. Warunki ogólne

- 1) Procedurze podlegają Zmiany, o których mowa w ust. 2 pkt 1.
- 2) Za ewidencjonowanie Zgłoszeń zapotrzebowania na Zmianę odpowiada Administrator Systemów Informatycznych.
- 3) Termin realizacji zmiany będzie każdorazowo ustalany pomiędzy Administrator Systemów Informatycznych a Sekretarzem **Gminy** z uwzględnieniem ważności zmiany

oraz obłożenia bieżącymi i wcześniej zaplanowanymi zadaniami.

- 4) Sekretarz **Gminy** powinny zgłaszać zapotrzebowanie na zmiany przed ustaleniem budżetu na rok następny.
- 5) Za realizację procedury w zakresie teleinformatycznym odpowiada Sekretarz **Gminy** oraz wskazani przez niego, Administrator Systemów Informatycznych.
- 6) Za realizację procedury w zakresie merytorycznym odpowiada Sekretarz **Gminy** oraz Administrator Systemów Informatycznych.
- 7) W przypadku większych Zmian, zaleca się przeprowadzenie testów pośrednich weryfikujących poszczególne funkcjonalności – w takim przypadku zaleca się także stosowanie niniejszych wytycznych.
- 8) Obligatoryjnym testem jest test weryfikujący wdrożenie całej Zmiany (test końcowy).
- 9) Testy powinny być przeprowadzane w środowisku testowym.
- 10) Przez środowisko testowe rozumie się (w zależności od możliwości, potrzeb i wymagań testowanego systemu):
 - a. bazę danych będącą kopią bazy produkcyjnej (normalnie wykorzystywanej w pracy systemu);
 - b. oddzielną instalację systemu teleinformatycznego/komponentów/usług.

4. Czynności do wykonania – zgłaszanie i realizacja nowych rozwiązań teleinformatycznych

- 1) Sekretarz **Gminy** zgłasza zapotrzebowanie na wprowadzenie Zmiany do Administratora Systemów Informatycznych na Wniosku, którego wzór stanowi **Załącznik nr 1** do niniejszej procedury. W opisie Sekretarz **Gminy** powinien jak najdokładniej opisać swoje wymagania określając wymagania merytoryczne i użytkowe m.in. na ilu stanowiskach i w jakim zakresie zmiana będzie wykorzystywana oraz wstępnie oszacować koszty uwzględniając m.in. zakres merytoryczny, ilość licencji, migrację danych, szkolenia, gwarancję.
- 2) Administrator Systemów Informatycznych analizuje i opiniuje wnioski. W ramach analizy weryfikowane są posiadane już lub wymagane zasoby teleinformatyczne (np. serwery, bazy danych, licencje systemowe, parametry stacji roboczych), posiadane dane, możliwość integracji z innymi systemami oraz automatyzacji, sposoby

licencjonowania, wymogi formalne związane z przepisami o ochronie danych osobowych. Na podstawie wszystkich tych informacji określana jest wykonalność Zmiany oraz szacowane są całkowite koszty. Jeżeli zmiana dotyczy danych osobowych to zgłoszenie zapotrzebowania na zmianę akceptuje **IOD**.

- 3) W przypadku braków w części merytorycznej Wniosku, Administrator Systemów Informatycznych zwraca Wniosek do Sekretarza **Gminy** z prośbą o uzupełnienie informacji.
- 4) Decyzję o realizacji Zmiany – po zaopiniowaniu przez Sekretarza **Gminy**- podejmuje **Wójt Gminy, Skarbnik Gminy** – każdy w swoim zakresie. Jeżeli zmiana może zostać zrealizowana w ramach posiadanych środków oraz jej zasadność nie budzi wątpliwości to decyzję o realizacji może podjąć Sekretarz **Gminy**.
- 5) W przypadku realizacji Zmiany w trybie Zamówień Publicznych, w skład komisji przetargowej **wchodzą pracownicy Sekretarz Gminy, Administrator Systemów Informatycznych i pracownik Zamówień Publicznych.**
- 6) Po zakończeniu procedury przetargowej - lub w przypadku realizacji Zmiany poza trybem Zamówień Publicznych - dalsze prace prowadzi zespół wdrożeniowy, w skład, którego wchodzi wskazani we Wniosku Administrator Systemów Informatycznych, Sekretarz **Gminy**.
- 7) Administrator Systemów Informatycznych odpowiada za realizację i wdrożenie Zmiany, w tym za: dokładne opisanie wymagań merytorycznych, nadzór nad wykonawcą i terminową realizacją Zmiany, testowanie i odbiór wdrożonej Zmiany w zakresie merytorycznym.
- 8) Administrator Systemów Informatycznych pełni nadzór nad realizacją i wdrożeniem Zmiany w zakresie teleinformatycznym, w tym nad: koordynacją wprowadzenia Zmiany, prawidłowym określeniem wymagań technicznych, przygotowaniem i konfiguracją środowiska instalacji – zarówno na serwerach jak i na stacjach roboczych, określeniem wymaganych zakresów uprawnień i ich nadaniem, współpracą z wykonawcą w zakresie technicznym, konfiguracją możliwości zdalnego serwisowania. Po okresie wdrożenia Administrator Systemów Informatycznych przejmuje bieżące serwisowanie.
- 9) Wprowadzenie zmiany musi zakończyć się testowaniem nowych rozwiązań teleinformatycznych zgodnie z ust. 5.

5. Czynności do wykonania – testowanie nowych rozwiązań teleinformatycznych

- 1) Testowanie jest realizowane po zgłoszeniu przez Wykonawcę Zmiany gotowości do odbioru Zmiany (przeprowadzenia testu).
- 2) Wykonawca Zmiany przygotowuje arkusze testów zgodnie ze wzorem, który stanowi **Załącznik nr 2** do niniejszej procedury.
- 3) Zaleca się, aby scenariusz testu zawierał – oprócz opisu poszczególnych kroków – odpowiednie zrzuty ekranów.
- 4) Przed rozpoczęciem testu, Administrator Danych Osobowych musi zaakceptować scenariusz testu.
- 5) Administrator Systemów Informatycznych weryfikują warunki początkowe określone w scenariuszu i przygotowują środowisko testowe.
- 6) Test jest wykonywany przez osoby, o których mowa w ust. 3 pkt 6.
- 7) Osoby, o których mowa w ust. 3 pkt 5 nadzorują wprowadzanie Zmiany i realizację testu w zakresie teleinformatycznym (systemy operacyjne, bazy danych, instalacja oprogramowania, definiowanie użytkowników i uprawnień, zabezpieczanie danych itp.).
- 8) W przypadku negatywnego wyniku testu, należy w polu Uwagi opisać przyczynę niezaliczenia testu. W takim przypadku Wykonawca Zmiany musi wykonać czynności naprawcze, a sam test musi być przeprowadzony ponownie.
- 9) Przeprowadzenie testu jest potwierdzone wypełnionym i podpisanym – przez osoby przeprowadzające test - arkuszem testowym. Arkusze testowe mają być przechowywane razem z protokołami odbioru.

6. Odbiór wdrożonej Zmiany

- 1) Odbiór Zmiany może nastąpić dopiero po pozytywnym zakończeniu testów.
- 2) Protokoły odbioru Zmiany podpisywane są przez:
 - a. Sekretarz Gminy w zakresie merytorycznym;
 - b. Administrator Systemów Informatycznych w zakresie teleinformatycznym; lub osoby przez nich wyznaczone.

- 3) Po przeprowadzeniu odbioru, Zmiana przechodzi z etapu testowania do etapu jej produkcyjnego wykorzystania.
- 4) Uruchomienie produkcyjne wiąże się m.in. z:
 - a. weryfikacją i aktualizacją uprawnień IT;
 - b. aktualizacją odpowiednich zasobów;
 - c. zdefiniowaniem uprawnień dla użytkowników;
 - d. zdefiniowaniem zasad zabezpieczania i archiwizacji danych przez administratorów.
- 5) Przed produkcyjnym uruchomieniem Sekretarz **Gminy**, zgodnie z zasadami określonymi w Polityce Zarządzania Bezpieczeństwem Informacji, składa wnioski o nadanie uprawnień dla podległych pracowników.

Załącznik nr 1
do Procedury zgłaszania, realizacji i testowania nowych rozwiązań teleinformatycznych:
Zgłoszenie zapotrzebowania na Zmianę.

Dane Wydziału merytorycznego:	
Temat Zmiany:	(nazwa Zmiany)
Zmiana:	(opis proponowanej Zmiany, oczekiwane rezultaty)
Wydziały merytoryczne:	(Wydział, który zgłasza zmianę)
Rodzaj zmiany:	☐ obligatoryjna ze względu na przepisy prawne ☐ usprawniająca pracę wydziału merytorycznego
Przyczyna wnioskowania o zmianę:	(przyczyna, stan obecny, zakładane efekty)
Podstawa prawna:	(podstawa prawna, przepisy branżowe, prawo miejscowe, wymogi UE)
Wymagany termin wdrożenia zmiany:	(termin wdrożenia zmiany wymagany przepisami prawnymi lub innymi czynnikami)
Szkolenia:	(czy i w jakim zakresie są konieczne szkolenia merytoryczne)
Szacunkowa wycena: (jeżeli istnieje analogiczne wdrożenia)	(szacunkowa wycena uwzględniająca m.in. zakres merytoryczny, ilość licencji, migrację danych, szkolenia, gwarancję)

Proponowane źródło finansowania:	(proponowane źródło finansowania)
Wydziały/biuro/instytucje współpracujące w zakresie Zmiany:	(inne jednostki/instytucje korzystające ze Zmiany)
Rozpoznane wdrożenia w innych instytucjach:	(przykłady wdrożeń w innych jednostkach/instytucjach)
Pracownicy Wydziałów merytorycznych oddelegowani do przeprowadzenia zmiany	(lider – koordynator Wydziału merytorycznego) (pracownicy merytoryczni)
Podpis Naczelnika Wydziału merytorycznego	(data) (podpis)
Administrator Systemów Informatycznych	
Dostępne zasoby sprzętowe/techniczne:	(analiza wykonalności Zmiany pod kątem dostępnych zasobów sprzętowych)
Dostępne zasoby programowe:	(analiza wykonalności Zmiany pod kątem dostępnych zasobów programowych)
Dostępne dane:	(analiza wykonalności Zmiany pod kątem dostępnych danych)
Szkolenia:	(czy i w jakim zakresie są konieczne szkolenia teleinformatyczne)
Weryfikacja szacunkowej wyceny:	(weryfikacja szacunkowej wyceny Wydziału merytorycznego z uwzględnieniem wymagań teleinformatycznych)

Opinia n/t możliwości realizacji Zmiany:	☐ pozytywna	☐ negatywna	☐ warunkowa
Zalecenia, uzasadnienie opinii, uwagi:	☐ zalecenia do umowy ☐ zalecane testy pośrednie (uzasadnienie do opinii warunkowej lub negatywnej)		
Pracownicy Wydziału Informatyki oddelegowani do przeprowadzenia zmiany	(lider – koordynator Wydziału Informatyki) (pracownicy Wydziału Informatyki)		
Podpis Naczelnika Wydziału Informatyki	(data)	(podpis)	
Podpis IOD	(data)	(podpis)	
Decyzja Wójta Gminy, Pełnomocnika Wójta Gminy ds. Inwestycji i Gospodarki Przestrzennej, Sekretarza lub Skarbnika			
Decyzja:			

Wzór arkusza testowego

Załącznik nr 2 do Procedury zgłaszania, realizacji i testowania nowych rozwiązań teleinformatycznych:
Arkusz testowy

Temat testu:	(temat testu)	
Rodzaj testu:	☐ pośredni	☐ końcowy
Scenariusz testu merytorycznego (opracowuje Wykonawca Zmiany)		
Warunki początkowe konieczne do przeprowadzenia testu:	(opis wymagań koniecznych do spełnienia przed przystąpieniem do testu)	
Czynności konieczne do przeprowadzenia testu:	(opis czynności testowych)	
Oczekiwane rezultaty:	(opis oczekiwanych rezultatów)	
Akceptacja Naczelnika wydziału merytorycznego:	(data akceptacji testu)	(podpis)
Wynik testu merytorycznego (wypełnia Administrator Systemów Informatycznych)		
Wynik testu:	☐ pozytywny ☐ negatywny	
Uwagi, komentarze:	(uwagi, komentarze do testu merytorycznego)	
Podpisy osób testujących:	(data testu)	(podpis)

Weryfikacja Wydziału Informatyki (wypełnia Wydział informatyki)	
Wynik weryfikacji:	☐ pozytywny ☐ negatywny
Uwagi, komentarze:	(uwagi, komentarze do weryfikacji teleinformatycznej)
Podpisy osób weryfikujących:	(data weryfikacji) (podpis)

PROCEDURA

**„POSTĘPOWANIE W ZAKRESIE WYKONYWANIA
I OBSŁUGI KOPII ZAPASOWYCH ORAZ
OKRESOWEGO BADANIA NOŚNIKÓW SŁUŻĄCYCH
DO PRZECHOWYWANIA INFORMACJI”**

Spis treści

1. Cel.....	3
2. Wykonywanie kopii zapasowych (backup) i archiwizacja	3
3. Odtwarzanie	7
4. Okresowe badanie nośników służących do przechowywani informacji (kopii archiwalnych/nośników archiwalnych)	8
5. Przechowywanie	9
6. Likwidacja kopii	10
Załącznik 1	11
Załącznik 2.....	12

1. Cel

Celem procedury wykonywania i obsługi kopii zapasowych jest zapewnienie bezpieczeństwa przetwarzanych informacji, tj. zapewnia możliwość powrotu do stanu sprzed awarii lub innego zdarzenia związanego z naruszeniem danych. W celu zapewnienia bezpieczeństwa przetwarzania informacji wykonuje się kopie zapasowe i archiwalne. Archiwizacja jest procesem zbliżonym do wykonywania kopii zapasowych (backupu). Najistotniejsza różnica polega na przeznaczeniu skopiowanej informacji. Kopie zapasowe mają za zadanie umożliwić doraźne odtworzenie danych po awarii, niepożądaną zmianie lub skasowaniu, podczas gdy rolą kopii archiwalnych jest z jednej strony umożliwienie wglądu w dane historyczne, z drugiej – zapewnienie możliwości odzyskania danych w sytuacji, gdy dane z backupu zawiodą.

2. Wykonywanie kopii zapasowych (backup) i archiwizacja

2.1 Warunki ogólne

1. Harmonogram wykonywania kopii:
 - a. zapasowych – tam, gdzie to możliwe co najmniej raz dziennie, we wszystkie dni robocze,
 - b. archiwalnych - nie rzadziej niż raz w miesiącu.

Harmonogram wykonywania kopii zapasowych lub archiwalnych stanowi załącznik **nr 1** do niniejszej Procedury.

2. Termin przechowywania kopii:
 - a. zapasowych – 2 tygodnie,
 - b. archiwalnych - co najmniej tak długo, aby możliwe było odtworzenie z nich danych, do przechowywania których **Urząd** jest zobowiązany. Jeżeli kilka kopii archiwalnych zawiera te same wymagane dane lub jeżeli dane z jednej kopii są podzbiorem drugiej – przechowywanie nadmiarowej kopii archiwalnej nie jest konieczne.
3. Kopie zapasowe zawierają wszystkie pliki i programy z wyjątkiem:
 - a. danych o charakterze tymczasowym, które nie są niezbędne do odtworzenia stanu systemu,

- b. danych o dużej objętości i pomijalnym znaczeniu dla systemu informatycznego **Urzędu**.
 - c. danych przechowywanych na dyskach lokalnych stacji roboczych.
4. Archiwizacji podlegają wszystkie pliki i programy z wyjątkiem:
- a. danych, dla których nie wykonuje się kopii zapasowych opisanych w punkcie 3,
 - b. danych, które można łatwo pozyskać z innych (zaufanych i zewnętrznych) źródeł, a których objętość mogłaby być uciążliwa w procesie archiwizacji,
 - c. danych o pomijalnym znaczeniu dla systemu informatycznego **Urzędu**,
 - d. danych z systemów będących w eksploatacji, których archiwizacja nie jest wymagana żadnymi przepisami prawa.
5. W trakcie wykonywania kopii zapasowych i archiwalnych należy weryfikować nośniki, poprzez włączenie w wykorzystywanym oprogramowaniu opcji „weryfikacji” kopii.
6. Administrator Systemów Informatycznych odpowiedzialny jest za funkcjonowanie poszczególnych aplikacji zobowiązany jest do aktualizacji listy danych podlegających backupowi i archiwizacji.
7. Nośniki z kopiami przechowuje się w sposób zapewniający maksymalną ochronę przed uszkodzeniem danych przez czynniki zewnętrzne takie jak zalanie, pożar czy kradzież.
8. Jeżeli kopia zapasowa spełnia wszystkie wymagania stawiane kopii archiwalnej dopuszczalne jest przeniesienie nośnika z kopią zapasową do archiwum i uznanie go za kopię archiwalną. Przeniesienie takie wymaga odnotowania w wykazie nośników archiwalnych i oznaczenia nośnika w sposób przyjęty dla nośników archiwalnych.
9. Kopie archiwalne przechowuje się w lokalizacji innej niż lokalizacja w jakiej znajdują się dane oryginalne.
10. Kopie zapasowe i archiwalne wykonuje się na przenośnych nośnikach wysokiej trwałości lub na urządzeniach zapewniających odpowiednią trwałość i bezpieczeństwo zapisu.

11. Kopie zapasowe wykonywane na tym samym dysku twardym, na którym znajdują się dane nie mogą być uznane za backup służący do ochrony danych (nie dotyczy to urządzeń takich jak macierze dyskowe).
12. Nośniki zawierające kopie zapasowe i archiwalne muszą być chronione przed dostępem osób nieuprawnionych.
13. Nośniki przechowywane w sposób niezgodny z zaleceniami producenta muszą być wyłączone z użycia.
14. Zarówno nośniki jak i sprzęt nie mogą być użytkowane dłużej i do większej ilości kopii niż jest to określone przez producenta.
15. Jakiegokolwiek podejrzenia co do jakości i trwałości nośnika wykluczają jego użycie do czasu dokładnego zweryfikowania podejrzeń.
16. Należy dążyć do eliminacji pojedynczego punktu awarii w zakresie sprzętu wykorzystywanego do wykonywania kopii zapasowych i archiwalnych.

2.2 Czynności do wykonania – kopie zapasowe

Administrator Systemów Informatycznych odpowiedzialny za wykonanie kopii zapasowych ma obowiązek realizować następujące czynności:

1. Zaktualizować listy danych podlegających backupowi, jeżeli zgłoszono mu nowe dane do zabezpieczenia (**załącznik nr 1** do niniejsze Procedury). Listy przechowywane są w oprogramowaniu do wykonania kopii zapasowej.
2. Wybrać nośnik i typ backupu odpowiedni do szczegółowego harmonogramu. Szczegółowy harmonogram zapisany jest w oprogramowaniu wykorzystywanym do wykonania kopii zapasowych.
3. Zapisać w dzienniku kopii zapasowych (**załącznik nr 2** do niniejsze Procedury) identyfikator nośnika, zakres, z czasem wykonania i wersją oprogramowania stosowanego do backupu. Dane te mogą być automatycznie zapisywane w wykorzystywanym oprogramowaniu. Okres przechowywania wpisów w dzienniku wynosi 30 dni od daty wykonania kopii zapasowej.
4. Wykonać kopię zapasową zgodnie z Harmonogramem wykonywania kopii zapasowych (**załącznik nr 1** do niniejszej Procedury).
5. Zweryfikować i zanotować w dzienniku status backupu zgłaszany przez

oprogramowanie. Czynność ta może zostać wykonana automatycznie przez wykorzystywane oprogramowanie. Okres przechowywania wpisów w dzienniku wynosi 30 dni od daty wykonania kopii zapasowej.

2.3 Czynności do wykonania – kopie archiwalne

Administrator Systemów Informatycznych odpowiedzialny za wykonanie kopii archiwalnych ma obowiązek realizować następujące czynności:

1. Zaktualizować listy danych podlegających archiwizacji, jeżeli zgłoszono mu nowe dane do zabezpieczenia (**załącznik nr 1** do niniejsze Procedury). Listy przechowywane są w oprogramowaniu do wykonania kopii archiwalnej.
2. Wybrać nośnik służący do zapisu kopii archiwalnej.
3. Zapisać w dzienniku kopii archiwalnych (**załącznik nr 2** do niniejsze Procedury) identyfikator nośnika, zakres wraz z czasem wykonania, wersją oprogramowania stosowanego do wykonania kopii. Dane te mogą być automatycznie zapisywane w wykorzystywanym oprogramowaniu. Okres przechowywania wpisów w dzienniku wynosi 30 dni od daty wykonania kopii archiwalnej.
4. Wykonać kopię zgodnie z Harmonogramem wykonywania kopii archiwalnych (**załącznik nr 1** do niniejszej Procedury).
5. Zweryfikować i zanotować w dzienniku status operacji zgłaszany przez oprogramowanie. Czynność ta może zostać wykonana automatycznie przez wykorzystywane oprogramowanie. Okres przechowywania wpisów w dzienniku wynosi 30 dni od daty wykonania kopii archiwalnej.
6. Uzupełnić wykaz nośników archiwalnych o nowy nośnik. Wykaz jest prowadzony w formie elektronicznej, plik z wykazem przechowywany jest w systemie obiegu dokumentów.
7. Jeśli to możliwe, zabezpieczyć nośnik przed przypadkowym wykasowaniem informacji.
8. Opisać nośnik w sposób gwarantujący trwałe związanie opisu z nośnikiem. Opis zawierać musi te same dane, które zawiera wpis w wykazie nośników archiwalnych.
9. Przenieść użyte nośniki w miejsce ich przechowywania.

3. Odtwarzanie

3.1. Warunki ogólne

1. Odtworzenie danych może dotyczyć ich dowolnego zakresu.
2. Podczas odtwarzania należy zachować szczególną ostrożność, aby w sposób niezamierzony nie zniszczyć (nadpisać) innych danych przechowywanych na serwerze.
3. Do odtwarzania powinny być użyte nośniki z puli kopii zapasowych. Jeżeli ich zastosowanie nie pozwala osiągnąć zamierzonego celu – użyć można kopii archiwalnych.
4. Jeżeli dane produkcyjne zostały od czasu stworzenia kopii zmodyfikowane, po odtworzeniu kopii zapasowej należy uzupełnić dane odtworzone stosownie do możliwości technicznych i faktycznych potrzeb.

3.2. Czynności do wykonania

Administrator Systemów Informatycznych odpowiedzialny za wykonanie kopii zapasowych w trakcie odtwarzania realizuje następujące czynności:

1. Sprawdzić w dzienniku kopii zapasowych i ewentualnie w dzienniku kopii archiwalnych na którym nośniku znajdują się dane mające zostać odtworzone.
2. Pobrać nośniki z lokalizacji, w której są przechowywane.
3. Wykonać odtworzenie zgodnie z procedurami producenta sprzętu i oprogramowania.
4. Sprawdzić w dzienniku oprogramowania czy odtworzenie danych przebiegło bez błędów. Jeśli wystąpiły błędy należy sprawdzić przyczyny błędu i je usunąć. W razie uszkodzenia nośnika kopii należy odtworzyć dane z innej kopii. Uszkodzony nośnik należy usunąć zgodnie z procedurą.
5. Przenieść odtworzone dane na system produkcyjny.

4. Okresowe badanie nośników służących do przechowywani informacji (kopii archiwalnych/nośników archiwalnych)

4.1. Warunki ogólne

1. Weryfikacja kopii archiwalnych może odbywać się poza środowiskiem produkcyjnym.
2. Weryfikacji podlegają wyrywkowo wybrane nośniki, należy jednak zwrócić uwagę, aby badaniu podlegały kopie archiwalne zapisane na wszystkich rodzajach nośników oraz we wszystkich okresach.
3. Tam, gdzie producent to zaleca, należy wykonać przewinięcie (retencję) taśm i inne prace konserwacyjne w sposób i z częstotliwością określoną przez producenta.
4. O ile to możliwe, kopie niepełnowartościowe powinny być zastępowane identycznymi funkcjonalnie kopiami o jakości nie budzącej zastrzeżeń.
5. Okresowo raz w roku należy przeprowadzić analizę:
 - a. dostępności danych zgromadzonych na nośnikach oraz analizę używanych rozwiązań archiwizacyjnych. W uzasadnionych przypadkach należy zaopatrzyć archiwum w odpowiednie produkty umożliwiające dostęp do danych archiwalnych,
 - b. aktualności kopii archiwalnych, kopie po dacie ważności należy przeznaczyć do likwidacji.

4.2. Czynności do wykonania

Administrator Systemów Informatycznych odpowiedzialny za wykonanie kopii archiwalnych ma obowiązek realizować następujące czynności:

1. Przejrzeć archiwum pod kątem jego stanu zewnętrznego i braków nośników.
2. Wyznaczyć nośniki do weryfikacji bazując między innymi na ich znaczeniu, czasie powstania i czasie ostatniej weryfikacji.
3. Wykonać wyrywkowe próbne odtworzenie, połączone w miarę możliwości ze sprawdzeniem sum kontrolnych.
4. Zanotować wynik weryfikacji, datę, identyfikator nośnika oraz dane

wykonującego w dzienniku weryfikacji.

5. O ile zostały pobrane z archiwum – zwrócić nośniki i dziennik weryfikacji.
6. W sytuacji, w której weryfikacja danych archiwalnych wykazuje, że ich odzyskanie jest niemożliwe, a istnieje inne, równoważne źródło tych danych – archiwum należy uzupełnić korzystając ze źródła równoważnego.

5. Przechowywanie

5.1. Warunki ogólne

1. Kopie przechowywane są w sposób zapewniający maksymalną ochronę przed utratą danych przez czynniki zewnętrzne takie jak zalanie, pożar czy kradzież.
2. Kopie archiwalne powinny być przechowywane w innej lokalizacji niż miejsce przetwarzania danych.
3. Kopie archiwalne muszą być przechowywane co najmniej tak długo, aby możliwe było odtworzenie z nich danych, do przechowywania których **Urząd** jest zobowiązany. Jeżeli kilka kopii archiwalnych zawiera te same wymagane dane lub jeżeli dane z jednej kopii są podzbiorem drugiej – przechowywanie nadmiarowej kopii archiwalnej nie jest wymagane.
4. Okres przechowywania dla kopii archiwalnych danych i systemów będących nadal w użyciu:
 - a. kopie miesięczne – 3 lata
 - b. kopie roczne – 5 lat.
5. Nie należy przechowywać zbędnych kopii danych. Większa liczba kopii zwykle przekłada się na większe trudności z zapanowaniem nad ich stanem, liczbą i lokalizacją, co może prowadzić do ich gorszego zabezpieczenia i narazić na nieuprawniony dostęp.
6. Kopie archiwalne powinny, o ile to możliwe, gwarantować, że zapisane na nich dane nie zostaną w sposób niezauważalny zmodyfikowane.
7. Nośniki z kopiami archiwalnymi powinny być w sposób jednoznaczny oznaczane identyfikatorem. Należy prowadzić wykaz nośników archiwalnych zawierający identyfikatory nośników, datę wykonania kopii oraz opis zawartości.

5.2. Czynności do wykonania

Administrator Systemów Informatycznych odpowiedzialny za wykonanie kopii zapasowych i archiwalnych ma obowiązek realizować następujące czynności:

1. Niezwłocznie po wykonaniu kopii zweryfikować jej poprawność. Weryfikacja poprawności może zostać przeprowadzona automatycznie przez oprogramowanie – wynik weryfikacji jest zapisywany w dzienniku aplikacji.
2. Dla kopii archiwalnych zabezpieczyć nośnik przed modyfikacją. Następnie nadać identyfikator, w wykazie nośników archiwalnych odnotować datę wykonania i zawartość.
3. Przenieść nośnik do lokalizacji przewidzianej do przechowywania kopii.
4. Raz w roku sprawdzić dla których kopii upłynął już termin przechowywania i po zweryfikowaniu, że dana kopia nie jest już potrzebna, przeprowadzić jej likwidację.

6. Likwidacja kopii

Wszelkie zbędne kopie oraz uszkodzone nośniki kopii należy likwidować w sposób uniemożliwiający odzyskanie i odczyt z nich danych. Likwidacja może polegać na zamazaniu danych poprzez zapis innych danych na tym samym nośniku lub na fizycznym zniszczeniu nośnika.

Załącznik 1

Harmonogram wykonywania kopii zapasowych / archiwalnych *) w Urzędzie Gminy Wiśniewo

Lp.	Nazwa systemu informatycznego	Typ bazy danych / program	Lokalizacja	Metody i narzędzia tworzenia kopii zapasowych	Częstotliwość tworzenia kopii zapasowych	Nośniki kopii zapasowych	Miejsce przechowywania kopii zapasowych
1	2	3	4	5	6	7	8

*) wybrać odpowiednie

Załącznik 2

Dziennik kopii zapasowych / archiwalnych ^{*)}
w Urzędzie Gminy Wiśniewo

Lp.	Nazwa systemu informatycznego	Typ bazy danych / program	Identyfikator nośnika (opis nośnika)	Data i godzina	wersją oprogramowania stosowanego do wykonania kopii.	Osoba wykonująca	Podpis osoby wykonującej	Uwagi

^{*)} wybrać odpowiednie

PROCEDURA

„POSTĘPOWANIE W PRZYPADKU WYSTĄPIENIA AWARII SYSTEMU INFORMATYCZNEGO ORAZ ZASADY ICH ZGŁASZANIA”

Spis treści

1.	Cel.....	3
2.	Awarie systemu informatycznego.....	3
3.	Reagowanie na awarie.....	3
4.	Rodzaje awarii.....	5

1. Cel

Procedura postępowania w przypadku wystąpienia awarii systemu informatycznego ma na celu zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych oraz ochroną krytycznych procesów przed rozległymi awariami lub katastrofami.

2. Awaria systemu informatycznego

Awaria systemu informatycznego - nieprawidłowe działanie systemu informatycznego.

3. Reagowanie na awarie

3.1. Warunki ogólne

1. Reakcja na awarie musi minimalizować straty, na jakie narażony jest **Urząd** w wyniku danego zdarzenia.
2. Informowanie o awariach osób nie będących pracownikami **Urzędu** wskazane jest jedynie w sytuacji, gdy wymaga tego uzyskanie wsparcia spoza **Urzędu**.
3. Awarie są usuwane przez Administratora Systemów Informatycznych zgodnie z jego zakresem obowiązków. Administrator Systemów Informatycznych może usuwać awarię poza zakresem jego obowiązków na polecenie Sekretarza **Gminy**.

3.2. Czynności do wykonania

1. Użytkownicy systemu informatycznego zobowiązani są do zgłaszania nietypowych zdarzeń, nieprawidłowej pracy sprzętu za pomocą narzędzi wskazanych przez Sekretarza **Gminy** tj. telefonicznie lub osobiście Administratorowi Systemów Informatycznych. Zgłoszenie telefoniczne/osobiste nie zwalnia użytkownika z obowiązku wypełnienia zgłoszenia elektronicznie po uzyskaniu dostępu do systemu zgłaszania awarii.
2. Administrator Systemów Informatycznych otrzymujący zgłoszenie dokonuje analizy i klasyfikacji awarii według następujących kryteriów:
 - a. jakich elementów systemu dotyczy awaria bezpośrednio, a jakich pośrednio,
 - b. czy awaria jest zagrożeniem dla poufności czy integralności danych,
 - c. jakie dane mogą być zagrożone awarią i kto jest Zarządzającym Zasobem

(ZZ),

- d. czy awaria będzie rozwiązana przez naprawę uszkodzonego elementu, jego wymianę na inny czy przez stworzenie tymczasowych mechanizmów awaryjnych,
 - e. jak poważne będą skutki awarii (szczególnie naruszenie dostępności, integralności i poufności informacji).
3. W przypadku, gdy zgłoszenie dotyczy dostępności, integralności, poufności danych informuje o tym zgłoszeniu Sekretarza **Gminy** lub **IOD** w celu weryfikacji czy nie doszło do incydentu naruszenia bezpieczeństwa informacji. Zgłoszenia dotyczące braku dostępności danych dla pojedynczych użytkowników systemu informatycznego nie podlegają zgłoszeniu Sekretarzowi **Gminy**, są realizowane zgodnie z harmonogramem prac Administratora Systemów Informatycznych.
 4. Dla zgłoszeń będących incydem naruszenia bezpieczeństwa informacji odpowiedzialnym za zgłoszenie tego faktu IOD jest Administrator Systemów Informatycznych.
 5. Jeżeli sytuacja może zagrażać poufności danych, Administrator Systemów Informatycznych odpowiedzialny za obsługę awarii po uzyskaniu akceptacji Sekretarza **Gminy** i **IOD** podejmuje działania mające na celu odcięcie źródła danych od drogi komunikacji, przez którą poufność może być naruszona.
 6. Administrator Systemów Informatycznych wraz z Zarządzającym Zasobem (ZZ) wykonuje analizę skutków awarii, czasu potrzebnego na jej usunięcie i kosztów usunięcia awarii.
 7. Administrator Systemów Informatycznych przedstawia metodę usunięcia awarii, w oparciu o ww. analizę, do akceptacji Sekretarzowi **Gminy**.
 8. W zależności od charakteru awarii, należy wykonać określone działania opisane w poniższym punkcie.
 9. Jeżeli podjęta została decyzja o czasowym wyłączeniu części usług systemu, należy poinformować użytkowników tych usług.
 10. Jeżeli awaria jest powiązana z celowymi działaniami mającymi na celu zaatakowanie **Urzędu**, należy rozważyć poinformowanie Policji.

11. Jeżeli system lub dokumentacja (w szczególności Regulamin Zarządzania Bezpieczeństwem Teleinformatycznym – **załącznik nr 1 do PBI**) wymaga wprowadzenia modyfikacji, należy podjąć działania mające na celu ich przeprowadzenie.

4. Rodzaje awarii

4.1. Awarie oprogramowania

Jeżeli analiza wykaże, że awaria spowodowana jest przez wadliwie działające oprogramowanie, należy podjąć następujące działania:

1. Określić, czy awaria uniemożliwia dalsze korzystanie z oprogramowania i danych:
 - a. jeżeli dalsza praca jest możliwa i nie zagraża kolejnymi awariami – pracownicy powinni powrócić do normalnej pracy;
 - b. jeżeli dalsza praca jest niemożliwa, należy określić czy tworzenie rozwiązania awaryjnego jest uzasadnione i w razie potrzeby – stworzyć je.
2. Określić, czy znane są okoliczności wystąpienia awarii a także (w miarę możliwości) czy są one powtarzalne.
3. Jeżeli okoliczności są powtarzalne i błędu nie można doraźnie wyeliminować, należy poinformować użytkowników aplikacji, że nie powinni wykonywać określonych operacji.
4. Określić, czy istnieją poprawki/nowsze wersje oprogramowania eliminujące zaobserwowaną awarię.
5. Jeżeli poprawki są dostępne, można wdrożyć je, w drodze wyjątku nie poprzedzając wszystkimi działaniami (testami) związanymi z zarządzaniem zmianami. W trakcie aplikowania poprawek, należy zadbać o możliwość przywrócenia pierwotnego stanu, a po przywróceniu sprawności systemu niezwłocznie wykonać wszystkie czynności, których wymaga zarządzanie zmianami.
6. Jeżeli oprogramowanie jest tworzone na zamówienie, należy zgłosić producentowi konieczność stworzenia poprawek, udostępniając potrzebne dane o awarii w sposób minimalizujący ryzyko ujawnienia informacji poufnych.

7. Jeżeli awaria lub proces jej usuwania naruszył integralność danych, należy przywrócić ich poprawny stan.

4.2. Awarie sprzętu

W przypadku, kiedy analiza przyczyn awarii wskaże, że awaria została spowodowana przez sprzęt, należy wykonać następujące działania:

1. Jeżeli uszkodzony sprzęt ma zapewnione mechanizmy redundancji, procesy naprawcze powinny być przeprowadzone jak najszybciej, w sposób najmniej zaburzający pracę **Urzędu**.
2. Jeżeli szybka wymiana uszkodzonego elementu nie jest możliwa – należy rozważyć przeniesienie funkcji uszkodzonego elementu w inne miejsce. Jeżeli przeniesienie funkcji jest możliwe, rozwiązanie takie należy na bieżąco dokumentować. Ponadto, określić należy, na jaki czas planowane jest użycie rozwiązania zastępczego.
3. Jeżeli awaria lub proces jej usuwania naruszył integralność danych, należy przywrócić ich poprawny stan.
4. Jeżeli uszkodzony sprzęt to nośnik danych, to należy go fizycznie zniszczyć **w obecności IOD** lub osoby przez niego upoważnionej. W szczególnych przypadkach, jeśli istnieje konieczność odzyskania danych z uszkodzonego nośnika, możliwe jest przekazanie nośnika do naprawy firmie posiadającej stosowne poświadczenie bezpieczeństwa, po podpisaniu z nią umowy na przekazanie przetwarzania danych znajdujących się na nośniku.

REGULAMIN ZARZĄDZANIA PRACĄ
UŻYTKOWNIKA W SYSTEMACH
TELEINFORMATYCZNYCH

Spis treści

1. Nadawanie uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym wraz z ich rejestracją	3
2. Modyfikacja uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym	4
3. Wycofywanie uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym	5
Załącznik nr 1	6
Załącznik nr 2	7
Załącznik nr 3	8

1. Nadawanie uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym wraz z ich rejestracją

- 1.1 Przetwarzanie danych osobowych w systemie teleinformatycznym może odbywać się wyłącznie przez osoby posiadające pisemne upoważnienie wydane przez Administratora Danych Osobowych.
- 1.2 Nadanie przez Administratora Danych Osobowych upoważnienia do przetwarzania danych osobowych w systemie teleinformatycznym oraz rejestracja użytkownika przetwarzającego dane osobowe w systemie teleinformatycznym następuje na wniosek Sekretarza Gminy.
- 1.3 W celu nadanie uprawnienia do przetwarzania danych osobowych w systemie teleinformatycznym Sekretarz Gminy składa wniosek: **„Wniosek o nadanie uprawnień dla użytkownika w systemie teleinformatycznym”** stanowiący **załącznik nr 1** do niniejszego Regulaminu do Administratora Danych Osobowych o wydanie upoważnienia do przetwarzania danych osobowych w systemie teleinformatycznym.
- 1.4 Wniosek po rozpatrzeniu przez Administratora Danych Osobowych zostaje przekazany do Sekretarza Gminy. Sekretarz Gminy kieruje podpisanym wnioskiem do Administratora Systemów Informatycznych o przydzielenie uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym. Po nadaniu uprawnień Administrator Systemów Informatycznych przekazuje: **„Nadanie uprawnień dla użytkownika w systemie teleinformatycznym”** stanowiący **załącznik nr 1** do niniejszego Regulaminu do Sekretarza Gminy z zachowaniem kopii dla siebie.
- 1.5 Identyfikator (Login) i hasło tymczasowe do systemu teleinformatycznego przetwarzającego dane osobowe jest przydzielany użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych Osobowych.
- 1.6 Identyfikator użytkownika (Login) jest unikalny i niezmienny.
- 1.7 Hasło jest niepowtarzalne i składa się z minimum 8 znaków.
- 1.8 Zmiana hasła odbywa się:
 - a) przy pierwszym uruchomieniu w celu zmiany hasła tymczasowego,
 - b) cyklicznie tj. uwzględniając zalecenia z audytów wewnętrznych,

- c) po wystąpieniu incydentu teleinformatycznego w zakresie poufności / integralności / dostępności danych w obrębie stanowiska komputerowego lub całej infrastruktury IT.
- 1.9 Za przydzielenie i wygenerowanie identyfikatora (Loginu) oraz hasła tymczasowego użytkownikowi, który pierwszy raz będzie korzystał z systemu teleinformatycznego, odpowiada Administrator Systemów Informatycznych. Identyfikator użytkownika (Login) oraz hasło tymczasowe zostaje wpisane do dokumentu: **„Nadania uprawnień dla użytkownika w systemie informatycznym** stanowiącego **załącznik nr 1** do niniejszego Regulaminu.
- 1.10 Inspektor Ochrony Danych w ramach podejmowanych czynności audytowych sprawuje nadzór nad procesem nadawania uprawnień w systemie teleinformatycznym.
- 1.11 Rejestr udzielonych upoważnień określony został w **„Rejestrze upoważnień do systemów informatycznych w Urzędzie Gminy Wiśniewo”** stanowiący **załącznik nr 3** do niniejszego Regulaminu.
- 2. **Modyfikacja uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym**
 - 2.1 Modyfikacja uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym odbywa się na wniosek Sekretarza Gminy w następujących przypadkach:
 - a) modyfikacja uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym z powodu zmiany zakresu czynności.
 - 2.2 Pisemny wniosek o modyfikację uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym składa Sekretarz Gminy do Administratora Danych Osobowych poprzez wniosek: **„Wniosek o modyfikowanie uprawnień dla użytkownika w systemie teleinformatycznym”** stanowiący **załącznik nr 1** do niniejszego Regulaminu. Wniosek po rozpatrzeniu przez Administratora Danych Osobowych zostaje przekazany do Administratora Systemów Informatycznych.
 - 2.3 Po modyfikacji uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym Administrator Systemów Informatycznych przekazuje: **„Modyfikację uprawnień dla użytkownika w systemie**

informatycznym” stanowiący **załącznik nr 1** do niniejszego Regulaminu do Sekretarza Gminy z zachowaniem kopii dla siebie.

2.4 Inspektor Ochrony Danych w ramach podejmowanych czynności audytowych sprawuje nadzór nad procesem modyfikacji uprawnień w systemie teleinformatycznym.

3. Wycofywanie uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym

3.1 Wycofanie uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym może nastąpić na wniosek Sekretarza Gminy w następujących przypadkach:

- a) wycofanie uprawnień użytkownika z powodu zakończenia przetwarzania danych osobowych w obrębie systemu teleinformatycznego,
- b) wycofanie uprawnień użytkownika z powodu ustania stosunku pracy.

3.2 Pisemny wniosek o wycofanie uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym składa Sekretarz Gminy do Administratora Danych Osobowych poprzez wniosek: **„Wniosek o odebranie uprawnień dla użytkownika w systemie teleinformatycznym”** stanowiącego **załącznik nr 2** do niniejszego Regulaminu. Wniosek po rozpatrzeniu przez Administratora zostaje przekazany do Administratora Systemów Informatycznych.

3.3 Po wycofaniu uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym, Administrator Systemów Informatycznych przekazuje: **„Odebranie uprawnień dla użytkownika w systemie informatycznym”** stanowiący **załącznik nr 2** do niniejszego Regulaminu do Sekretarza Gminy z zachowaniem kopii dla siebie.

3.4 Po wycofaniu uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym Administrator Systemów Informatycznych dokonuje zablokowania identyfikatora użytkownika celem uniemożliwienia przydzielenia innemu użytkownikowi.

3.5 Inspektor Ochrony Danych w ramach podejmowanych czynności audytowych sprawuje nadzór nad procesem wycofywania uprawnień w systemie teleinformatycznym.

Załącznik nr 1

**Wniosek o nadanie/ Wniosek o modyfikowanie/Nadanie/Modyfikacja uprawnień
dla użytkownika w systemie informatycznym*)**

Wnoszę o nadanie/ o modyfikowanie/ Przyznaję/ Modyfikuję*) uprawnienia w systemie informatycznym dla Pani/Pana:

(imię i nazwisko)

(stanowisko)

Lp.	Nazwa systemu	Dostęp	Login	Hasło tymczasowe	Użytkownik/ Administrator	Przeglądanie	Wprowadzanie	Modyfikowanie	Usuwanie	Archiwizowanie
		Tak / Nie				Tak / Nie				
1.										
2.										
3.										
4.										
5.										
6.										
7.										
8.										
9.										
10.										

.....
Data i podpis Wnioskującego /Administratora
(ADO) *)

.....
Data i podpis ASI

*) wybrać odpowiednie

Załącznik nr 2

Wniosek o odebranie/ Odebranie uprawnień dla użytkownika w systemie informatycznym*)

Wnoszę o/ Polecam*) wykonanie:

1. odebranie uprawnień w systemie informatycznym w niżej określonym zakresie (*wypełnić odpowiednie*)
2. odebranie wszystkich dotychczas przydzielonych uprawnień w związku z ustaniem zatrudnienia/stażu/praktyki/ zmiany stanowiska pracy z dniem

dla Pani/Pana:

--

(imię i nazwisko)

Lp.	Nazwa systemu	Zablokowanie konta/ Odebranie uprawnień
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		

.....
Data i podpis Wnioskującego /Administratora
(ADO) *)

.....
Data i podpis ASI

*) wybrać odpowiednie

REGULAMIN PRZETWARZANIA I OCHRONY
DANYCH OSOBOWYCH W PRACY ZDALNEJ
w Urzędzie Gminy Wiśniewo

REGULAMIN PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH W PRACY ZDALNEJ

w Urzędzie Gminy Wiśniewo

§ 1.

Pracodawca określając zasady ochrony danych osobowych w ramach pracy zdalnej, kieruje się wytycznymi art. 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, oraz uchylecia dyrektywy 95/46/WE (dalej: RODO), który nakazuje wdrożenie odpowiednich środków technicznych i do ryzyka związanego z przetwarzaniem danych, które mają gwarantować odpowiedni poziom bezpieczeństwa przetwarzania danych, oraz wymogiem § 20 ust. 2 pkt. 8 Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów Teleinformatycznych wskazującym na obowiązek ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

§ 2.

Biorąc pod uwagę specyfikę pracy zdalnej oraz ograniczone możliwości wpływania na warunki organizacyjno – techniczne tego miejsca, Pracodawca przed wydaniem polecenia pracy zdalnej odbiera od Pracownika oświadczenie potwierdzające przygotowanie miejsca wykonywania pracy zdalnej w sposób gwarantujący odpowiednie zabezpieczenie danych osobowych (**Załącznik nr 1**).

§ 3.

Pracownik wykonuje pracę zdalną wyłącznie z wykorzystaniem powierzonego przez pracodawcę sprzętu służbowego. Przekazanie sprzętu następuje w formie protokołu udostępnienia sprzętu informatycznego na czas wykonywania pracy zdalnej wraz z oświadczeniem pracownika. Wzór dokumentu stanowi (**Załącznik nr 2**).

§ 4.

Pracodawca w sytuacjach wyjątkowych, podyktowanych brakiem możliwości zabezpieczenia na potrzeby pracy zdalnej sprzętu informatycznego/mobilnego, może na wniosek pracownika

wyrazić zgodę na wykorzystanie do pracy zdalnej sprzętu prywatnego. Wzór wniosku stanowi (**Załącznik nr 3**).

§ 5.

Pracownik w związku z wykonywaniem pracy zdalnie, zobowiązany jest do przestrzegania polityk, zasad i procedur ochrony danych osobowych obowiązujących u Pracodawcy.

§ 6.

Pracownik wykonując prace zdalnie otrzymuje dostęp do danych osobowych w zakresie niezbędnym do realizacji powierzonych mu obowiązków służbowych. Dostęp do danych osobowych możliwy jest po nadaniu pracownikowi upoważnienia do ich przetwarzania i trwa do momentu ustania wykonywania przez pracownika pracy zdalnej, lub do momentu cofnięcia upoważnienia przez Pracodawcę. Wzór upoważnienia stanowi (**Załącznik nr 4**).

Część integralną upoważnienia stanowi zbiór wytycznych i zasad dotyczących bezpiecznego przetwarzania danych w pracy zdalnej, które to wytyczne Pracownik zobowiązuje się przestrzegać potwierdzając ten fakt stosownym oświadczeniem.

§ 7.

Nie jest dopuszczalne wykorzystywanie danych osobowych przetwarzanych w ramach pracy zdalnej w innym celu niż wykonywanie obowiązków pracowniczych.

§ 8.

Podstawową formą dostępu do danych w związku z wykonywaniem pracy zdalnej, jest forma elektroniczna. Dostęp do danych osobowych przetwarzanych elektronicznie odbywa się w sposób zdalny i następuje poprzez:

- 1) dostęp do skrzynki pocztowej pracownika w domenie pracodawcy,
- 2) dostęp do systemu informatycznego przetwarzającego dane osobowe (w tym:),
- 3) dostęp do określonych zasobów w infrastrukturze IT pracodawcy przy użyciu szyfrowanego połączenia zdalnego VPN. Pracownik zobowiązuje się do zachowania w tajemnicy powierzonych mu danych dostępowych (danych uwierzytelniających) - Załącznik nr 5,
- 4) udostępnienie pracownikowi elektronicznych kopii dokumentów na zaszyfrowanym nośniku służbowym (np. pendrive),

- 5) komunikacja za pomocą komunikatora internetowego (Np. MS Teams, Zoom, Webex),
- 6) korzystanie z usług chmurowych (nazwa usługi np. OneDrive, Dysk Google) w zakresie (zakres zadań).

§ 9.

Komunikacja służbowa odbywa się w sposób zapewniający bezpieczeństwo informacji i danych osobowych, wyłącznie poprzez wskazane przez pracodawcę narzędzia i połączenia zdalne. Przenoszenie służbowych danych na inne urządzenia niż wskazane przez Pracodawcę, w tym prywatne komputery i urządzenia mobilne, bez zgody Pracodawcy jest zabronione.

§ 10

Pracownik zobowiązany jest do zachowania w tajemnicy otrzymanych od pracodawcy danych dostępowych, w tym loginu i hasła oraz zabezpiecza je przed dostępem osób nieuprawnionych, w tym domowników. Zasady dotyczące zmiany hasła, jego budowy i przechowywania określają wewnętrzne procedury obowiązujące u Pracodawcy.

§ 11.

Pracownik korzystając z przydzielonego mu dostępu do danych przetwarzanych elektronicznie jest zobowiązany do pracy w ramach przydzielonego mu konta w systemie informatycznym. Nie jest dopuszczalne udostępnianie konta, loginu, hasła osobom nieuprawnionym, w tym innym pracownikom lub domownikom, ani też korzystanie z konta, loginu, hasła innego pracownika.

§ 12.

Pracownik nie powinien przysyłać plików z danymi osobowymi za pomocą poczty elektronicznej w celu pracy z danymi osobowymi), tj. na potrzeby wykonywania pracy zdalnej, jeżeli możliwy jest dostęp do danych w systemie informatycznym lub za pomocą połączenia zdalnego VPN.

§ 13.

Jeżeli pracownik przesyła załączniki zawierające dane osobowe w wiadomościach mailowych, muszą być one zaszyfrowane odpowiednim programem (np. zip).

Hasło do odszyfrowania załącznika nie może być przesyłane do adresata w treści tej samej wiadomości. Pracownik przekazuje hasło wykorzystując inną formę komunikacji tj. telefonicznie, SMS-em.

Instrukcja szyfrowania załączników do wiadomości mailowych za pomocą programu 7-ZIP, szyfrowania nośników danych za pomocą narzędzia BitLocker, oraz korzystania z przeglądarki internetowej w formie incognito (tryb prywatny) stanowi (**Załącznik nr 6**).

§ 14

Pracodawca jedynie w uzasadnionych przypadkach podyktowanych okolicznościami uniemożliwiającymi dostęp do danych w wersji elektronicznej, wyraża zgodę pracownikowi na wnoszenie dokumentów papierowych.

Aby zminimalizować ryzyko utraty, zniszczenia lub naruszenia integralności dokumentów, pracownik w pierwszej kolejności otrzymuje kopie tych dokumentów.

Wynoszenie przez pracownika kopii dokumentów nie zwalnia go od stosowania tych samych reguł i procedur bezpieczeństwa, co w odniesieniu do dokumentacji oryginalnej.

§ 15.

Pracodawca w sytuacji, w której dokumenty wynoszone będą w oryginale, może wprowadzić obowiązek ewidencjonowania wydanych pracownikowi dokumentów zawierających dane osobowe, w celu kontroli poprawności zwrotu wyniesionej dokumentacji.

Pracownik zobowiązany jest do niezwłocznego zwrotu dokumentów po wykonaniu pracy, do której te dokumenty były mu niezbędne.

§ 16

W przypadku wystąpienia incydentu mogącego naruszyć bezpieczeństwo danych osobowych oraz spowodować ryzyko naruszenia poufności, integralności lub dostępności danych, pracownik zobowiązany jest niezwłocznie, najpóźniej do godziny od ustalenia incydentu zawiadomić o tym fakcie Pracodawcę lub Inspektora Ochrony Danych.

§ 17.

Pracownik ma prawo do wsparcia technicznego ze strony Pracodawcy. Pracownik niezwłocznie zgłasza Pracodawcy lub wyznaczonej przez Pracodawcę osobie realizującej wsparcie techniczne, wszelkie uzasadnione potrzeby w tym zakresie.

W przypadku sprzętu informatycznego/mobilnego zgłoszenie należy przesłać do służb IT.

§ 18.

Pracodawca realizuje wobec pracownika obowiązek informacyjny z art. 13 RODO, informując go o zasadach przetwarzania danych w związku z poleceniem pracy zdalnej, przy pierwszej czynności związanej z decyzją o przejściu pracownika na tryb pracy zdalnej.

§ 19.

Nieprzestrzeganie zasad ochrony danych może być kwalifikowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

§ 20

Przed przystąpieniem do wykonywania pracy zdalnej Pracownik zapoznaje z treścią niniejszego Regulaminu, co potwierdza pisemnym lub elektronicznym oświadczeniem i zobowiązaniem do jego przestrzegania. Wzór oświadczenia stanowi (**Załącznik nr 7**) do niniejszego Regulaminu.

§ 21

W przypadku wykonywania przez pracownika pracy zdalnej z wykorzystaniem sprzętu prywatnego obowiązuje (**Załącznik nr 8**) do niniejszego Regulaminu.

§ 23

W sprawach nieuregulowanych niniejszym Regulaminem zastosowanie mają wewnętrzne procedury obowiązujące u Pracodawcy oraz przepisy z zakresu ochrony danych osobowych oraz z zakresu prawa pracy.

załącznik nr 1
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

Oświadczenie pracownika

Oświadczam, że dysponuję warunkami organizacyjno-technicznymi umożliwiającymi mi prawidłowe zabezpieczenie danych osobowych w miejscu wskazanym do wykonywania pracy zdalnej. Znam i będę stosował(a) zalecenia przetwarzania i ochrony danych osobowych w pracy zdalnej obowiązujące u Pracodawcy, w tym wytyczne i procedury zawarte w *Regulaminie przetwarzania i ochrony danych osobowych w pracy zdalnej w Urzędzie Gminy Wiśniewo*. Jednocześnie informuję, iż otrzymałam(em) do stosowania instrukcję szyfrowania załączników, szyfrowania nośników danych za pomocą narzędzia BitLocker, oraz korzystania z przeglądarki internetowej w formie incognito (tryb prywatny) - INSTRUKCJA ADMINISTRATORA DANYCH i zobowiązuję się do przestrzegania zasad tam zawartych.

.....

Data i podpis pracownika

załącznik nr 2
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

Protokół
udostępnienia sprzętu elektronicznego do celów służbowych

Z dniemudostępniam Pani/Panu
zatrudnionemu na stanowisku
niżej wymieniony sprzęt elektroniczny:

LP	Typ sprzętu	Model	Numer seryjny
1	np. Smartfon		
2	Laptop		

Uwagi: *Wyżej wymieniony sprzęt w dniu przekazania był nowy i w pełni sprawny*

Pracodawca zobowiązuje się dostarczyć wszelkich niezbędnych materiałów eksploatacyjnych dla danego sprzętu, niezbędnych do wykonania, przez pracownika, czynności służbowych.

podpis pracodawcy / osoby
wydającej sprzęt,
upoważnionej przez
pracodawcę

data i podpis pracownika

**Oświadczenie pracownika o odpowiedzialności za używanie służbowego sprzętu
informatycznego / mobilnego w celu wykonywania pracy zdalnej**

1. Pracownik, zwany dalej również Użytkownikiem, oświadcza, że otrzymał sprawny technicznie sprzęt informatyczny/mobilny zgodnie z protokołem przekazania.
2. Komputer posiada zainstalowane oprogramowanie niezbędne do wykonywania czynności służbowych oraz został zabezpieczony przed nieautoryzowanym uruchomieniem (wprowadzony został proces uwierzytelniania dostępu do zasobów komputera).
3. Pracownik zobowiązuje się w okresie obowiązywania polecenia wykonywania pracy zdalnej - używać powierzony sprzęt komputerowy sprzęt mobilny wyłącznie do celów służbowych związanych z wykonywaniem pracy zdalnej, zgodnie z procedurami i regulaminami dotyczącymi zasad użytkowania sprzętu informatycznego wdrożonymi do stosowania u pracodawcy.
4. Pracodawca udostępnia komputer przenośny / sprzęt mobilny w celu umożliwienia wykonywania pracy zdalnej w miejscu wskazanym przez pracownika, przy zachowaniu przez pracownika szczególnej staranności podczas użytkowania i przenoszenia komputera/sprzętu mobilnego. Za bezpieczeństwo komputera/sprzętu mobilnego odpowiada pracownik.
5. Pracownik zobowiązuje się niezwłocznie powiadomić pracodawcę w formie pisemnej lub elektronicznej o:
 - a) zaistnieniu zmiany stanu technicznego komputera/sprzętu mobilnego, uniemożliwiającego jego poprawną eksploatację,
 - b) kradzieży lub zaginięcia komputera/urządzenia mobilnego,
 - c) zaistnieniu innych niż wymienione w punktach a) i b) okoliczności, uniemożliwiających używanie sprzętu do celów służbowych,
 - d) incydencie mogącym naruszyć ochronę przetwarzanych danych osobowych, w tym wystąpienia ryzyka naruszenia poufności, integralności lub dostępności danych.
6. Samowolne otwieranie (demontaż) komputera, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych części/elementów jest zabronione.
7. Pracownik zobowiązuje się do korzystania wyłącznie z oprogramowania już zainstalowanego, udostępnionego przez pracodawcę.
8. Pracownik nie ma prawa kopiować oprogramowania zainstalowanego na

komputerze/urządzeniach mobilnych na swoje własne potrzeby ani na potrzeby osób trzecich.

9. Instalowanie jakiegokolwiek oprogramowania na komputerze/ urządzeniu mobilnym może być dokonane wyłącznie przez osobę upoważnioną.
10. Pracownik ma prawo zapisywania dokumentów elektronicznych wyłącznie na dysku udostępnionego komputera służbowego oraz na dysku komputera w zakładzie pracy udostępnionego zdalnie za pomocą łącza VPN.
11. Pracownik nie ma prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną, odpowiedzialną za konfigurację systemu operacyjnego.
12. W przypadku naruszenia któregoś z powyższych postanowień osoba upoważniona przez pracodawcę ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.
13. Pracodawca lub upoważniony przez niego Informatyk lub inne osoby wyznaczone przez pracodawcę mają prawo monitorować i kontrolować pracę na komputerze, z zachowaniem przepisów prawa i po uprzednim poinformowaniu pracownika.
14. Użytkownik nie ma prawa podłączać komputera służbowego do publicznych sieci Wi-Fi oraz do zewnętrznych ogólnodostępnych innych form pośredniczących w dostępie do Internetu.
15. Pracownik wykonujący prace zdalnie może korzystać z nośników zewnętrznych, w tym dysków USB, pendrive itp., wyłącznie za wiedzą i zgodą Pracodawcy oraz z wykorzystaniem wyłącznie nośników zaszyfrowanych.
16. Pracownik oświadcza, że zobowiązuje się przestrzegać zasad ochrony danych osobowych podczas wykorzystywania udostępnionego sprzętu, w tym zobowiązuje się do:
 - a) dołożenia wszelkich starań przy wykonywaniu powierzonych obowiązków w celu ochrony danych osobowych,
 - b) zachowaniu w tajemnicy loginu i hasła do systemu operacyjnego komputera służbowego oraz do właściwego zabezpieczenia loginu i hasła przed dostępem osób nieuprawnionych,
 - c) przetwarzania danych zgodnie z obowiązującymi w tym zakresie przepisami prawa i regulacjami wewnętrznymi Pracodawcy,
 - d) do zabezpieczenia przetwarzanych danych przed ich:
 - udostępnieniem osobom nieupoważnionym,
 - zabranieniem przez osobę nieuprawnioną,
 - przetwarzaniem z naruszeniem przepisów prawa,

- nieuprawnioną zmianą lub zniszczeniem,
 - utratą,
 - uszkodzeniem,
- e) w przypadku łączenia się zdalnie z komputerem w zakładzie pracy, po zakończeniu pracy pracownik zobowiązany jest zakończyć połączenie VPN (przerwać połączenie) z **Urzędem Gminy Wiśniewo**, wylogować się z komputera, oraz odpowiednio zabezpieczyć komputer deponując w bezpiecznym miejscu.
- f) należytego dbania o powierzony sprzęt, w szczególności o jego sprawność i czystość.
17. Pracownik akceptuje, że niewłaściwe korzystanie z systemów, sieci i zasobów komputerowych może prowadzić do zawieszenia praw dostępu, do postępowania dyscyplinarnego i/lub prawnego.
18. Na polecenie Pracodawcy, wraz z zakończeniem polecenia wykonywania pracy zdalnej - Pracownik zobowiązany jest do zwrotu technicznie sprawnego komputera wraz z wszelkimi danymi służbowymi bez prawa ich skopiowania w jakiegokolwiek formie.

.....
(data i podpis pracownika)

Zwrot udostępnionego sprzętu elektronicznego

Uwagi:

Data zwrotu:

podpis osoby odbierającej
sprzęt,
upoważnionej przez
pracodawcę

Świadoma/świadom odpowiedzialności cywilnej jak i karnej oraz art. 107 ustawy z dn. 10 maja 2018 r. o ochronie danych osobowych oświadczam, iż zdałam/em udostępniony sprzęt elektroniczny i nie jestem w posiadaniu żadnych dokumentów i innych materiałów zawierających informacje poufne, w szczególności dane osobowe, jakie sporządziłam/em, zebrałam/em, opracowałam/em lub otrzymałam/em w czasie wykonywania pracy, włączając w to kopie, odpisy, a także zapisy na innych nośnikach.

data i podpis pracownika

załącznik nr 3
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

Oświadczenie
o wyrażeniu zgody na wykorzystywanie prywatnego sprzętu informatycznego
w celu wykonywania pracy zdalnej

Oświadczam, że posiadam niezbędny sprzęt informatyczny wraz z niezbędnym do pracy zdalnej oprogramowaniem i wyrażam zgodę na bezpłatne jego wykorzystywanie w celu wykonywania pracy zdalnej na rzecz **Urzędu Gminy Wiśniewo, Wiśniewo 86, 06-521 Wiśniewo, tel. 23 655 70 25, email: ugwisniewo@ugwisniewo.pl**

Wykorzystywany przeze mnie do pracy zdalnej sprzęt prywatny umożliwia poszanowanie i ochronę informacji poufnych i innych tajemnic prawnie chronionych, w tym danych osobowych, a także informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

.....
data, podpis pracownika

załącznik nr 4
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

U p o w a ż n i e n i e
do przetwarzania danych w ramach pracy zdalnej

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO), Dz. Urz. UE L z 2016 r. nr 119/1, w związku z przepisami Kodeksu pracy

u p o w a ż n i a m

Panią/Pana

Stanowisko:

do przetwarzania danych osobowych poza siedzibą **Urzędu Gminy Wiśniewo**, w zakresie niezbędnym do wykonywania obowiązków służbowych wynikających z powierzonego Pani/Panu zakresu czynności w ramach pracy zdalnej.

Upoważnienie obejmuje następujący sposób przetwarzania:

[X] - elektronicznie

[] - papierowo

upoważnienie obowiązuje od dnia do (dnia.... / zakończenia wykonywania przez Panią/Pana pracy zdalnej.)

Upoważnienie do przetwarzania danych obejmuje wyłącznie miejsce wykonywania pracy zdanej określone w porozumieniu Pani/Pana z pracodawcą tj. Pani/Pana miejsce zamieszkania, W przypadku wyrażenia przez Pracodawcę zgody na wnoszenie dokumentacji papierowej, upoważnienie obejmuje również możliwość przemieszczania się z dokumentacją papierową z miejsca wykonywania pracy zdalnej do siedziby pracodawcy tj. **Urzędu Gminy Wiśniewo**.

Jednocześnie w związku z wykonywaniem pracy zdalnej zobowiązuję Panią/ Pana do przestrzegania następujących zasad i procedur dotyczących przetwarzania danych osobowych:

- 1) dane zarówno w wersji papierowej jak i elektronicznej należy zabezpieczać przed dostępem osób trzecich. Nie należy udostępniać urządzeń na których wykonywana jest praca zdalna domownikom, współlokatorom lub innym osobom postronnym;
- 2) zabronione jest przemieszczanie się z dokumentacją służbową w inne miejsca, aniżeli miejsce uzgodnione z pracodawcą na potrzeby wykonywania pracy zdalnej tj. miejsce zamieszkania pracownika, z uwzględnieniem drogi dostarczenia dokumentacji z miejsca wykonywania pracy zdalnej do siedziby pracodawcy tj. **Urząd Gminy Wiśniewo** (dostarczenie dokumentacji/odbiór dokumentacji);
- 3) zabronione jest przekazywanie dokumentacji papierowej osobom trzecim, celem jej dostarczenia do zakładu pracy bez wcześniejszego powiadomienia o tym fakcie pracodawcy oraz otrzymania od niego zgody;
- 4) przenosząc (transportując) dokumentację zawierającą dane osobowe pomiędzy zakładem pracy, a miejscem wykonywania pracy zdalnej, należy zastosować odpowiednie środki bezpieczeństwa, polegające w szczególności na przenoszeniu/przewożeniu dokumentów w zamkniętej teczce, i w żadnym wypadku nie wolno pozostawiać dokumentacji bez nadzoru w miejscach publicznych, ogólnodostępnych;
- 5) dokumenty niepotrzebne zawierające dane osobowe należy przechowywać do momentu bezpiecznego zniszczenia w niszczarce – zabrania się ręcznego targania dokumentów i wyrzucania dokumentów służbowych do kosza na śmieci;
- 6) Wymiana danych między zakładem pracy tj. siedzibą pracodawcy, a miejscem wykonywania pracy zdalnej opiera się głównie na komunikacji elektronicznej i wymaga przestrzegania następujących zasad:

a) poczta elektroniczna:

- Komunikacja możliwa jest wyłącznie za pomocą poczty służbowej. Zabronione jest korzystanie z poczty prywatnej w celach służbowych.
- Przesyłając dane osobowe pocztą elektroniczną należy każdorazowo wykorzystywać mechanizmy kryptograficzne (szyfrowanie załączników z danymi).
- W przypadku zabezpieczenia plików (załączników z danymi) hasłem, obowiązuje zasada zastosowania przynajmniej 8 znaków: duże i małe litery

i cyfry lub znaki specjalne a hasło należy przesłać odrębnym kanałem komunikacji np. telefonicznie lub SMS-em.

- Należy zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
- Bez weryfikacji wiarygodności nadawcy, nie należy korzystać z hiperlinków w wiadomościach e-mail.
- Nie należy otwierać załączników (plików) w poczty elektronicznej nawet od znanych nam nadawców bez uważnej weryfikacji tegoż nadawcy.
- Przy korzystaniu z poczty elektronicznej, Pracownik ma obowiązek przestrzegać tajemnicy pracodawcy, prawa własności przemysłowej i prawa autorskiego.

b) zewnętrzne nośniki danych (pendrive, dysk zewnętrzny)

- Dozwolone jest używanie wyłącznie zaszyfrowanych służbowych nośników zewnętrznych dopuszczonych przez Administratora do pracy zdalnej.
- W przypadku kradzieży lub zgubienia służbowego nośnika danych, należy natychmiast powiadomić o tym Pracodawcę lub Inspektora ochrony danych oraz Administratora IT, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.

c) zasady korzystania z komputera służbowego

- Zasady użytkowania sprzętu informatycznego udostępnionego pracownikowi na czas wykonywania pracy zdalnej oraz odpowiedzialność za używanie służbowego sprzętu określone zostały w „Oświadczeniu o odpowiedzialności za używanie służbowego sprzętu informatycznego w celu wykonywania pracy zdalnej”.

Na podstawie niniejszego upoważnienia jest Pan/Pani zobowiązany/a do przetwarzania danych osobowych wyłącznie we wskazanym zakresie oraz zgodnie z przepisami RODO i obowiązującymi u Pracodawcy procedurami oraz polityką ochrony danych. Informuję, jednocześnie, iż podpisane przez Panią/Pana oświadczenie do zachowania w tajemnicy danych osobowych oraz sposób ich zabezpieczenia, obowiązuje nie tylko w stosunku do przetwarzania danych w siedzibie pracodawcy, ale w każdym miejscu wykonywania obowiązków służbowych, również w przypadku wykonywania pracy zdalnej, oraz rozciąga się na okres po ustaniu zatrudnienia.

Wystawił:.....

*(data i podpis Administratora Danych
Osobowych)*

Oświadczenie pracownika

Oświadczam, iż o niniejszym upoważnieniu i jego zakresie zostałem/am poinformowany/a w dniu oraz że rozumiem jego treść i zobowiązuję się do przestrzegania zawartych w nim postanowień i wytycznych oraz postanowień i wytycznych zawartych w Regulaminie.

.....
(data i podpis pracownika)

załącznik nr 5
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

Przyznanie uprawnień do dostępu zdalnego VPN

dla Pani/Pana

.....
.....

stanowisko:

.....
.....

Nadaję Pani/Panu uprawnienia umożliwiające pracę zdalną oraz dostęp do wewnętrznych zasobów Sieci Komputerowej Pracodawcy za pomocą VPN na okres od DD.MM.RRRR do DD.MM.RRRR \ do odwołania.

Identyfikator:.....

Hasło:

.....

Podpis pracodawcy

Oświadczenie

Oświadczam, że zostałem poinformowany o obowiązku zachowania w tajemnicy przyznanych mi danych uwierzytelniających do dostępu do sieci służbowej VPN oraz o odpowiedzialności dyscyplinarnej oraz karnej za naruszenie zapisów niniejszego oświadczenia.

.....

Podpis pracownika

Przyznanie uprawnień do laptopa służbowego na poziomie systemu operacyjnego

dla Pani/Pana

.....
.....

stanowisko:

.....
.....

Nadaję Pani/Panu identyfikator i hasło startowe do systemu operacyjnego komputera udostępnionego na potrzeby wykonywania pracy zdalnej na okres od DD.MM.RRRR do DD.MM.RRRR \ bezterminowo.

Identyfikator:.....

Hasło:

Jednocześnie zobowiązuję Panią/Pana do zmiany hasła przy pierwszej próbie zalogowania się do systemu operacyjnego udostępnionego komputera oraz zachowania hasła w tajemnicy pod rygorem odpowiedzialności

.....

Podpis pracodawcy

Przyjąłem/przyjęłam do wiadomości i stosowania:

.....

Data i Podpis pracownika

załącznik nr 7
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

Oświadczenie pracownika

W związku z powierzeniem mi wykonywania pracy zdalnie na zasadach obowiązujących u Pracodawcy oświadczam, że zapoznałem/zapoznałam się z **Regulaminem przetwarzania i ochrony danych osobowych w pracy zdalnej w Urzędzie Gminy Wiśniewo** i zobowiązuję się do jego przestrzegania i respektowania wszelkich zasad z niego wynikających.

.....

(data i podpis pracownika)

załącznik nr 8
do Regulaminu przetwarzania
i ochrony informacji w pracy zdalnej

**Procedura użytkowania prywatnego sprzętu informatycznego / mobilnego w celu
wykonywania pracy zdalnej**

1. Pracownik (dalej również Użytkownik) oświadcza, że dysponuje sprzętem informatycznym, który dobrowolnie udostępnia pracodawcy na cele wykonywania pracy zdalnej. Sprzęt komputerowy jest sprawny technicznie i jest podłączony do prywatnego Internetu pracownika.
2. Użytkownik na czas udostępnienia komputera prywatnego na potrzeby wykonywania pracy zdalnej nie będzie korzystał z zewnętrznych form pośredniczących w dostępie do Internetu, w tym z zewnętrznych publicznych sieci Wi-Fi.
3. Pracownik oświadcza, że komputer posiada zainstalowane oprogramowanie antywirusowe
4. Pracownik w godzinach pracy tj od do zobowiązuje się używać komputera prywatnego wyłącznie do wykonywania zadań służbowych w formie pracy zdalnej.
5. Praca zdalna na komputerze prywatnym pracownika polega na połączeniu się z miejsca wykonywania pracy zdalnej – z poziomu komputera prywatnego pracownika, poprzez funkcję pulpitu zdalnego z komputerem służbowym w zakładzie pracy.
6. Pracownik w celu połączenia się za pomocą pulpitu zdalnego z komputerem służbowym w pracy musi przeprowadzić proces uwierzytelniania (zalogowania się) zgodnie z nadanymi uprawnieniami do nawiązania bezpiecznego połączenia tunelowego VPN.
7. Pracownik zobowiązuje się w okresie obowiązywania polecenia wykonywania pracy zdalnej - w godzinach wykonywania obowiązków służbowych na komputerze prywatnym zabezpieczyć sprzęt przed dostępem osób trzecich, w tym domowników/współlokatorów.
8. Pracownik zobowiązany jest kategorycznie przestrzegać wprowadzonych zasad komunikacji zdalnej umożliwiającej mu połączenie się zdalne ze stanowiskiem komputerowym w zakładzie pracy i wykonywaniem zadań służbowych, w szczególności poprzez:
 - a) łączenie się za pomocą pulpitu zdalnego wyłącznie na czas wykonywania pracy zdalnej,
 - b) po zakończeniu pracy za pomocą pulpitu zdalnego lub odejściu od stanowiska pracy

- na dłużej, bez możliwości monitorowania stanu uruchomionego komputera pracownik zobowiązany jest przerwać połączenie zdalne, wylosowując się bezpiecznie z funkcji zdalnego dostępu do komputera w zakładzie pracy.
9. Przetwarzanie informacji służbowych, w tym szczególnie danych osobowych za pomocą komputera prywatnego wymaga przestrzegania przez pracownika zasad i procedur obowiązujących u pracodawcy, a dotyczących bezpiecznego przetwarzania danych w formie elektronicznej.
 10. Pracownik zobowiązuje się niezwłocznie powiadomić pracodawcę w formie pisemnej lub elektronicznej o:
 - a) zaistnieniu zmiany stanu technicznego komputera prywatnego, uniemożliwiającego jego eksploatację,
 - b) zaistnieniu innych niż wymienione w punkcie a) okoliczności, uniemożliwiających używanie komputera prywatnego do celów służbowych.
 19. Użytkownik ma prawo zapisywania dokumentów elektronicznych wyłącznie na udostępnionym zdalnie za pomocą łącza VPN komputerze w zakładzie pracy lub służbowym nośniku zewnętrznym (np. pendrive).
 20. Użytkownik oświadcza, że zobowiązuje się przestrzegać zasad ochrony danych na komputerze podczas wykonywania obowiązków służbowych, w tym zobowiązuje się do:
 - a) dołożenia wszelkich starań przy wykonywaniu powierzonych obowiązków w celu ochrony danych osobowych,
 - b) zachowaniu w tajemnicy loginu i hasła do łączenia się z zakładem pracy,
 - c) przetwarzania danych zgodnie z obowiązującymi w tym zakresie przepisami prawa i regulacjami wewnętrznymi Pracodawcy,
 - d) do zabezpieczenia przetwarzanych danych przed ich:
 - udostępnieniem osobom nieupoważnionym,
 - zabránieniem przez osobę nieuprawnioną,
 - przetwarzaniem z naruszeniem przepisów prawa,
 - nieuprawnioną zmianą lub zniszczeniem,
 - utratą,
 - uszkodzeniem,
 - e) do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia.
 21. Nieprzestrzeganie przez pracownika zapisów niniejszego regulaminu, będzie stanowić

naruszenie obowiązków pracowniczych wynikających z Kodeksu pracy.

Oświadczam, że zapoznałem się z procedurą użytkowania prywatnego sprzętu informatycznego w celu wykonywania pracy zdalnej i zobowiązuję się do stosowania zapisów w niej zawartych.

.....
(data i podpis pracownika)

Klauzula informacyjna dla pracownika wykonującego pracę zdalną

1. Administratorem Pani/Pana danych osobowych jest **Gmina Wiśniewo, Wiśniewo 86, 06-521 Wiśniewo, tel. 23 655 70 25 e-mail: ugwisniewo@ugwisniewo.pl**, dalej: Administrator.
2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można skontaktować się za pośrednictwem następujących danych kontaktowych: **e-mail:**
3. Pani/Pana dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej RODO, w związku z przepisami ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy i przepisami wykonawczymi w celu wypełnienia obowiązku administratora w zakresie realizacji praw i obowiązków pracodawcy wynikających z Kodeksu pracy, w tym w zakresie umożliwienia pracownikowi wykonywania pracy zdalnej, jej ewidencji i kontroli. W przypadku wykonywania pracy zdalnej na podstawie wniosku pracownika posiadającego orzeczenie o niepełnosprawności albo orzeczenie o znacznym stopniu niepełnosprawności albo pracownika sprawującego opiekę nad innym członkiem najbliższej rodziny lub inną osobą pozostającą we wspólnym gospodarstwie domowym posiadającym takie orzeczenie, dane osobowe będą przetwarzane na podstawie art. 9 ust. 2 lit. b) RODO.
4. Podane przez Panią/Pana dane osobowe będą udostępniane wyłącznie podmiotom uprawnionym do ich przetwarzania na podstawie przepisów prawa. Dane osobowe będą udostępnione podmiotom zapewniającym, na podstawie umów zawartych przez administratora, obsługę działalności administratora (np. dostawcy usług informatycznych, poczty elektronicznej, systemów kadrowych, systemów monitorowania i ewidencji czasu pracy).
/w tym punkcie można także doprecyzować odbiorców danych osobowych, jeżeli dane udostępniane są jeszcze innym podmiotom/
5. Dane osobowe będą przechowywane przez czas trwania stosunku pracy (np. w zakresie związanym z komunikacją służbową) albo przez czas trwania stosunku pracy i niezbędnej archiwizacji (w odniesieniu do danych osobowych niezbędnych do wypełnienia obowiązków pracodawcy, ewidencji czasu pracy zdalnej, kontroli pracy zdalnej).

6. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia w przypadkach przewidzianych przepisami prawa oraz ograniczenia przetwarzania.
7. Posiada Pani/Pan prawo wniesienia skargi do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych, jeżeli uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.
8. Podanie danych osobowych jest dobrowolne, ale niezbędne do weryfikacji gotowości do świadczenia pracy zdalnej, wniosku o świadczenie pracy zdalnej a następnie zawarcia umowy dotyczącej wykonywania pracy zdalnej. Niepodanie danych osobowych oznacza brak możliwości zawarcia i wykonywania umowy.
9. Dane osobowe nie będą podlegały profilowaniu, na podstawie tych danych, nie będą podejmowane decyzje w sposób zautomatyzowany.

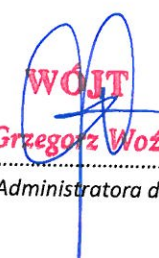
Załącznik 6

do Regulaminu przetwarzania i
ochrony danych osobowych w pracy
zdalnej

**ZASADY BEZPIECZEŃSTWA PRZETWARZANIA DANYCH DLA UŻYTKOWNIKÓW
SYSTEMÓW INFORMATYCZNYCH**

PORADNIK ADMINISTRATORA DANYCH

.....
Pieczęć firmowa


WÓJT
mgr Grzegorz Woźniak
.....
podpis Administratora danych

INSTRUKCJE

1. SZYFROWANIE POSZCZEGÓLNYCH PLIKÓW I FOLDERÓW

Instrukcja nr 1 - Instrukcja instalacji oraz używania programu 7-zip

2. SZYFROWANIE I UŻYTKOWANIE PENDRIVE'ÓW

Instrukcja nr 2 – Instrukcja szyfrowania pendrive'ów narzędziem BitLocker

3. BEZPIECZNE KORZYSTANIE Z PRZEGLĄDARKI INTERNETOWEJ

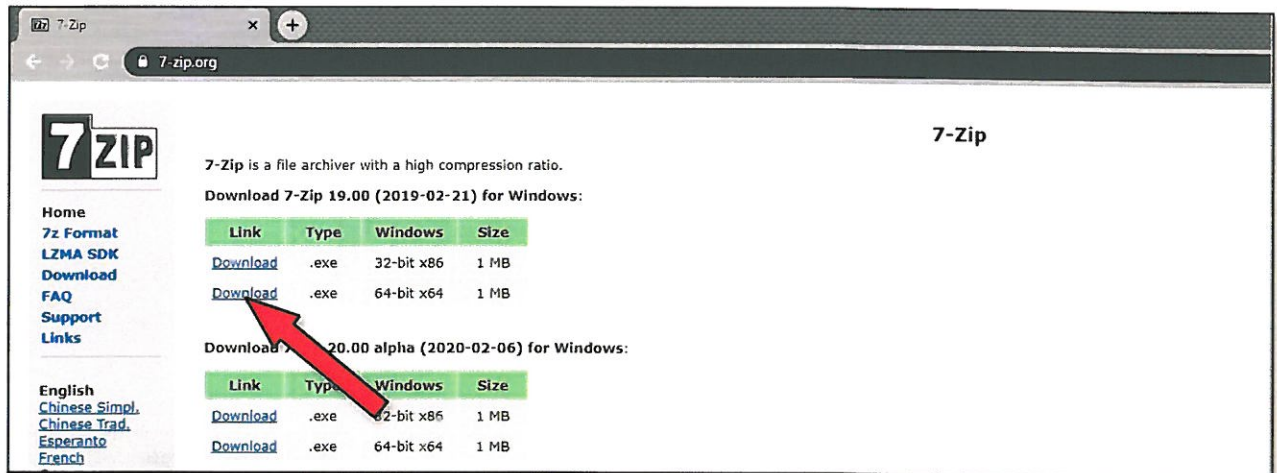
Instrukcja nr 3 – Instrukcja bezpiecznego korzystania z przeglądarki internetowej

SZYFROWANIE POSZCZEGÓLNYCH PLIKÓW I FOLDERÓW (Instrukcja użytkowania oprogramowania)

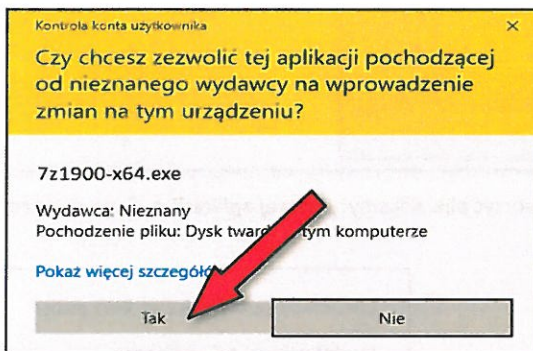
NAZWA OPROGRAMOWANIA:	7-ZIP
ZAKRES INSTRUKCJI:	Instalacja, konfiguracja oraz szyfrowanie danych (plików i folderów)

ETAP I: INSTALACJA

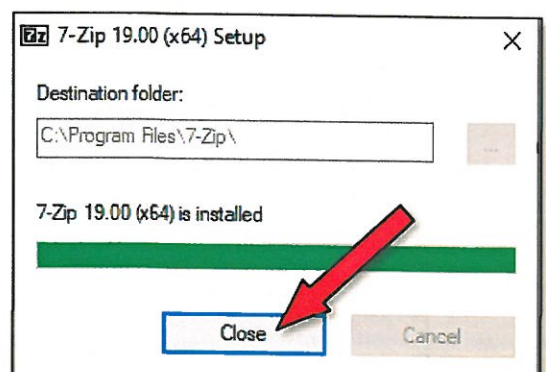
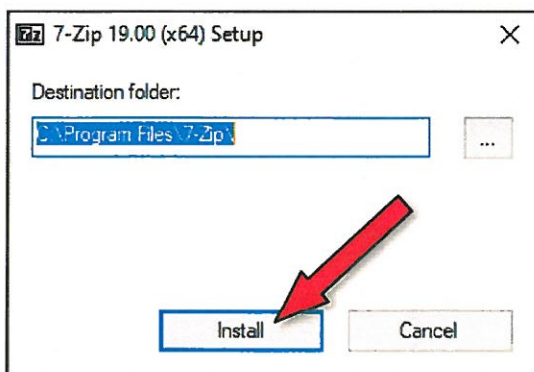
1. Otwórz przeglądarkę internetową (Chrome, Firefox, Edge itp.), następnie w pasku adresu wpisz: „7-zip.org” oraz naciśnij „ENTER”. Otworzy się następująca strona internetowa:



2. Aby pobrać program, kliknij „Download” dla wersji 64-bit x64. Jest to wersja programu 7-zip dla systemu operacyjnego Windows 7, 8, 8.1, 10 w wersji 64 bitowej (bardzo rzadko spotyka się już systemy Windows wersji 32 bitowej z uwagi na przestarzałą technologię).
3. Następnie uruchom program. W przeglądarce Chrome znajdziemy skrót do programu w dolnym lewym rogu. W innych przeglądarkach zazwyczaj pobrane programy znajdują się w katalogu: „Pobrane”. Po uruchomieniu programu może się pojawić komunikat i klikamy „Tak”:



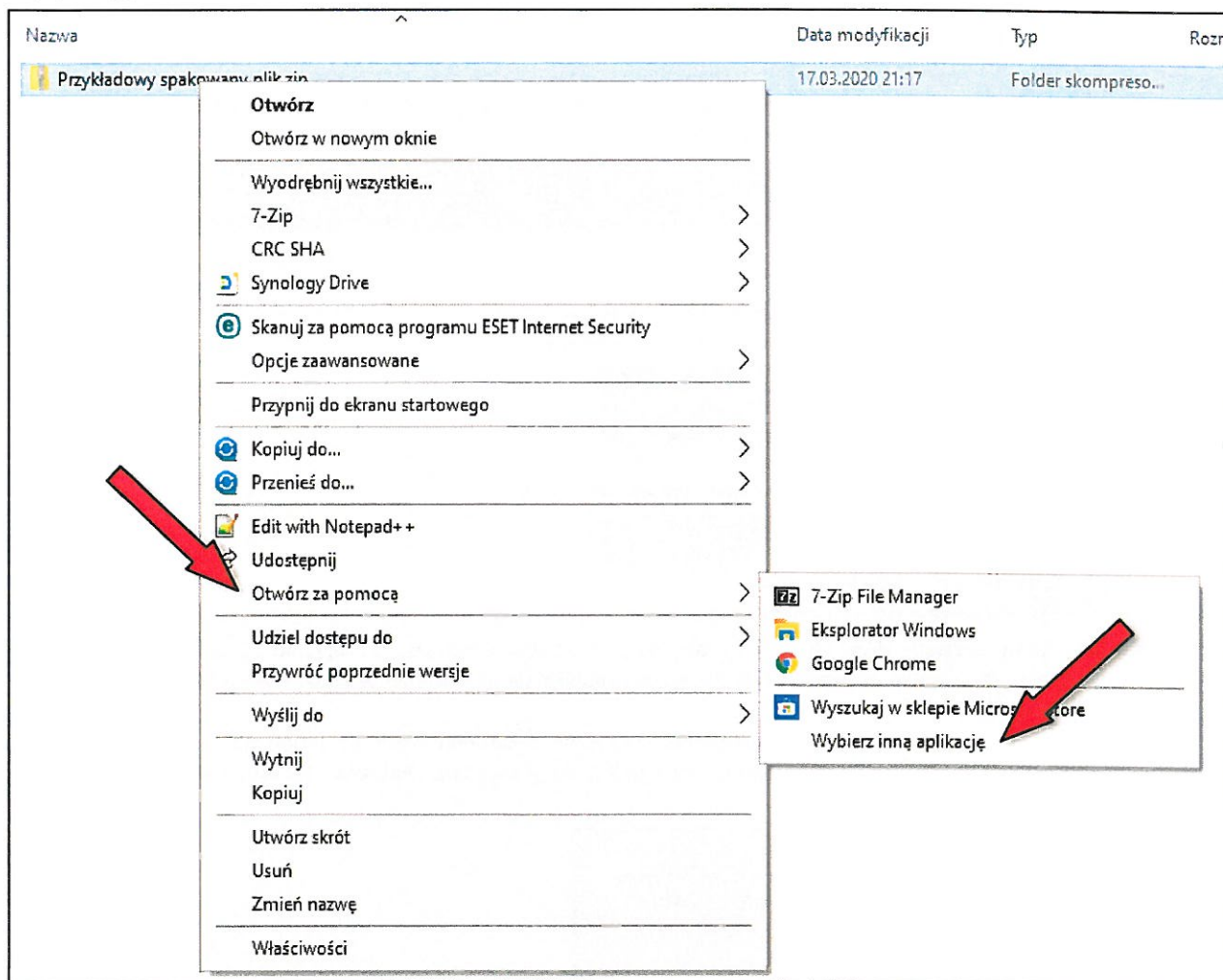
4. Następnie pojawi się okno w którym wskazujemy miejsce zainstalowania programu. Nie trzeba nic zmieniać. Klikamy tylko „Install”, a po zainstalowaniu programu „Close”:



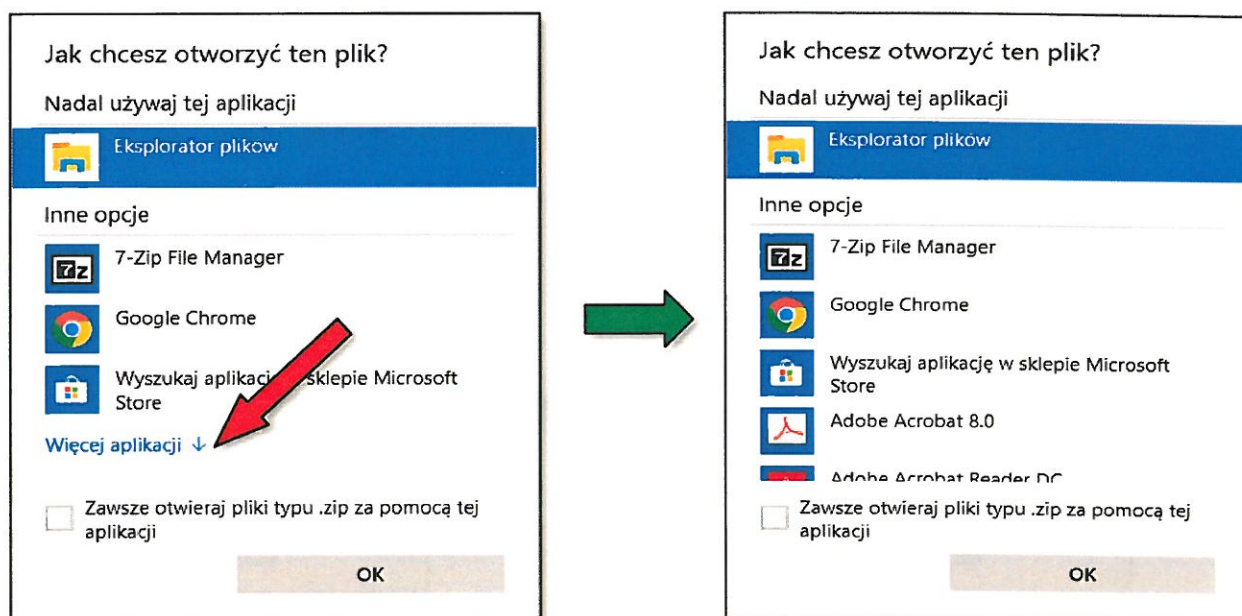
5. Od teraz masz zainstalowany program kompresujący pliki o nazwie 7-zip.

ETAP II: KONFIGURACJA

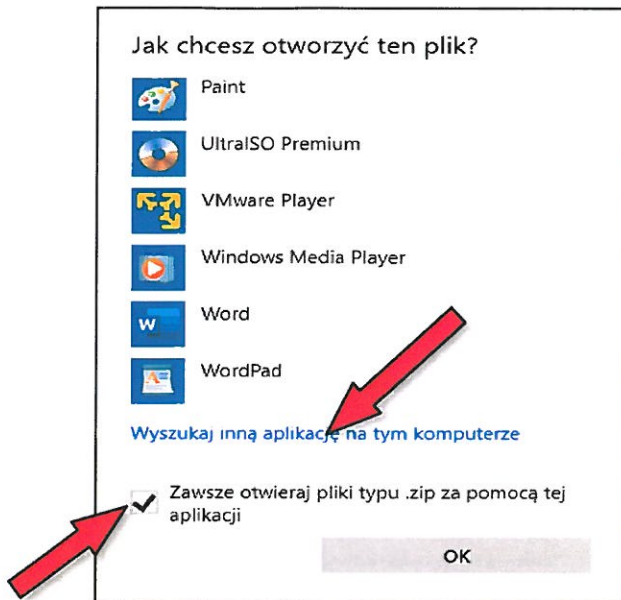
1. Czasami system operacyjny Windows pomimo instalacji programu 7-zip otwiera pliki skompresowane „spakowane” poprzez swoje zaimplementowane narzędzie do archiwów. Stwarza to częste problemy w przypadku „zahasłowanych” archiwów. Warto to zmienić. Aby to wykonać:
2. Znajdź na swoim komputerze jakikolwiek „skompresowany „spakowany” plik z rozszerzeniem *.zip.
3. Kliknij go prawym przyciskiem myszy → rozwinie się podręczne menu, w którym klikamy po kolei: „Otwórz za pomocą” → „Wybierz inną aplikację”:



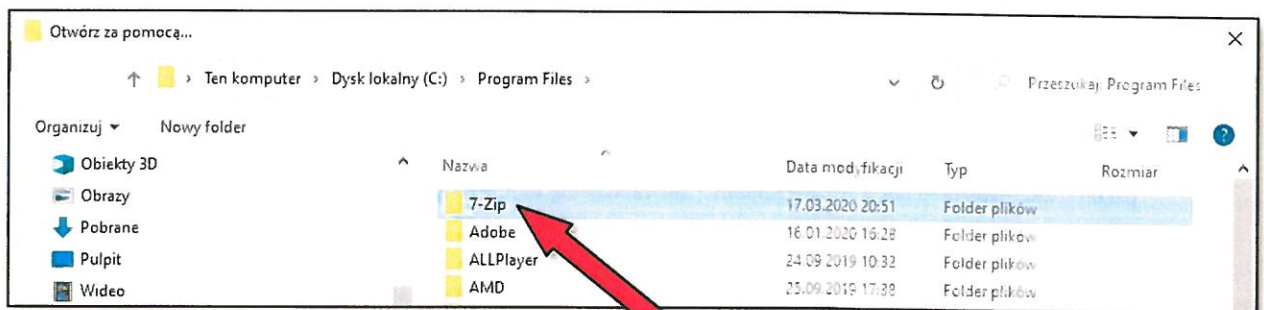
4. Otworzy się okno, w którym określasz w jaki sposób chcesz otworzyć plik. Klikamy: „Więcej aplikacji”, po czym rozwinie się lista z większą ilością programów:



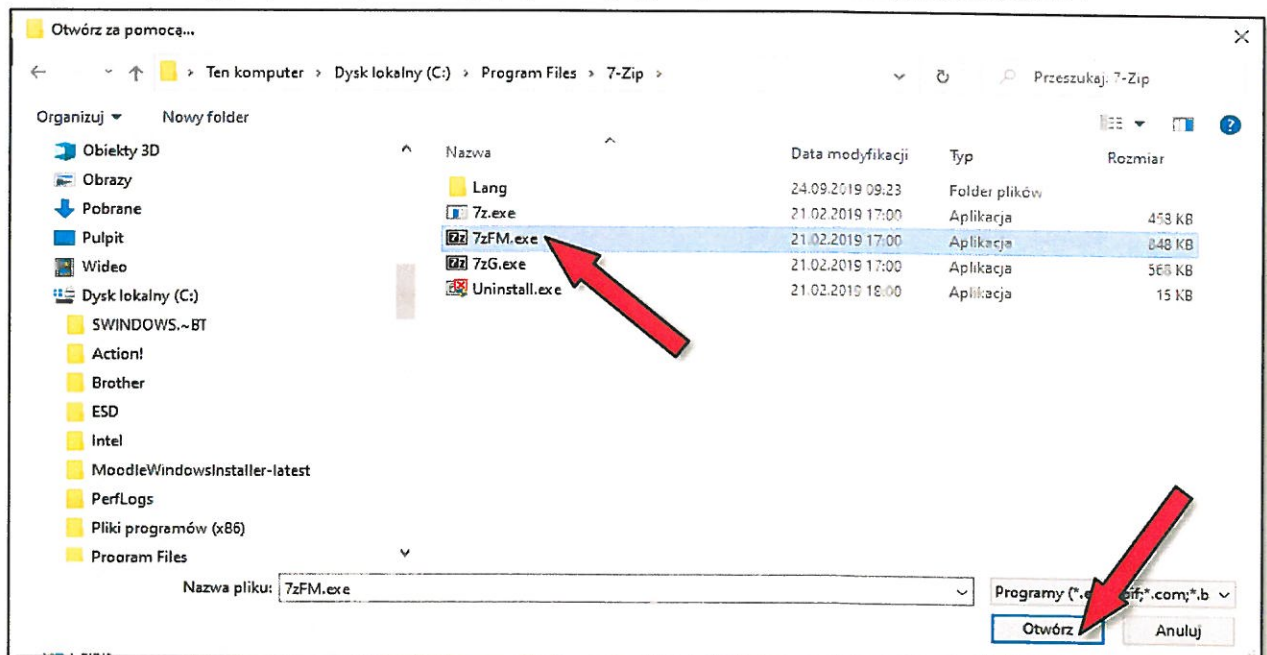
5. Następnie przewiń listę na sam dół, zaznacz „✓” checkbox „Zawsze otwieraj pliki typu .zip za pomocą tej aplikacji” oraz kliknij „Wyszukaj inną aplikację na tym komputerze”.



6. Teraz otworzy się okno, w którym wskazujemy folder zawierający program 7-zip. W każdej wersji Windowsa (czy to 7, 8, 8.1 bądź 10) może być inaczej. Niniejsza instrukcja opiera się o system operacyjny Windows 10, gdzie folder z programem ma następującą ścieżkę: „/Ten komputer/Dysk lokalny (C:)/Program files/7-Zip/” lub w nomenklaturze informatycznej: „C:\Program Files\7-Zip”. A więc klikamy dwa razy lewym przyciskiem myszy (aby otworzyć) folder „7-Zip”:



7. Następnie zaznaczamy jednym kliknięciem lewego przycisku myszy plik: „7zFM.exe” i klikamy przycisk „Otwórz”:

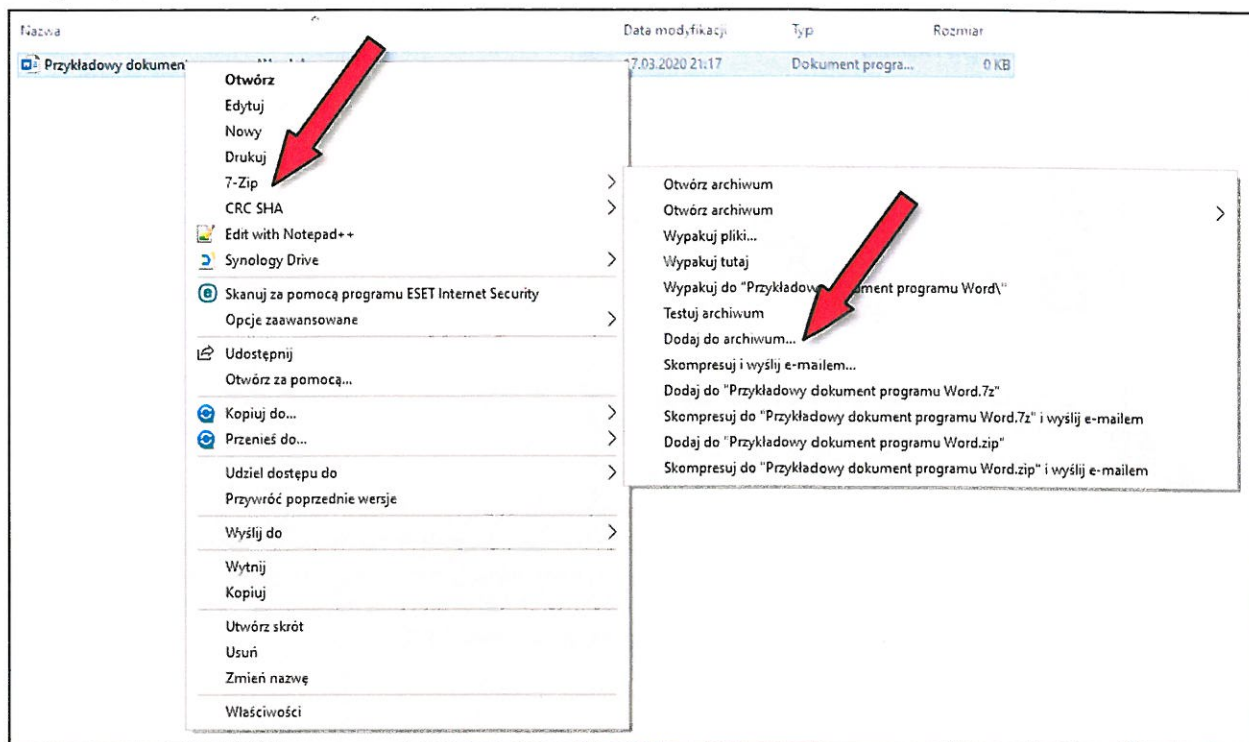


8. Od teraz każdy plik (archiwum) w formacie *.zip będzie otwierane przez program 7-Zip, co umożliwi bezproblemowe otwieranie „zahasłowanych” plików.

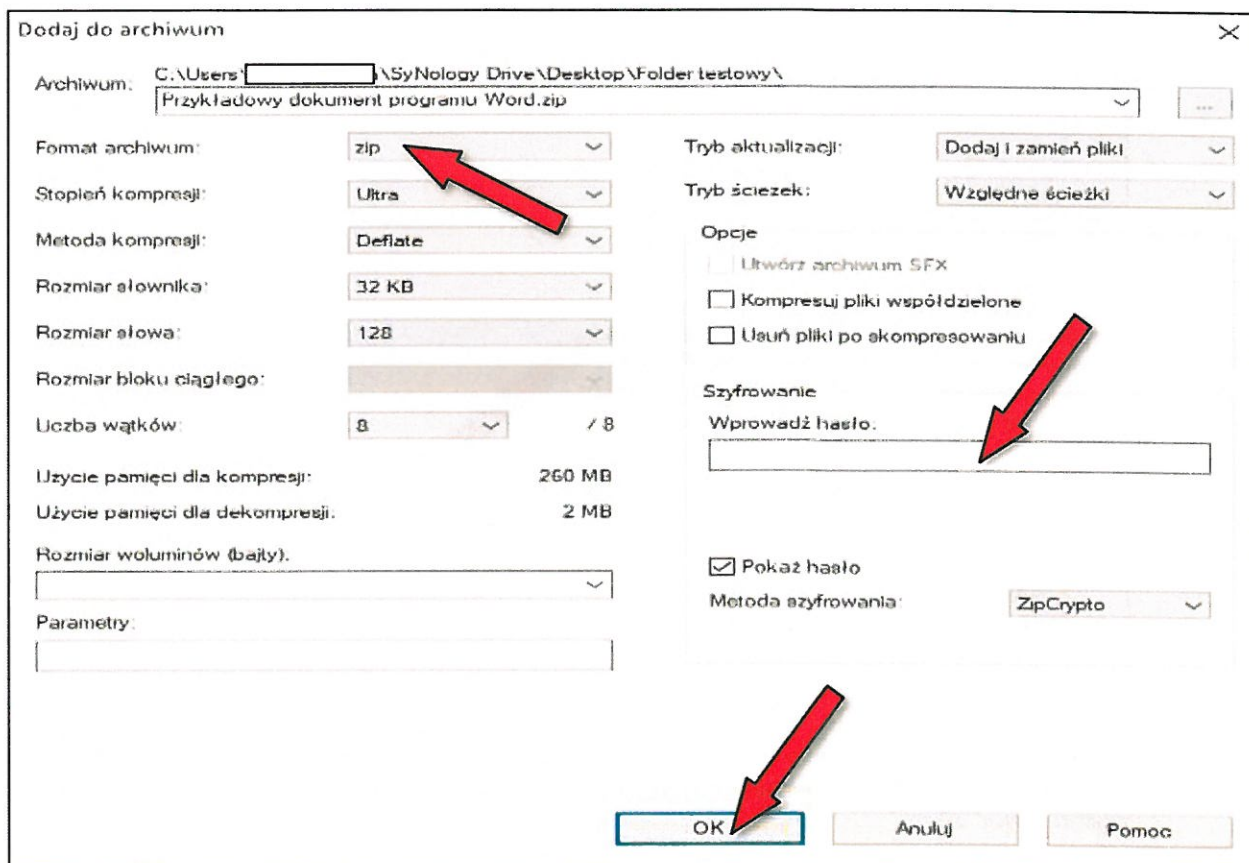
ETAP III: SZYFROWANIE DANYCH (PLIKÓW I FOLDERÓW)

Chcąc zaszyfrować plik lub cały folder, musisz wykonać następujące czynności:

1. Kliknij prawym przyciskiem myszy na wybrany plik⁽¹⁾ lub folder⁽²⁾. Następnie kliknij w menu „7-Zip” oraz „Dodaj do archiwum...”:



2. Teraz otworzy się okno konfiguracji kompresji i szyfrowania dla wybranego przez Ciebie pliku(ów) lub folderu(ów). Warto ustawić format archiwum na „ZIP”. W przyszłości automatycznie każda czynności kompresji i szyfrowania będzie zapamiętana dla tego ustawienia. Oczywiście w polu „Wprowadź hasło” wpisujemy je. Następnie klikamy „OK”. Po skompresowaniu („spakowaniu”) pliku(ów) lub folderu(ów) plik z rozszerzeniem *.zip zapisze się w macierzystym katalogu, w którym były źródłowe dane. Wszystko gotowe :



SZYFROWANIE I UŻYTKOWANIE PENDRIVE'ÓW (Instrukcja użytkowania oprogramowania)

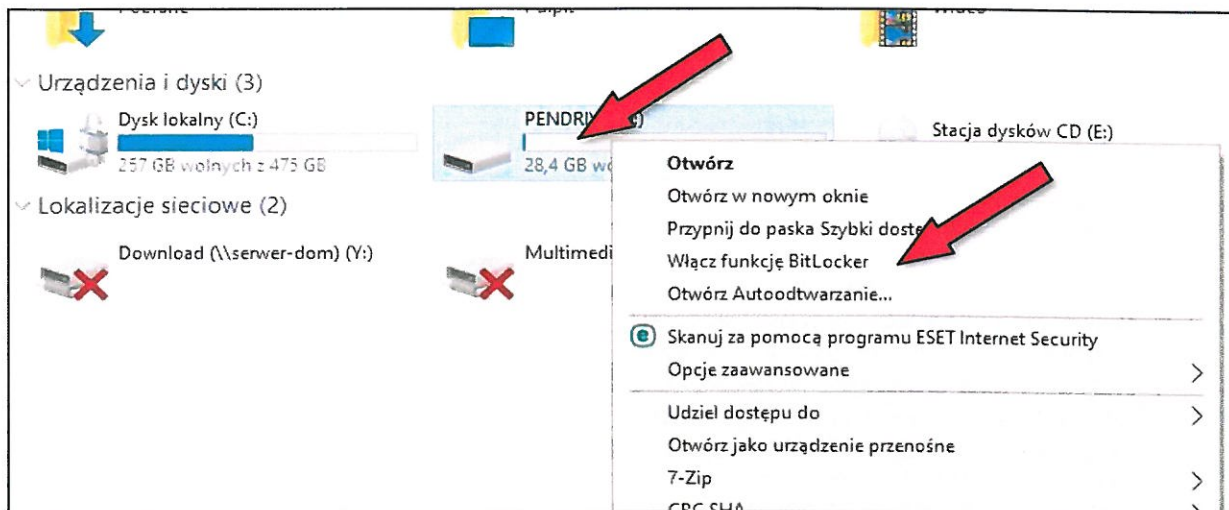
NAZWA OPROGRAMOWANIA:	<i>BitLocker</i>
ZAKRES INSTRUKCJI:	<i>Warunki techniczne, proces pierwszego szyfrowania, użytkowanie zaszyfrowanego pendrive'a, odzyskiwanie pendrive'a poprzez „klucz odzyskiwania”.</i>

ETAP I: WARUNKI TECHNICZNE

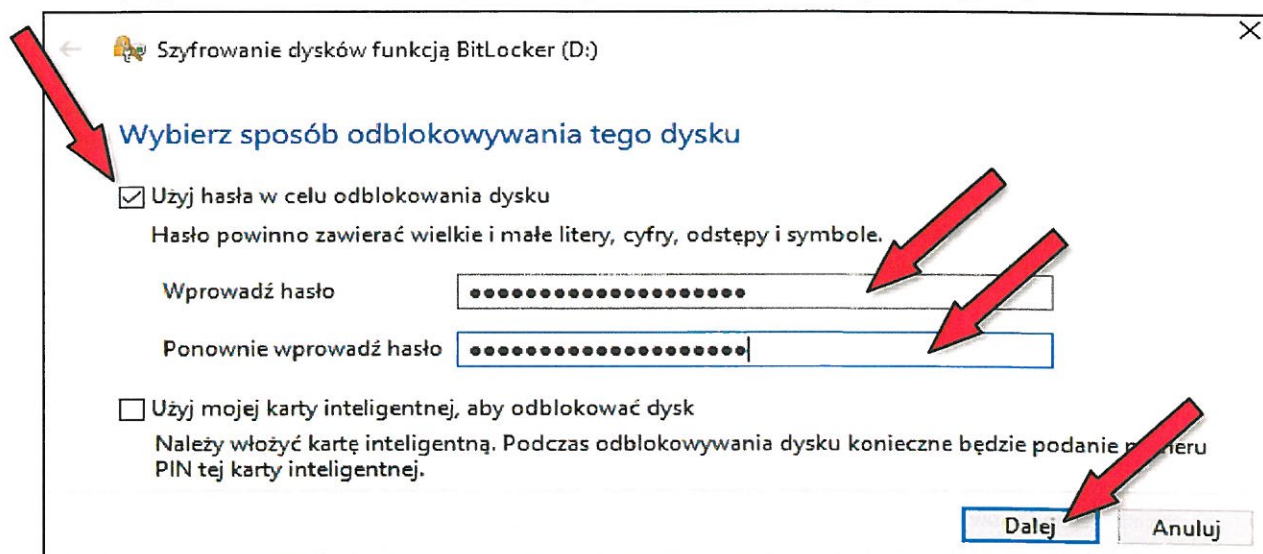
- Chcąc korzystać z szyfrowania urządzeń zewnętrznych (np. pendrive'ów) na rynku IT jest wiele dostępnych narzędzi płatnych oraz bezpłatnych. Warto zauważyć, że większość z nich wymaga specjalistycznego oprogramowania oraz aby umożliwić odczyt zaszyfrowanego urządzenia na każdym komputerze → wymaga się zainstalowanego „agenta” lub innej formy dostępu do danych (w tym też dodatkowych plików „rozruchowych” na pendrive'ie). Jest to uciążliwe i w praktyce nie zawsze zapewniające w 100% bezpieczeństwo (choćby z uwagi na częste praktyki dzielenia przestrzeni pamięci pendrive'a na zaszyfrowaną i niezaszyfrowaną, co skłania użytkowników do częstego zapisu w tej części niezaszyfrowanej). Obecne techniki szyfrowania opierają się algorytmu szyfrowania typu AES-256, które gwarantują bardzo wysoki poziom bezpieczeństwa.
- Zalecaną formą szyfrowania jest wbudowana funkcja BitLocker w system operacyjny Microsoft Windows, jednakże tylko niektóre wersje potrafią szyfrować przy czym każda obsługuje (odczyt i zapis) zaszyfrowany pendrive (oczywiście są wyjątki, ale mowa tu o bardzo przestarzałych wersjach sprzed parunastu lat).
- Systemy operacyjne Microsoft Windows, które mają wbudowaną funkcję szyfrowania urządzeń zewnętrznych to:
 - Windows 7 Ultimate oraz Enterprise,
 - Windows 8 Pro oraz Enterprise,
 - Windows 10 Pro Enterprise oraz Education
 - Windows 11 Pro Enterprise oraz Education.
- Jeżeli posiadamy chociażby jeden komputer z system operacyjnym spośród wyżej wymienionych, możemy zaszyfrować wszelkie pendrive i będą one działały na wszystkich systemach operacyjnych Microsoft Windows w tym na wersjach „Home”, które niestety dość często są używane w sektorze publicznym i niepublicznym z uwagi na koszt zakupu wraz z nowym sprzętem (warto zauważyć, iż podczas zakupu sprzętu poleasingowego, zjawisko to właściwie nie występuje).
- Warto rozważyć 2 scenariusze:
 - zakup pendrive'ów oraz ich zaszyfrowanie (proces ten nie musi się nawet odbyć na sprzęcie organizacji → oczywiście z zachowaniem najwyższej staranności w zakresie bezpieczeństwa informacji). Na obecną chwilę, ceny rynkowe pendrive'ów są bardzo niskie. Wystarczająca pojemność oscyluje w granicach od 2 do 4 GB pamięci.
 - wypracowanie z pracownikami organizacji wspólnego stanowiska co do zaszyfrowania ich prywatnego pendrive'a, co nie ograniczy swobody i prywatności pracownika (nadal ma pełny dostęp do danych), a wręcz polepszy ich prywatne bezpieczeństwo.
- Urządzenie (pendrive) zaszyfrowane ww. metodą jest nadal w pełni funkcjonalne, sam proces szyfrowania jest bardzo krótki (parę minut), a dodatkowo podłączanie do komputera ogranicza się do włożenia urządzenia do portu USB, oraz wpisania hasła w wyskakującym okienku. Po wyciągnięciu urządzenia, pendrive jest w 100% zaszyfrowany, co uchroni organizację przez utratą poufności danych.

ETAP II: PROCES PIERWSZEGO SZYFROWANIA

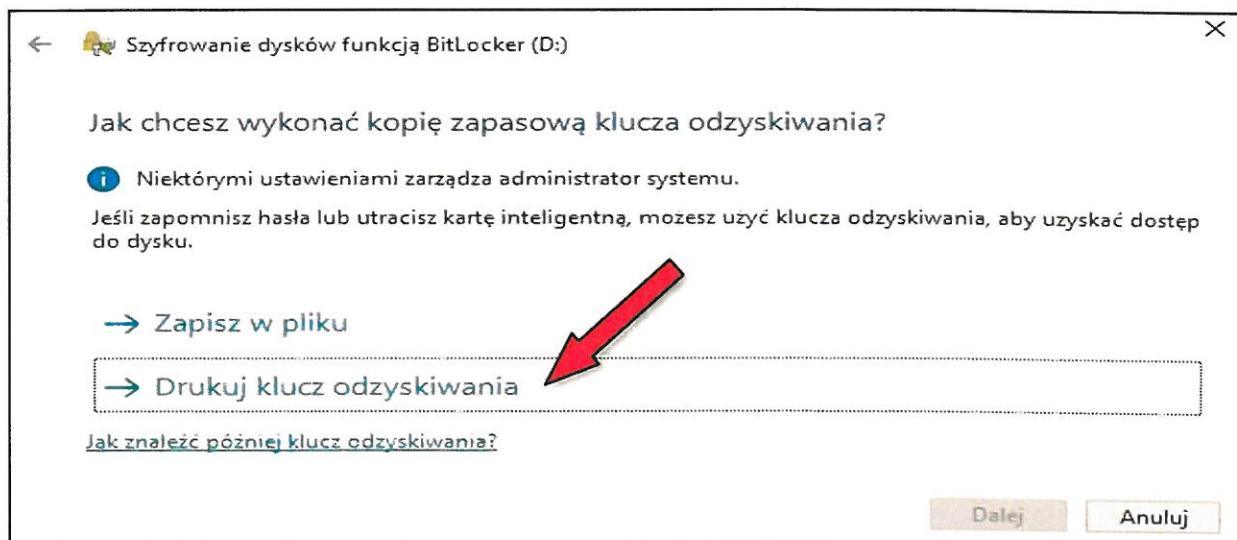
1. Włóż pendrive do jakiegokolwiek portu USB w komputerze z zainstalowanym systemem operacyjnym wymienionym w punkcie I-3.
2. Wejdź do „Eksplorator plików” oraz klikając prawym przyciskiem myszy na ikonę pendrive’a który chcemy zaszyfrować rozwiń podręczne menu. Następnie kliknij „Włącz funkcję BitLocker”:



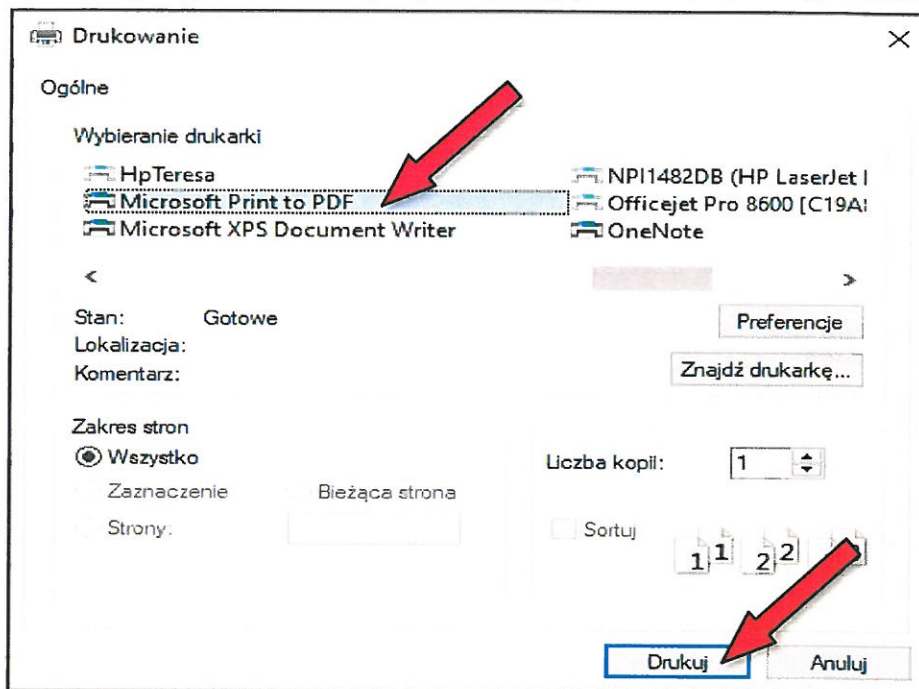
3. Zaznacz: „Użyj hasła w celu odblokowania dysku” oraz wpisz dwukrotnie hasło. Następnie kliknij „Dalej”.



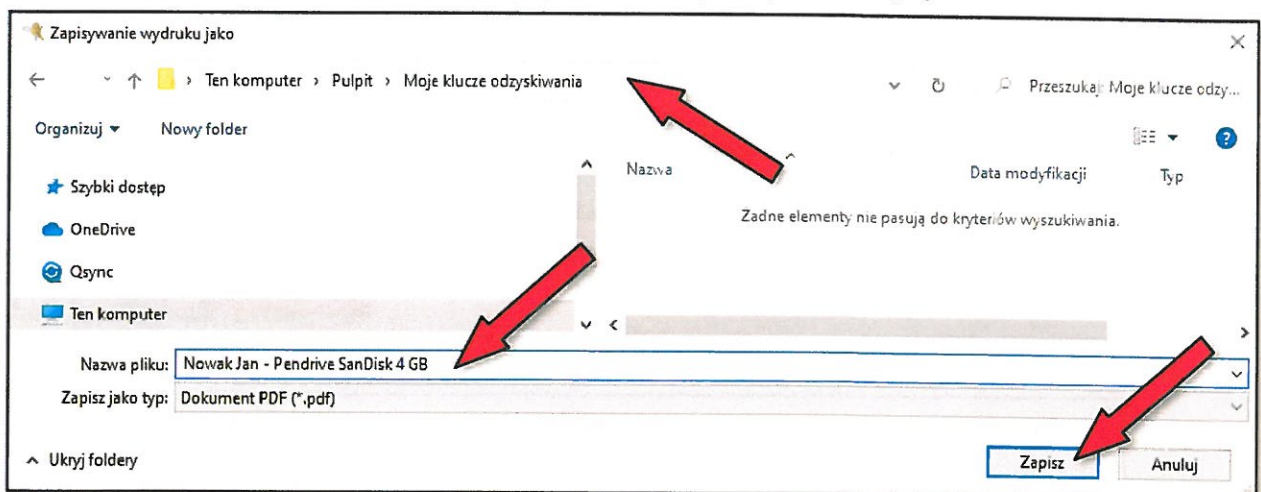
4. Teraz pojawi się okno, w którym wybierasz, gdzie zapisać klucz odzyskiwania (jest on potrzebny, gdy pracownik zapomni hasła, lub je zmieni bez wiedzy pracodawcy). Jeżeli wybierzesz opcję „Zapisz w pliku”, to będzie potrzebny dodatkowy pendrive (na dysku twardym komputera, lub docelowo szyfrowanym pendrive nie można zapisać klucza). Zaleca się zaznaczyć/kliknąć: „Drukuj klucz odzyskiwania”:



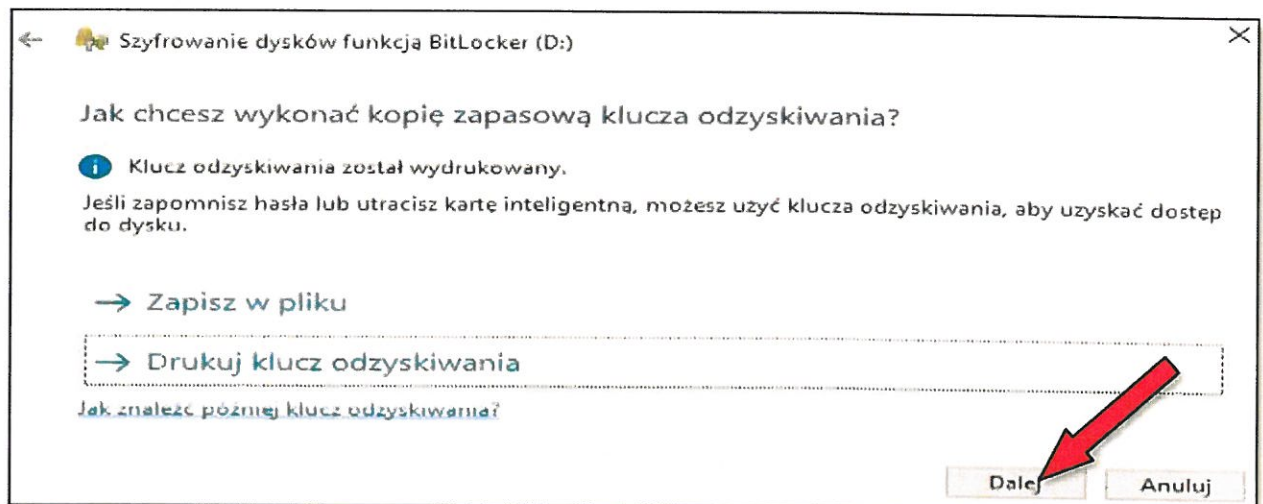
5. Następnie pojawi się okno „Drukowanie”. W nim możesz wybrać, czy chcesz wydrukować zapasowy klucz odzyskiwania lub „wirtualnie” wydrukować do pliku PDF (czyli zapisać do PDF na dysku komputera). Większość systemów operacyjnych Windows ma taką funkcję pod postacią wirtualnej drukarki o nazwie: „Microsoft Print to PDF”. Jeśli takiej nie masz, proponuje się zainstalować na komputerze darmową „drukarkę PDF” o nazwie PDF Creator (aby pobrać program, kliknij: [link](#)). Czyli zaznaczamy wirtualną drukarkę, w tym wypadku wbudowaną w system operacyjny Windows pod postacią „Microsoft Print to PDF” i klikasz „Drukuj”.



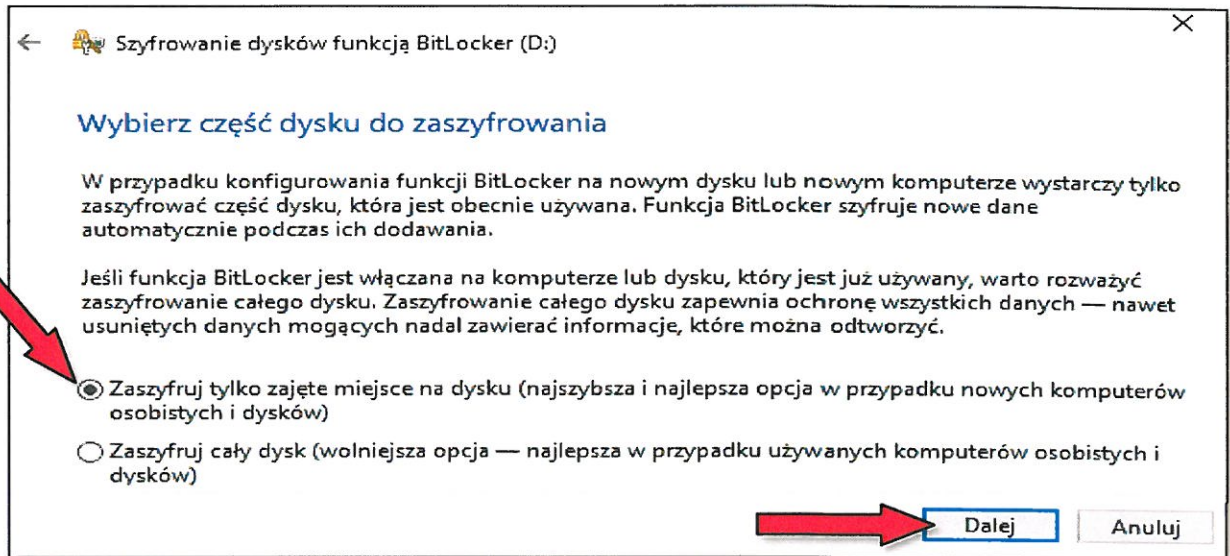
6. Teraz pojawi się okno, w którym powinieneś wybrać, gdzie chcesz zapisać wydruk klucza na komputerze (bądź innym urządzeniu zewnętrznym), nadajesz mu nazwę (najlepiej z nazwą użytkownika i urządzenia) oraz klikasz „Zapisz”



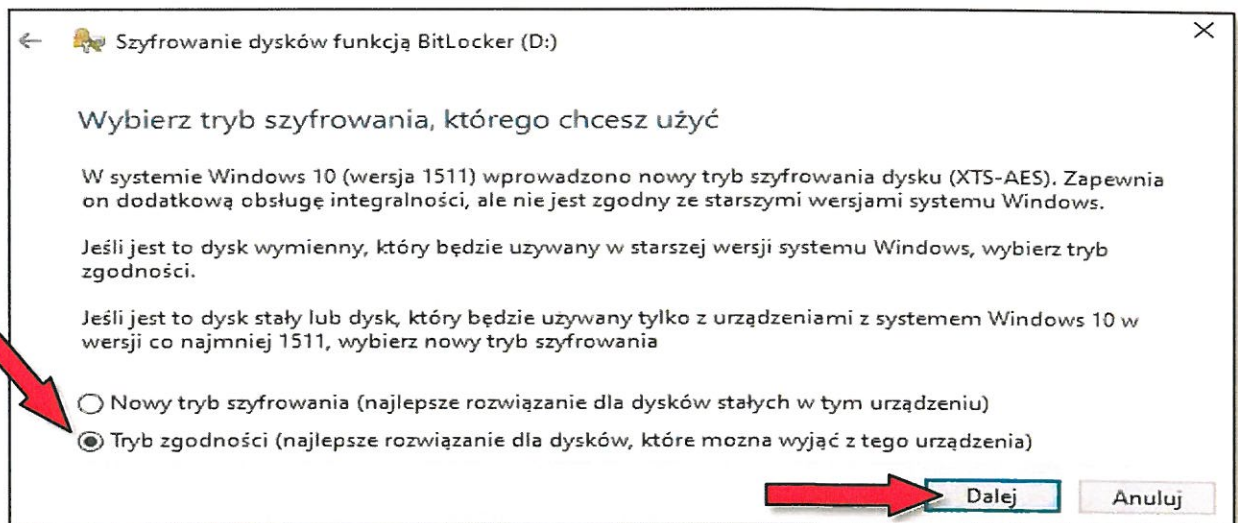
7. Ponownie pojawi się poniższe okno, w którym klikasz „Dalej”:



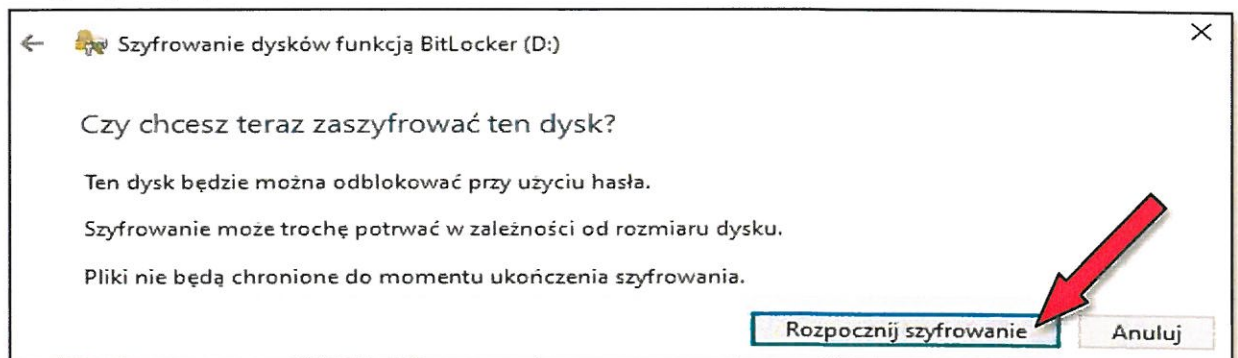
8. Na tym etapie wybierasz zakres szyfrowania tj. czy cały dysk, czy zapisaną część. Wszystko zależy, ile masz czasu, jednakże opcja „Zaszyfruj tylko zajęte miejsce na dysku...” jest wystarczająca. Każdy nowy plik dodany do pamięci pendrive'a będzie automatycznie szyfrowany. Zaleca się zaznaczenie poniższej opcji oraz kliknięcie „Dalej”:



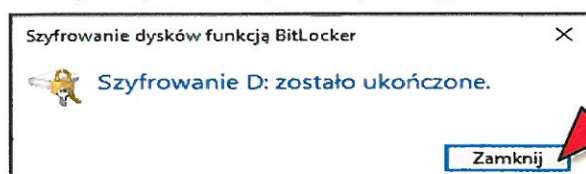
9. Teraz zaleca się zaznaczyć opcję: „Tryb zgodności” aby szyfrowany pendrive był kompatybilny ze starszymi wersjami systemu operacyjnego Windows, a następnie kliknąć „Dalej”:



10. Kliknij „Rozpocznij szyfrowanie”:



11. Poczekaj, aż szyfrowanie się dokończy i kliknij „Zakończ”:

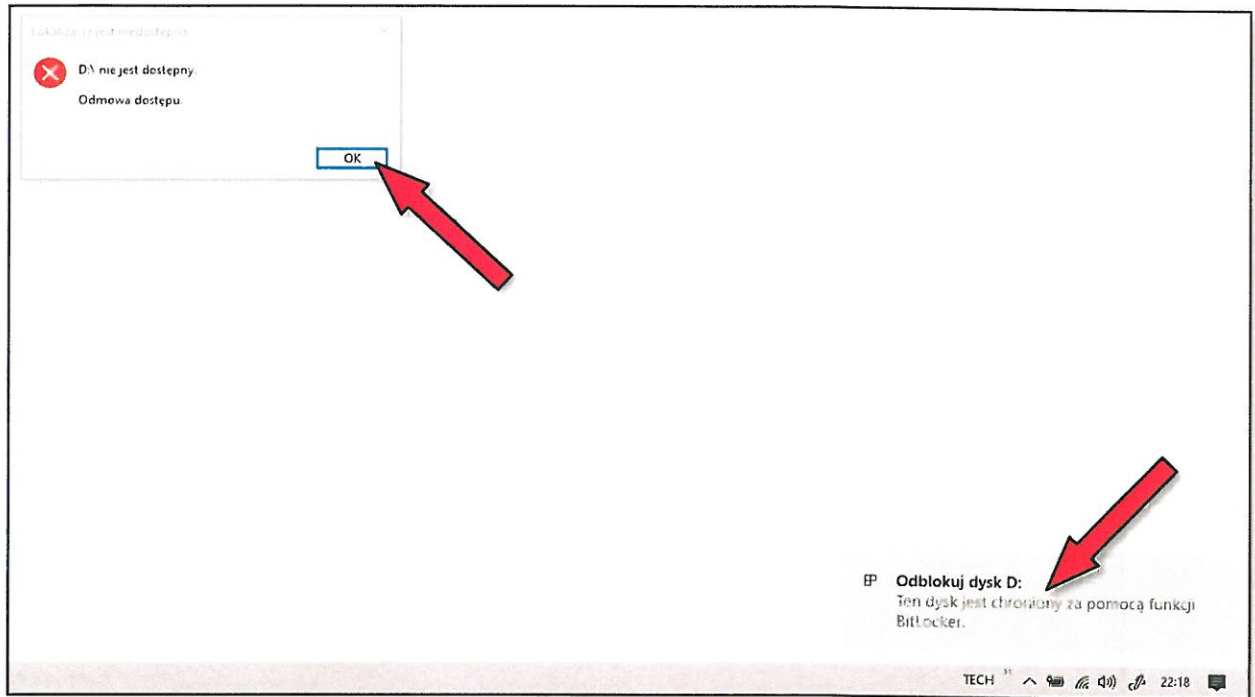


12. Teraz możesz odłączyć pendrive'a i ponownie włożyć do portu USB. System poprosi Cię o hasło.

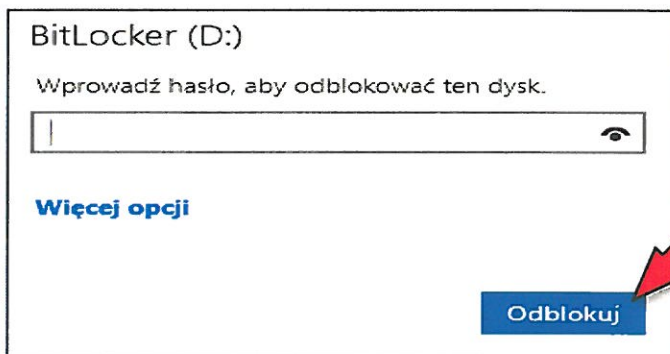
13. Pamiętaj, aby trzymać „klucze odzyskiwania” w wydzielonym miejscu na komputerze lub innym urządzeniu..

ETAP III: UŻYTKOWANIE ZASZYFROWANEGO PENDRIVE'A

1. Za każdym razem, gdy podłączasz zaszyfrowany pendrive do komputera zostaniesz poproszony o wpisanie hasła. W Windowsie 10 będzie to taki komunikat o niedostępności danego pendrive'a/urządzenia oraz okienko „Odblokuj dysk ...”. Kliknij „OK” oraz „Odblokuj dysk ...”



2. Teraz pojawi się okienko z możliwością podania Twojego hasła. Wpisz je i kliknij „Odblokuj”:

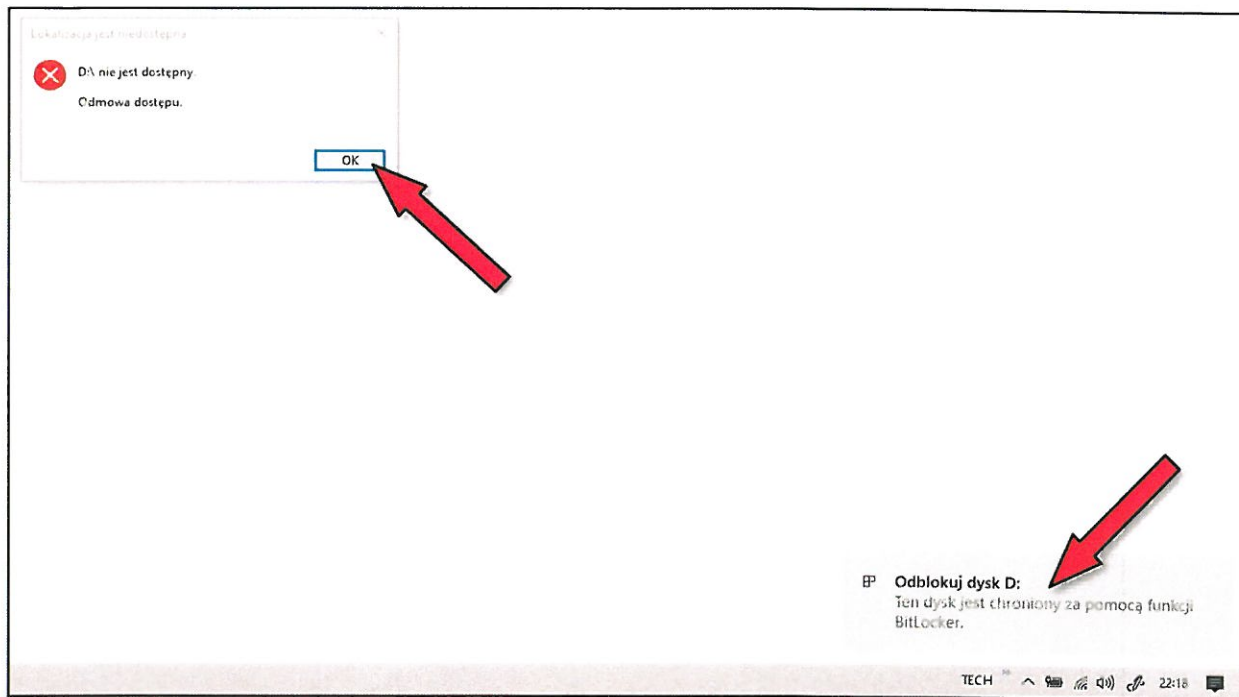


3. Jest jeszcze szerszy zakres dostępu do pendrive'a poprzez kliknięcie „Więcej opcji”. W tym momencie masz możliwość wpisania „Klucza odzyskiwania”, który powinien posiadać TYLKO Administrator organizacji (np. w przypadku zapomnienia/zmiany hasła przez użytkownika). Dodatkowo można zaznaczyć, aby na danym komputerze, pendrive został zapamiętany, aby w przyszłości nie trzeba było za każdym razem wpisywać hasła:

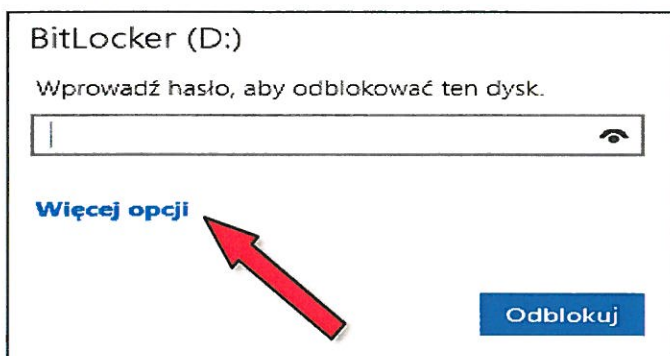


ETAP IV: ODZYSKIWANIE PENDRIVE'A POPRZECZ „KLUCZ ODZYSKIWANIA”

1. W przypadku, gdy użytkownik zapomni hasło, bądź je zmieni możesz uzyskać dostęp do pamięci pendrive'a. W tym celu podłącz zaszyfrowany pendrive do komputera. Następnie pojawi komunikat o niedostępności danego pendrive'a/urządzenia oraz okienko „Odblokuj dysk ...”. Kliknij „OK” oraz „Odblokuj dysk ...”:



2. Teraz pojawi się okienko z możliwością podania hasła, które ktoś zapomniał, lub zmienił. Kliknij „Więcej opcji”:



3. Następnie pojawi się okienko, w którym kliknij: „Wprowadź klucz odzyskiwania”:



4. Teraz znajdź swój wcześniej zapisany w pliku PDF na komputerze lub innym urządzeniu klucz odzyskiwania, składający się z 48 znaków. Na potrzeby tegoż poradnika takowy plik z kluczem został wygenerowany i zawiera przykładową następującą treść:

Klucz odzyskiwania do szyfrowania dysków funkcją BitLocker

Aby sprawdzić, czy jest to poprawny klucz odzyskiwania, porównaj początek następującego identyfikatora z wartością identyfikatora wyświetlaną na ekranie komputera.

Identyfikator:

AA5AAC47-7DFA-44D6-92E0-E6495DFA220A

Jeśli powyższy identyfikator jest zgodny z wartością wyświetlaną na ekranie komputera, odblokuj dysk za pomocą poniższego klucza.

Klucz odzyskiwania:

063943-680185-678667-401841-629420-621467-371327-297924

Jeśli powyższy identyfikator nie jest zgodny z wyświetlanym na komputerze, oznacza to, że nie jest to odpowiedni klucz do odblokowania dysku.

Spróbuj użyć innego klucza odzyskiwania albo przejdź do strony <https://go.microsoft.com/fwlink/?LinkID=260589>, aby uzyskać dodatkową pomoc.

5. Skopiuj ten klucz (zaznacz klucz → wciśnij kombinację znaków „Ctrl+C” oraz wklej do poniższego okna (kombinacja klawiszy „Ctrl+V”, a następnie kliknij „Odblokuj”

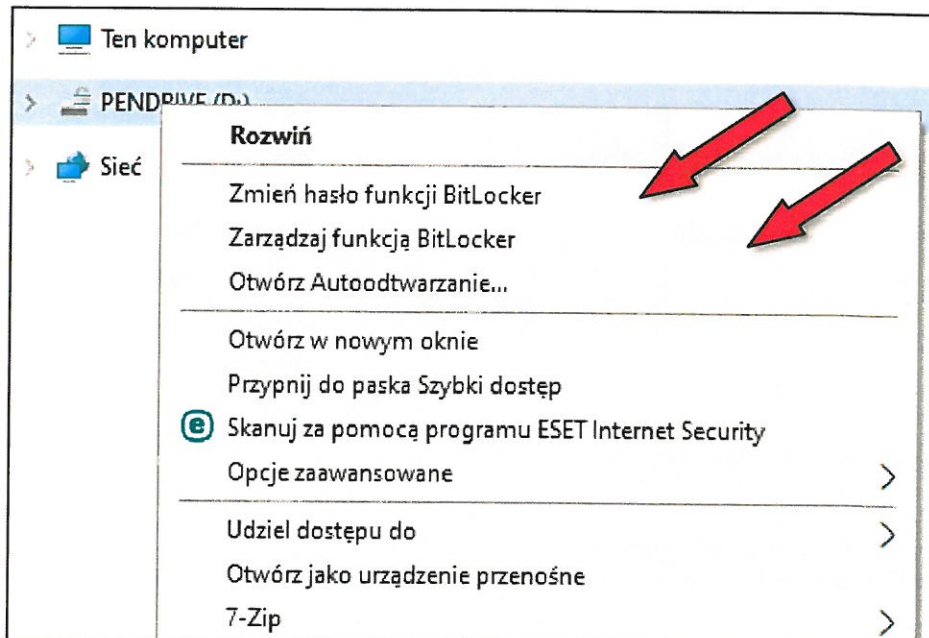
← BitLocker (D:)

Aby odblokować ten dysk, wprowadź 48-cyfrowy klucz odzyskiwania.
(Identyfikator klucza: AA5AAC47)

063943-680185-678667-401841-629420-621467-371327-297924

Odblokuj

6. Od tego momentu masz dostęp do danych na pendrive. Możesz wyłączyć szyfrowanie, bądź zmienić hasło, poprzez kliknięcie prawym przyciskiem myszy (rozwijając podręczne menu) na ikonke pendrive'a:



BEZPIECZNE KORZYSTANIE Z PRZEGLĄDARKI INTERNETOWEJ (Instrukcja użytkowania oprogramowania)

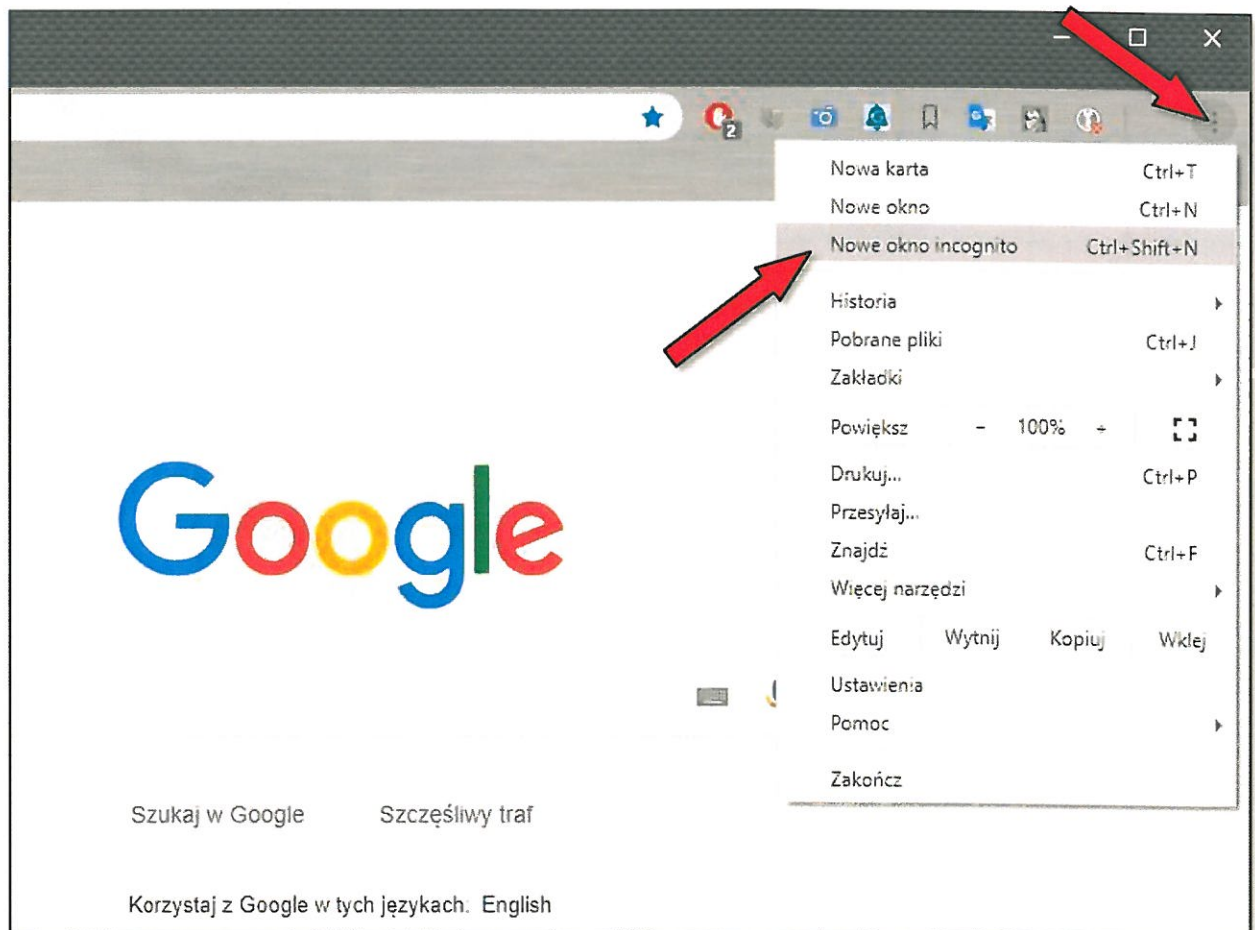
NAZWA OPROGRAMOWANIA:	<i>Przeglądarki internetowe: Chrome Firefox Opera Safari Internet Explorer Microsoft Edge</i>
ZAKRES INSTRUKCJI:	<i>Wstęp i wykaz przeglądarek internetowych; Instrukcja bezpiecznego korzystania z wybranej przeglądarki internetowej</i>

ETAP I: WSTĘP I WYKAZ PRZEGLĄDAREK INTERNETOWYCH

- W obecnych czasach jako administratorzy i użytkownicy sprzętu komputerowego używamy wielorakich przeglądarek internetowych. Niniejsza instrukcja ma na celu ograniczenie ryzyka w zakresie poufności danych podczas korzystania z dostępu do sieci www za pośrednictwem przeglądarki internetowej. Umożliwia:
 - brak zapisu „ciasteczek cookies”,
 - brak zapisu loginów i haseł,
 - brak zapisywania danych z auto-formularzy i wiele innych.
- Wyróżniamy następujące a jednocześnie najczęściej używane przeglądarki internetowe:
 - Chrome,
 - Firefox,
 - Opera,
 - Safari,
 - Internet Explorer,
 - Microsoft Edge.

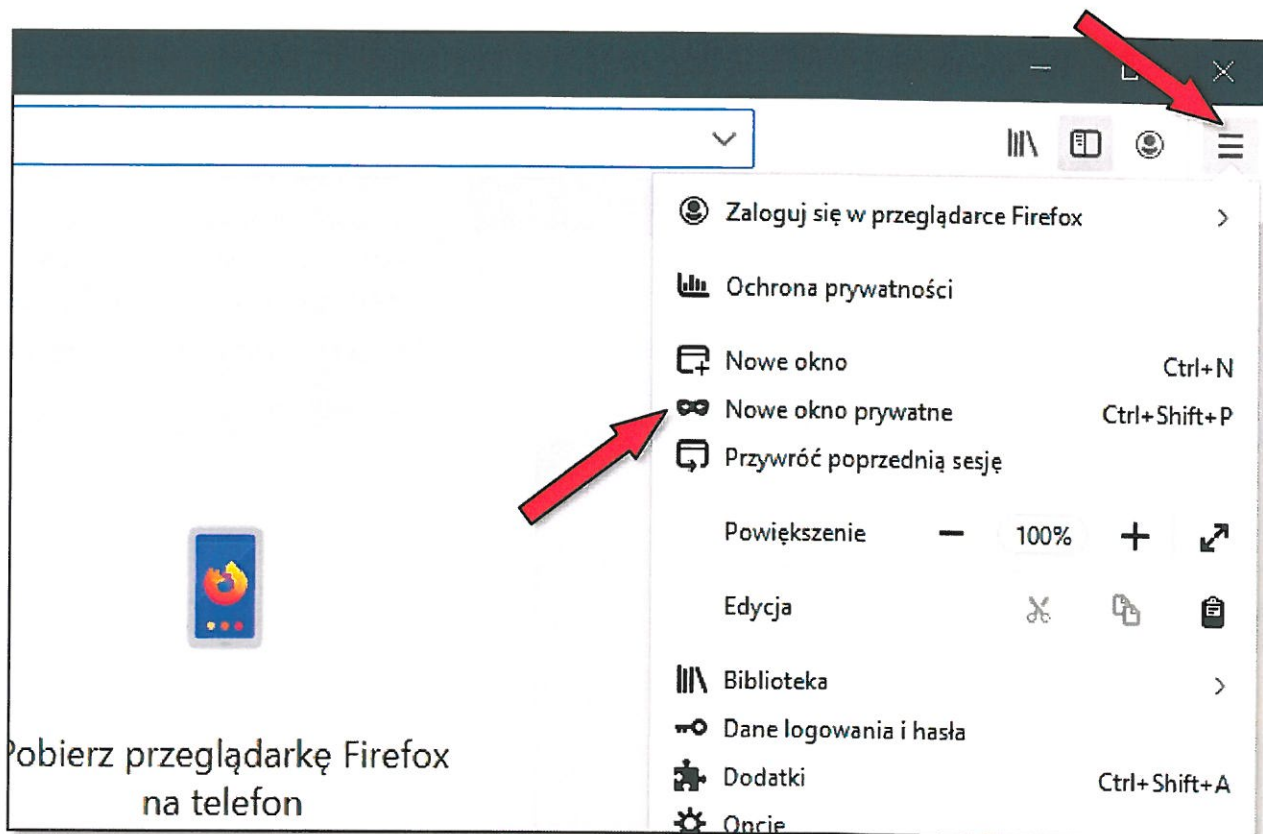
ETAP II-A: INSTRUKCJA BEZPIECZNEGO KORZYSTANIA PRZEGLĄDARKI CHROME

- Po uruchomieniu przeglądarki Chrome kliknij w prawym górnym rogu przycisk z trzema kropkami (menu przeglądarki) a następnie kliknij „Nowe okno incognito”:

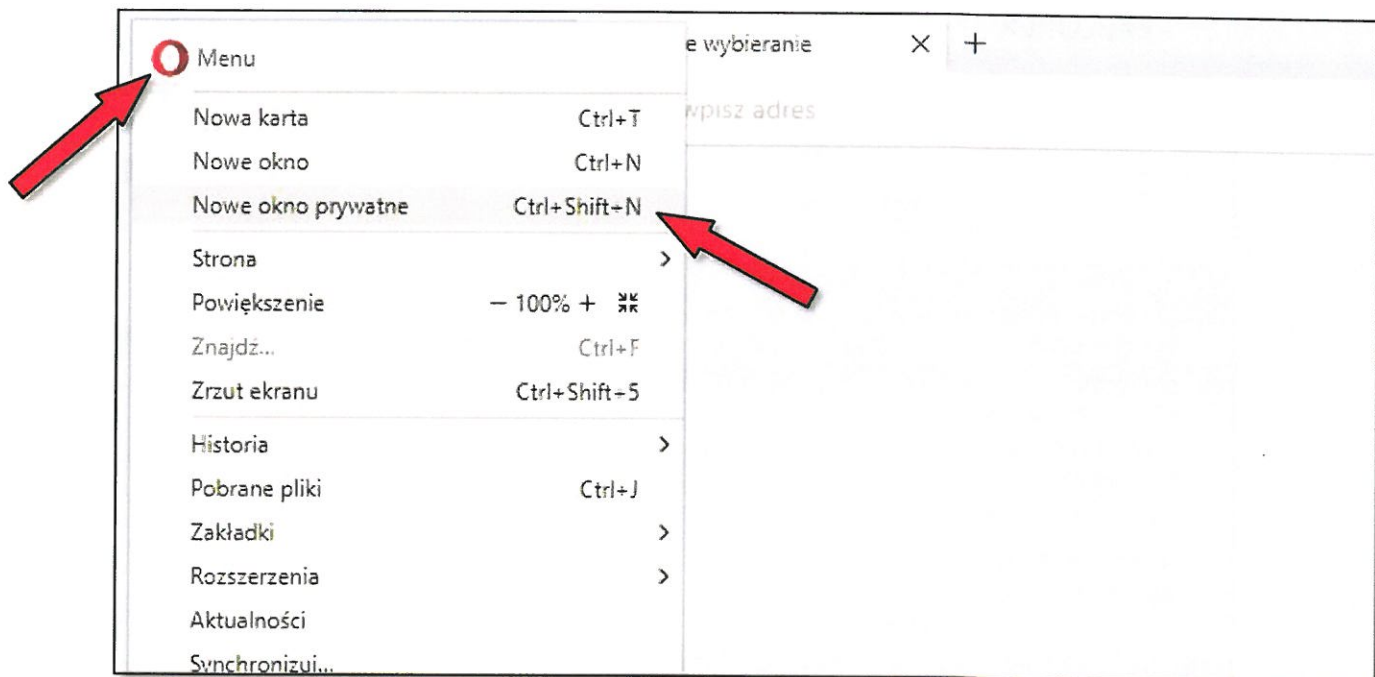


ETAP II-B: INSTRUKCJA BEZPIECZNEGO KORZYSTANIA PRZEGLĄDARKI FIREFOX

1. Po uruchomieniu przeglądarki Firefox kliknij w prawym górnym rogu przycisk z trzema kreskami (menu przeglądarki) a następnie kliknij „Nowe okno prywatne”:

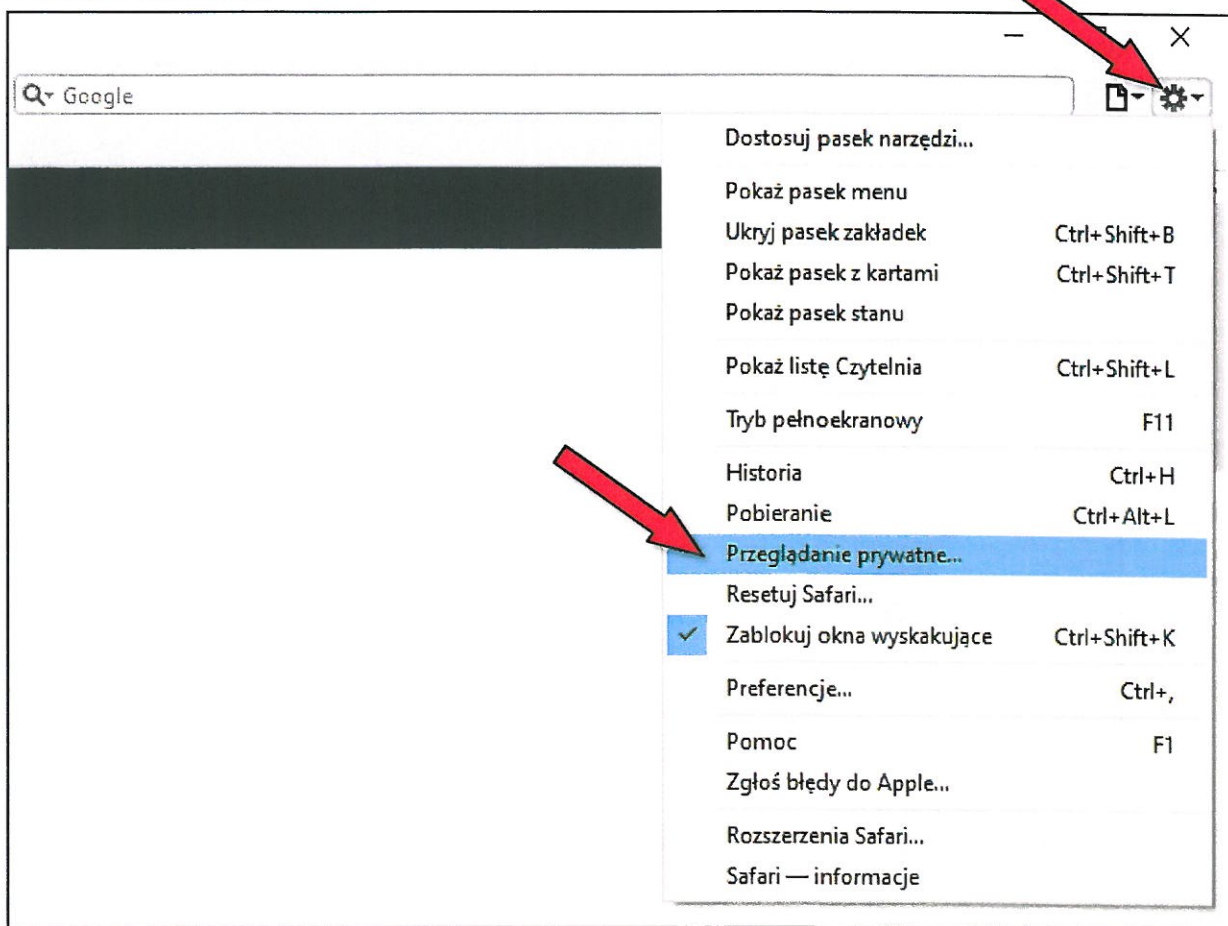
**ETAP II-C: INSTRUKCJA BEZPIECZNEGO KORZYSTANIA PRZEGLĄDARKI OPERA**

1. Po uruchomieniu przeglądarki Opera kliknij w lewym górnym rogu przycisk z literą „O” (menu przeglądarki) a następnie kliknij „Nowe okno prywatne”:



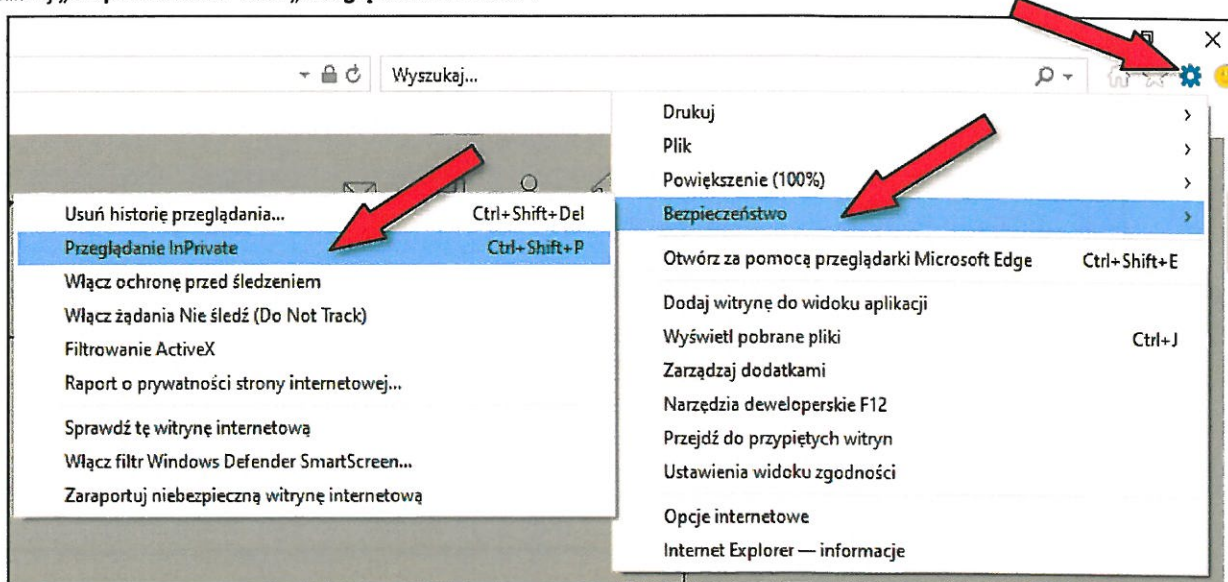
ETAP II-D: INSTRUKCJA BEZPIECZNEGO KORZYSTANIA PRZEGŁĄDARKI SAFARI

1. Po uruchomieniu przeglądarki Safari kliknij w prawym górnym rogu przycisk „zębatki” (menu przeglądarki) a następnie kliknij „Przeglądanie prywatne...”:



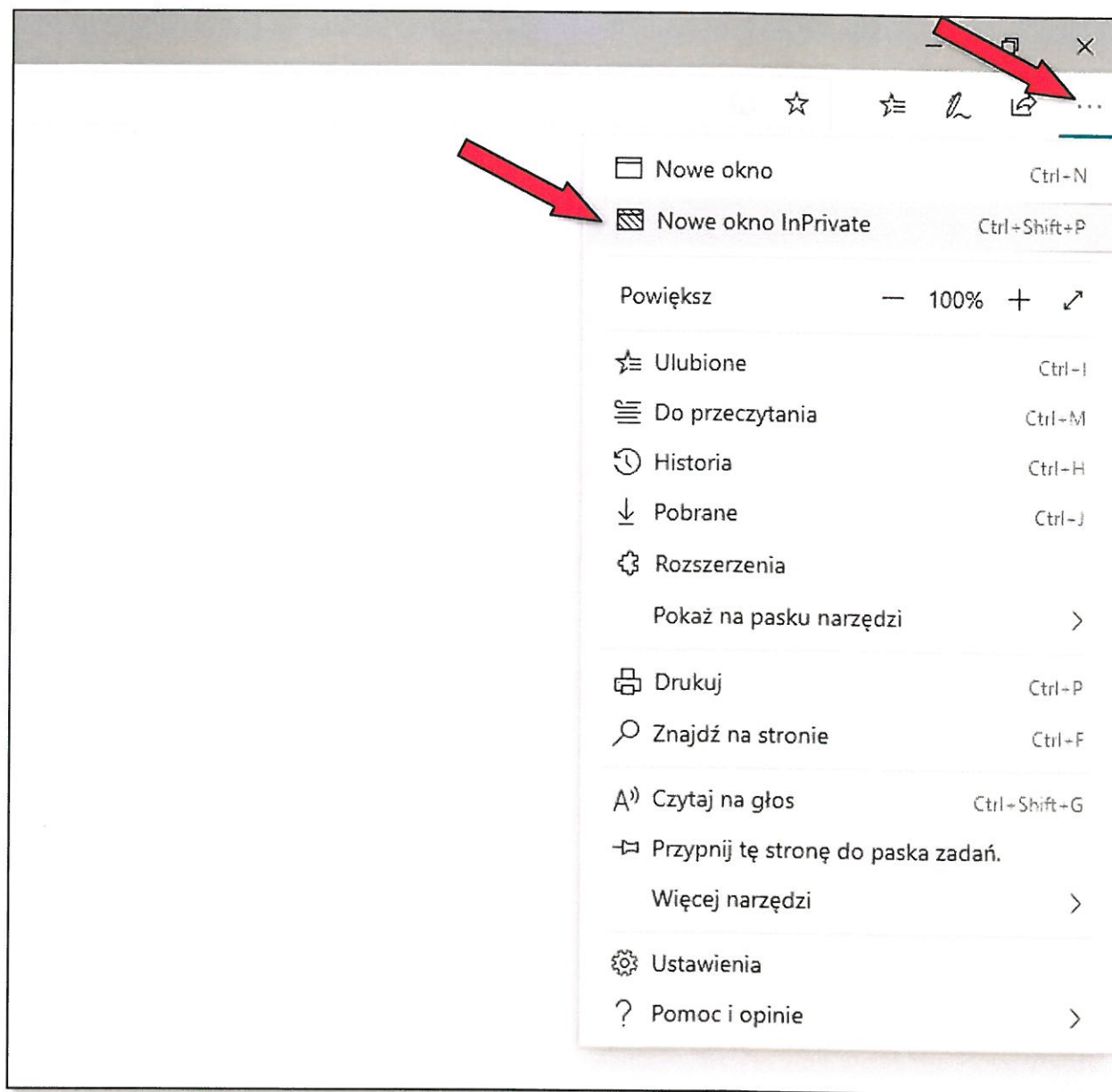
ETAP II-E: INSTRUKCJA BEZPIECZNEGO KORZYSTANIA Z PRZEGŁĄDARKI INTERNET EXPLORER

1. Po uruchomieniu przeglądarki Internet Explorer kliknij w prawym górnym rogu przycisk „zębatki” (menu przeglądarki), następnie kliknij „Bezpieczeństwo” oraz „Przeglądanie InPrivate”:



ETAP II-F: INSTRUKCJA BEZPIECZNEGO KORZYSTANIA Z PRZEGLĄDARKI MICROSOFT EDGE

1. Po uruchomieniu przeglądarki Microsoft Edge kliknij w prawym górnym rogu przycisk z trzema kropkami (menu przeglądarki), a następnie kliknij „**Nowe okno InPrivate**”:



[illegible]

[illegible]

[illegible]

Lp.	lok	typ	nazwa	producent / model	nr.ser.	nr.inw.	oprogramowanie	wersja

działa/ nie działa	

[illegible]

[illegible]

**PROCEDURA POSTĘPOWANIA Z INCYDENTAMI
BEZPIECZEŃSTWA INFORMACJI I NARUSZENIAMI
OCHRONY DANYCH OSOBOWYCH
w Urzędzie Gminy Wiśniewo**

Spis treści

1. Cel procedury	3
2. Przedmiot procedury	3
3. Zakres obowiązań.....	3
4. Odpowiedzialności.....	3
5. Podział zagrożeń	3
6. Identyfikacja zdarzenia	4
7. Analiza zaistniałego zdarzenia.....	5
8. Stwierdzenie naruszenia ochrony danych osobowych.....	5
9. Przykładowe zdarzenia związane z bezpieczeństwem danych osobowych.....	6
10. Rejestr incydentów bezpieczeństwa oraz działań korygujących i zapobiegawczych	8
11. Zgłoszenie naruszenia ochrony danych	8
Załącznik nr 1	9
Załącznik nr 2	11
Załącznik nr 3	12

1. Cel procedury

Celem procedury jest zapewnienie szybkiej, skutecznej i zorganizowanej reakcji na zdarzenia związane z bezpieczeństwem danych osobowych, funkcjonowaniem systemów teleinformatycznych oraz pozostałymi wady techniczne w **Urzędzie Gminy Wiśniewo**.

2. Przedmiot procedury

Przedmiotem procedury jest proces nadzoru nad zgłoszeniami użytkowników w związku z zauważonymi zdarzeniami mogącymi wpłynąć na bezpieczeństwo informacji, w tym danych osobowych, w celu zapewnienia ich wykrycia, odnotowania oraz podjęcia decyzji, co do ostatecznego postępowania ze zdarzeniem.

3. Zakres obowiązań

Procedura obowiązuje wszystkie osoby zobowiązane do przestrzegania zasad obowiązujących w **Urzędzie Gminy Wiśniewo**.

4. Odpowiedzialności

- 4.1 Osobami odpowiedzialnymi za nadzór nad procedurą są Administrator Systemów Informatycznych i Inspektor Ochrony Danych (IOD).
- 4.2 Za zgłoszenie odpowiadają wszyscy użytkownicy systemów informatycznych oraz inni pracownicy lub współpracownicy **Urzędu Gminy Wiśniewo**.
- 4.3 Administrator Systemów Informatycznych jest odpowiedzialny za obsługę zgłoszeń dotyczących zdarzeń związanych z funkcjonowaniem systemów teleinformatycznych.
- 4.4 IOD i Administrator Systemów Informatycznych odpowiedzialni są za obsługę zgłoszeń dotyczących zdarzeń związanych z ochroną danych osobowych.
- 4.5 Administrator Systemów Informatycznych odpowiedzialny jest za obsługę zgłoszeń dotyczących pozostałych wad technicznych.

5. Podział zagrożeń

- 5.1 Zagrożenia dla bezpieczeństwa informacji, w tym danych osobowych dzielimy na:
 - a) Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) - ich wystąpienie może prowadzić do utraty integralności danych, zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość działania organizacji, może dotyczyć naruszenia poufności i dostępności danych.

- b) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania) - ich wystąpienie może prowadzić do zniszczenia danych, zakłócenia ciągłości pracy systemu, może dotyczyć naruszenia poufności i dostępności danych.
- c) Zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia naruszenia poufności danych (zazwyczaj następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy).

6. Identyfikacja zdarzenia

- 6.1 Zdarzenia związane z funkcjonowaniem systemów teleinformatycznych należy zgłaszać do Administratora Systemów Informatycznych. Administrator Systemów Informatycznych ma obowiązek zareagowania na automatyczne powiadomienia systemu teleinformatycznego generowane przez moduł wykrywania włamań i innych zdarzeń związanych z bezpieczeństwem danych.
- 6.2 Zgłoszenia pozostałych wad technicznych należy kierować do Administrator Systemów Informatycznych.
- 6.3 Zdarzenia dotyczące możliwego naruszenia ochrony danych osobowych należy zgłaszać do IOD i Administratora Systemów Informatycznych.
- 6.4 Wybór środka przekazu zgłoszenia dokonuje zgłaszający i powinien być on adekwatny do zaistniałej sytuacji. Zgłoszenia należy dokonać drogą:
 - a) mailową,
 - b) telefoniczną,
 - c) osobiście.
- 6.5 Jeśli zgłoszone zdarzenie związane z funkcjonowaniem systemów teleinformatycznych Administrator Systemów Informatycznych zakwalifikuje jako potencjalne zdarzenie dotyczące naruszenia ochrony danych osobowych, niezwłocznie powiadamia Administratora Danych Osobowych i IOD.
- 6.6 Jeśli Administrator Systemów Informatycznych zakwalifikuje wykrytą wadę techniczną jako potencjalne zdarzenie dotyczące bezpieczeństwa danych osobowych, niezwłocznie powiadamia IOD.

7. Analiza zaistniałego zdarzenia

7.1 Każde zgłoszenie zdarzenia związanego z funkcjonowaniem systemów teleinformatycznych lub wady technicznej powinno być przypisane do pracownika odpowiedzialnego za obsługę i realizację zgłoszenia.

7.2 Priorytet załatwienia zgłoszonego zdarzenia związanego z funkcjonowaniem systemów teleinformatycznych lub wady technicznej określa się na podstawie potencjalnego wpływu na **Urząd Gminy Wiśniewo**.

7.3 Zdarzenie mogące stanowić naruszenie ochrony danych osobowych jest rozpatrywane przez Administratora Danych Osobowych i IOD niezwłocznie pod jego stwierdzeniu, celem ustalenia:

- Czy zdarzenie naruszyło ochronę danych osobowych?
- Czy zdarzenie miało wpływ na poufność, integralność lub dostępność danych?
- Potencjalna przyczyna wystąpienia zdarzenia?
- Czy zdarzenie wpływające na bezpieczeństwo należy traktować jako naruszenie?
- Jeżeli tak to czy rodzaj naruszenia podlega zgłoszeniu do organu nadzorczego?
- Jaki rozmiar miało naruszenie?
- Ile danych osobowych uległo utracie poufności lub integralności lub dostępności?
- W jakim stopniu prawdopodobne jest, aby zdarzenie skutkowało ryzykiem naruszenia praw i wolności osób fizycznych?

8. Stwierdzenie naruszenia ochrony danych osobowych

Jeśli zdarzenie zostało zakwalifikowane jako naruszenie ochrony danych osobowych, Administrator dokumentuje okoliczności każdego naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze i bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (art. 33 RODO). Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia

praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu (art. 34 RODO).

Zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego musi co najmniej:

- a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
- b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

9. Przykładowe zdarzenia związane z bezpieczeństwem danych osobowych

- Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby informacyjne jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja stron trzecich itp.
- Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.
- Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie teleinformatycznym służącym do przetwarzania danych osobowych.
- Próba lub modyfikacja danych lub zmiana w strukturze danych osobowych bez odpowiedniego upoważnienia (autoryzacji).
- Niedopuszczalna manipulacja danymi osobowymi w systemie teleinformatycznym.

- Ujawnienie osobom nieupoważnionym danych osobowych.
- Praca w systemie lub jego sieci komputerowej wskazująca na nieprzypadkowe odstępstwa od założonego rytmu pracy oraz na przełamanie lub zaniechanie ochrony danych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
- Podmiana lub zniszczenie nośników z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowanie lub kopiowanie danych.
- Rażąco naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa danych osobowych (np. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych).
- Nieprawidłowe zabezpieczenie miejsca przechowywania danych osobowych, w tym także osobowych (otwarte szafy, biurka, regały, i inne).
- Naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie danych osobowych (uszkodzone zamki, okna, drzwi, naruszone plomby, itp.).
- Nadmierne, w stosunku do wykonywanych zadań (zakres upoważnienia), uprawnienia użytkownika do zasobów systemu służącego do przetwarzania danych osobowych.
- Niestabilna praca (anomalie) systemu lub programu, mogące świadczyć np. o obecności wirusa.
- Duża liczba nieudanych logowań w krótkim czasie.
- Nowe, nieautoryzowane konta użytkownika.
- Logi świadczące o korzystaniu z systemu po godzinach pracy.
- Utrata częściowa lub całkowity brak możliwości odtworzenia danych osobowych.
- Wysłanie danych do niewłaściwej osoby.
- Wynoszenie danych osobowych w wersji papierowej i elektronicznej poza organizację bez odpowiedniej zgody i upoważnienia.
 - Utrata nośników przenośnych z danymi osobowymi.

10. Rejestr incydentów bezpieczeństwa oraz działań korygujących i zapobiegawczych

- 10.1 W przypadku wystąpienia incydentu lub podejrzenia jego wystąpienia niezbędne jest jego rejestracja w Rejestrze incydentów bezpieczeństwa oraz działań korygujących i zapobiegawczych, który stanowi **załącznik nr 1** do niniejszej procedury.
- 10.2 Administrator (ADO) lub IOD dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport - **załącznik nr 2** do niniejszej procedury.

11. Zgłoszenie naruszenia ochrony danych

- 11.1 Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).
- 11.2 Zgłoszenia można dokonać na 4 sposoby:
- a) Elektronicznie poprzez wypełnienie **dedykowanego formularza elektronicznego** dostępnego bezpośrednio na platformie **biznes.gov.pl** będącego odwzorowaniem formularza dostępnego w załączniku.
 - b) Elektronicznie poprzez wysłanie wypełnionego formularza na **elektroniczną skrzynkę podawczą ePUAP: /UODO/SkrytkaESP**
 - c) Elektronicznie poprzez wysłanie wypełnionego formularza (dostępnego poniżej w załączniku) za pomocą **pisma ogólnego dostępnego na platformie biznes.gov.pl** lub **platformie epuap.gov.pl**
 - d) Tradycyjną pocztą wysyłając wypełniony formularz na adres Urzędu.
- 11.3 Jeżeli naruszenie dotyczy danych osób w różnych krajach UE, Prezes UODO może być, ale nie musi być wiodącym (czyli właściwym dla administratora lub podmiotu przetwarzającego) organem nadzorczym. W przypadku transgranicznego naruszenia danych administrator powinien dokonać analizy, czy wiodącym organem nadzorczym w odniesieniu do czynności przetwarzania, które zostały objęte naruszeniem jest Prezes UODO, czy też może inny europejski organ nadzorczy.
- 11.4 Wzór Zgłoszenie naruszenia ochrony danych osobowych stanowi **załącznik nr 3** do niniejszej procedury.

[illegible]

RAPORT Z NARUSZENIA OCHRONY DANYCH

1. Data Godzina
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem

.....
(imię, nazwisko, stanowisko służbowe,):
3. Lokalizacja zdarzenia
(nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):
4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

.....
5. Podjęte działania:

.....

.....
6. Wstępna ocena przyczyn wystąpienia naruszenia:

.....

.....
7. Postępowanie wyjaśniające i naprawcze:

.....

.....

.....
(podpis pracownika)

.....
(data i podpis ADO/Inspektora ochrony danych)

Zgłoszenie naruszenia ochrony danych osobowych

1. Typ zgłoszenia

Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie.

Podaj swoją sygnaturę sprawy (opcjonalnie)
(np. sygnatura w Twoim wewnętrznym rejestrze naruszeń)

[Kliknij tutaj, aby wprowadzić tekst](#)

☒ Zgłoszenie kompletne/jednorazowe	☐ Zgłoszenie wstępne	☐ Zgłoszenie uzupełniające/zmieniające
	Podaj przybliżoną datę uzupełnienia zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę	Podaj datę poprzedniego zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę Podaj sygnaturę sprawy UODO Kliknij tutaj, aby wprowadzić tekst

☐ Naruszenie zostało lub zostanie zgłoszone organowi ochrony danych osobowych w innym państwie [Jeśli tak, podaj w jakim.](#)

☐ Naruszenie zostało lub zostanie zgłoszone innym organom np. Policja, CSIRT NASK, CSIRT GOV, CSIRT MON (należy wysłać na nazwę organu by dowiedzieć się więcej)

Podaj nazwy tych organów
[Kliknij tutaj, aby wprowadzić tekst.](#)

Podaj numer/sygnaturę zgłoszenia do innego organu
[Kliknij tutaj, aby wprowadzić tekst.](#)

2. Podmiot zgłaszający

2A. Dane administratora danych

Pełna nazwa administratora [Kliknij tutaj, aby wprowadzić tekst](#)

REGON (opcjonalnie) [Podaj numer.](#) NIP (opcjonalnie) [Podaj numer.](#) KRS (opcjonalnie) [Podaj numer.](#)

Sektor (opcjonalnie) Dla sektora publicznego: [Wybierz element.](#) Dla sektora prywatnego: [Wybierz element.](#)

2B. Adres siedziby administratora danych

Ulica Kliknij tutaj, aby wprowadzić tekst.	Numer domu Podaj numer	Numer lokalu Podaj numer
Miejscowość Kliknij tutaj, aby wprowadzić tekst	Kod pocztowy Kliknij tutaj, aby wprowadzić tekst.	
Gmina Kliknij tutaj, aby wprowadzić tekst	Powiat Kliknij tutaj, aby wprowadzić tekst.	
Województwo Kliknij tutaj, aby wprowadzić tekst	Państwo Kliknij tutaj, aby wprowadzić tekst.	

2C. Osoby uprawnione do reprezentowania administratora

1.	Imię i nazwisko Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst
2.	Imię i nazwisko Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
3.	Imię i nazwisko Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst
4.	Imię i nazwisko Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst
5.	Imię i nazwisko Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.

2D. Pełnomocnik

☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Jeśli zgłoszenie przesyłane jest w formie elektronicznej, należy załączyć pełnomocnictwo udzielone w formie elektronicznej oraz dowód uiszczenia opłaty skarbowej

2E. Inspektor ochrony danych

Imię i nazwisko Numer telefonu Adres e-mail

☐ Inspektor nie został wyznaczony

Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.
Kliknij tutaj, aby wprowadzić tekst.

Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie (np. podmiot przetwarzający, współadministrator, operator pocztowy itp.)

1.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
2.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
3.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
4.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
5.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.

3. Czas naruszenia

3A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia

Wskaz kiedy dowiedział się o naruszeniu.
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Sposób stwierdzenia naruszenia

Np. zgłoszenie osoby której dane dotyczą czy cyfrowy przebieg logów systemowych zgodnie z wytyczną polityki bezpieczeństwa.

Data powiadomienia przez podmiot przetwarzający

(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu

Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełnienia formularza jest dłuższy niż 72h.

3B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia

Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Data i czas zakończenia naruszenia

(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

4. Charakter naruszenia

4A. Opisz szczegółowo na czym polegało naruszenie

Kliknij tutaj, aby wprowadzić tekst.

4B. Na czym polegało naruszenie?

- | | |
|--|---|
| ☐ a) Zgubienie lub kradzież nośnika/urządzenia | ☐ h) Nieprawidłowa anonimizacja danych osobowych w dokumencie |
| ☐ b) Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji | ☐ i) Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora |
| ☐ c) Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy | ☐ j) Niezamierzona publikacja |
| ☐ d) Nieuprawnione uzyskanie dostępu do informacji | ☐ k) Dane osobowe wysłane do niewłaściwego odbiorcy |
| ☐ e) Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń | ☐ l) Ujawnienie danych niewłaściwej osoby |
| ☐ f) Złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych | ☐ m) Ustne ujawnienie danych osobowych |
| ☐ g) Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing) | |

4C. Działanie złośliwego oprogramowania (odpowiedz na poniższe pytania, jeśli w sekcji 4B zaznaczono pole f)

- a) Jeśli w ocenie administratora doszło wyłącznie do naruszenia dostępności danych, w jaki sposób stwierdzono, że nie doszło do naruszenia ich poufności? (w sytuacji gdy np. dane nie zostały pobrane przez osobę nieupoważnioną, a jedynie zaszyfrowane w sposób uniemożliwiający uzyskanie do nich dostępu)

Kliknij tutaj, aby wprowadzić tekst.

- b) Czy, a jeżeli tak, to w jakiej formie, złośliwe oprogramowanie poinformowało o konieczności uiszczenia opłaty w celu odzyskania dostępu do danych (podaj nazwę złośliwego oprogramowania, sposób poinformowania, żadaną kwotę, kanał komunikacji, sposób zapłaty oraz termin)

Kliknij tutaj, aby wprowadzić tekst.

- c) Jeżeli doszło do utraty dostępności danych, to czy administrator był w posiadaniu kopii zapasowej, jeśli tak to w jakim czasie ją przywrócił?

Kliknij tutaj, aby wprowadzić tekst.

UWAGA: Jeżeli zgłoszenie naruszenia dotyczy podejrzanych załączników, phishingu, szantażu czy działania złośliwego oprogramowania, rozważ zgłoszenie zdarzenia do CERT Polska pod adresem <https://incydent.cert.pl>. Dokonanie takiego zgłoszenia jest szczególnie zalecane w przypadku, kiedy odpowiedzi na powyższe pytania są utrudnione bądź niemożliwe. O fakcie zgłoszenia incydentu do CERT Polska poinformuj w zgłoszeniu uzupełniającym Prezesa UODO (pkt 1 formularza) podając datę zgłoszenia, jego numer oraz ewentualnie informacje na temat incydentu otrzymane od CERT Polska).

4D. Przyczyna naruszenia

- | | |
|---|--|
| ☐ Wewnętrzne działanie niezamierzone | ☐ Wewnętrzne działanie zamierzone |
| ☐ Zewnętrzne działanie niezamierzone | ☐ Zewnętrzne działanie zamierzone |

4E. Charakter

- ☐ Naruszenie poufności danych
Nieuprawnione lub przypadkowe ujawnienie lub udostępnienie danych
- ☐ Naruszenie integralności danych
Wprowadzenie nieuprawnionych zmian podczas edycji, zapisu, transmisji lub przechowywania
- ☐ Naruszenie dostępności danych
Brak możliwości wykorzystania danych na zgodnie w założonym czasie przez osobę do tego uprawnioną

4F. Dzieci

- ☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
(opcjonalnie)

5. Liczba osób i wpisów

Przybliżona liczba osób, których dotyczy naruszenie

Kliknij tutaj, aby wprowadzić tekst.

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie
Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów, np. jednej osobie można przypisać kilka wykonanych transakcji

[Kliknij tutaj, aby wprowadzić tekst.](#)

6. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

Dane podstawowe

- | | |
|--|--|
| ☐ Nazwiska i imiona | ☐ Nazwa użytkownika i/lub hasło |
| ☐ Imiona rodziców | ☐ Dane dotyczące zarobków i/lub posiadanego majątku |
| ☐ Data urodzenia | ☐ Nazwisko rodowe matki |
| ☐ Numer rachunku bankowego | ☐ Seria i numer dowodu osobistego |
| ☐ Adres zamieszkania lub pobytu | ☐ Numer telefonu |
| ☐ Numer ewidencyjny PESEL | ☐ Wizerunek |
| ☐ Adres e-mail | ☐ Inne, wskaź jakie: |

[Kliknij tutaj, aby wprowadzić tekst.](#)

6B. Dane szczególnej kategorii

- | | |
|---|---|
| ☐ Dane o pochodzeniu rasowym lub etnicznym | ☐ Dane dotyczące seksualności lub orientacji seksualnej |
| ☐ Dane o poglądach politycznych | ☐ Dane dotyczące zdrowia |
| ☐ Dane o przekonaniach religijnych lub światopoglądowych | ☐ Dane genetyczne |
| ☐ Dane o przynależności do związków zawodowych | ☐ Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej |

6C. Dane, o których mowa w art. 10 RODO

- | | | |
|---|---|-------------------------------|
| ☐ Dane dotyczące wyroków skazujących | ☐ Dane dotyczące czynów zabronionych | ☐ Inne |
|---|---|-------------------------------|

[Kliknij tutaj, aby wprowadzić tekst.](#)

7. Kategorie osób

- | | |
|---|--|
| ☐ Pracownicy | ☐ Klienci (obecni i potencjalni) |
| ☐ Użytkownicy | ☐ Klienci podmiotów publicznych |
| ☐ Subskrybenci | ☐ Pacjenci |
| ☐ Studenci | ☐ Dzieci |
| ☐ Uczniowie | ☐ Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.) |
| ☐ Służby mundurowe (np. wojsko, policja) | |

Szczegółowy opis kategorii osób, których dotyczy naruszenie:

Opisz np. Tego i w jakim przedziale czasowym dotyczy naruszenie

W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

[Kliknij tutaj, aby wprowadzić tekst.](#)

8. Możliwe konsekwencje

8A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą

- ☐ Utrata kontroli nad własnymi danymi osobowymi
- ☐ Ograniczenie możliwości realizowania praw z art. 15-22 RODO
- ☐ Ograniczenie możliwości realizowania praw
- ☐ Dyskryminacja
- ☐ Kradzież lub sfalszowanie tożsamości

- ☐ Strata finansowa
- ☐ Naruszenie dobrego imienia
- ☐ Utrata poufności danych osobowych chronionych tajemnicą zawodową
- ☐ Nieuprawnione odwrócenie pseudonimizacji
- ☐ Inne

Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

8B. Czy wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych?

☒ Tak

☐ Nie

Uzasadnienie

Kliknij tutaj, aby wprowadzić tekst.

9. Środki bezpieczeństwa i środki zaradcze

9A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych

Kliknij tutaj, aby wprowadzić tekst.

9B. Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia

Kliknij tutaj, aby wprowadzić tekst.

9C. Środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

10. Czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu?

☒ Tak	☐ Nie, ale zostaną zawiadomione Pamiętaj, że po powiadomieniu osób, należy przesłać treść zawiadomienia do UODO.	☐ Nie, nie zostaną zawiadomione, ponieważ:	☐ Nie ocenilem jeszcze
Czy indywidualnie? ☒ Tak Nie, gdyż indywidualne zawiadomienie każdej osoby, której dane dotyczą wymagałoby niewspółmiernie dużego wysiłku. W związku z tym został bądź zostanie wydany publiczny komunikat lub zastosowany podobny środek, za pomocą którego osoby, których dane dotyczą, zostały bądź zostaną poinformowane w równie skuteczny sposób.		Jeśli jeszcze nie ocenileś, czy zamierzasz zawiadomić osoby, których dane dotyczą, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.	
Wskaz datę zawiadomienia Kliknij tutaj, aby wprowadzić datę.	Wskaz datę planowanego zawiadomienia Kliknij tutaj, aby wprowadzić datę.	przed naruszeniem wdrożono odpowiednie techniczne i organizacyjne środki ochrony (wskazane w pkt. 9A formularza) i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, anonimizacja czy pseudonimizacja uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.	
Liczba zawiadomionych osób Kliknij tutaj, aby wprowadzić tekst.	☐ Nie znam jeszcze daty kiedy zamierzam zawiadomić osoby, których dane dotyczą	po naruszeniu zastosowano środki (wskazane w pkt. 9C formularza) eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.	
Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą Kliknij tutaj, aby wprowadzić tekst.		stwierdzono brak wysokiego ryzyka naruszenia praw lub wolności osób fizycznych (uzasadnienie w pkt. 8B formularza).	
Umieść zanonimizowaną treść zawiadomienia, którą przesłałeś bądź zamierzasz przesłać do osób, których dane dotyczą. Pamiętaj, że zawiadomienie powinno: • opisywać jasnym i prostym językiem charakter naruszenia ochrony danych osobowych, • zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji, • opisywać możliwe konsekwencje naruszenia ochrony danych osobowych, • opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosowanych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.			

Kliknij tutaj, aby wprowadzić tekst.

11. Przetwarzanie transgraniczne

☐ Naruszenie ma charakter transgraniczny

Zaznacz kraje Europejskiego Obszaru Gospodarczego, których dotyczy naruszenie:

- | | | | |
|--|-------------------------------------|-------------------------------------|--|
| ☐ Austria | ☐ Belgia | ☐ Bułgaria | ☐ Chorwacja |
| ☐ Cypr | ☐ Czechy | ☐ Dania | ☐ Estonia |
| ☐ Finlandia | ☐ Francja | ☐ Grecja | ☐ Hiszpania |
| ☐ Holandia | ☐ Irlandia | ☐ Islandia | ☐ Liechtenstein |
| ☐ Litwa | ☐ Luksemburg | ☐ Łotwa | ☐ Malta |
| ☐ Niemcy | ☐ Norwegia | ☐ Portugalia | ☐ Rumunia |
| ☐ Słowacja | ☐ Słowenia | ☐ Szwecja | ☐ Węgry |
| ☐ Wielka Brytania | ☐ Włochy | | |

Data, miejscowość
(dla zgłoszenia w formie
papierowej)

Podpis osoby lub osób
upoważnionych
do reprezentowania
administratora¹
(dla zgłoszenia w formie
papierowej)

¹ Jeżeli zgłoszenie podpisuje pełnomocnik, należy pamiętać o załączeniu pełnomocnictwa

Informacja:

Administrator danych osobowych.

Administratorem Państwa danych osobowych będzie Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stawki 2.

Można się z nami kontaktować w następujący sposób:

- a) listownie: ul. Stawki 2, 00-193 Warszawa
- b) przez elektroniczną skrzynkę podawczą dostępną na stronie <https://www.uodo.gov.pl/pl/p/kontakt>
- c) telefonicznie: (22) 531 03 00

Inspektor ochrony danych.

Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych pod adresem email IOD@uodo.gov.pl

Cele i podstawy przetwarzania.

Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu w celu przyjmowania zgłoszeń o naruszeniu ochrony danych osobowych zgodnie z art. 33 ust. 1, 3 i 4 RODO¹ bądź art. 44 ust. 1 – 5 DODO², podejmowania działań określonych w art. 34 ust. 4 oraz art. 58 ust. 2 RODO bądź art. 45 ust. 5 DODO, a także prowadzenia przez organ wewnętrzny rejestru naruszeń na podstawie art. 57 ust. 1 lit. u RODO. Następnie Państwa dane będziemy przetwarzać w celu wypełnienia obowiązku archiwizacji dokumentów wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Odbiorcy danych osobowych.

Odbiorcami Państwa danych osobowych będą Minister Cyfryzacji w związku z zamieszczeniem formularza na platformie E-PUAP bądź Minister Przedsiębiorczości i Technologii w związku z zamieszczeniem formularza na platformie biznes.gov.pl

Okres przechowywania danych.

Będziemy przechowywać Państwa dane przez czas realizacji uprawnień Prezesa UODO wskazanych w art. 34 ust. 4 RODO i art. 58 ust. 2 RODO bądź art. 45 ust. 5 DODO, a następnie - zgodnie z obowiązującą w Urzędzie Prezesa UODO Instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów - przez okres 10 lat od końca roku, w którym zgłoszono naruszenie ochrony danych, lub - w przypadku skierowania wystąpienia lub wydania decyzji administracyjnej - wieczysto.

Prawa osób, których dane dotyczą.

Zgodnie z RODO przysługuje Państwu:

- a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
- b) prawo do sprostowania (poprawiania) swoich danych;
- c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
- d) prawo do ograniczenia przetwarzania danych;
- e) prawo do wniesienia skargi do Prezesa UODO (na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)

Informacja o wymogu podania danych.

Podanie przez Państwa danych osobowych w niniejszym formularzu jest obowiązkiem wynikającym z art. 33 ust. 3 RODO oraz z art. 63 § 2-3a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego.

¹ Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) oraz podjętych działań.

² Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości

PROCEDURA ZARZĄDZANIA INCYDENTAMI
CYBERBEZPIECZEŃSTWA
w Urzędzie Gminy Wiśniewo

W związku z realizacją wytycznych ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa w **Urzędzie Gminy Wiśniewo, Wiśniewo 86, 06-521 Wiśniewo** wprowadzona zostaje procedura mająca na celu prawidłowe wywiązywanie się z nałożonych obowiązków w zakresie cyberbezpieczeństwa w **Urzędzie Gminy Wiśniewo**, określająca zasady postępowania w chwili wystąpienia zagrożenia lub ataku, która przedstawia się następująco:

1. Do monitorowania przypadków mogących mieć negatywny wpływ na cyberbezpieczeństwo, wyznacza się w **Urzędzie Gminy Wiśniewo Pełnomocnika ds. bezpieczeństwa cyberprzestrzeni** w osobie: [REDACTED], przy czym każdy pracownik **Urzędu**, który zauważy wystąpienie zdarzeń (zachowań w obsługiwanych systemach) mogących wskazywać na ingerencję w system osób trzecich, zobowiązany jest zawiadomić **Wójta Gminy Wiśniewo**.
2. **Urząd Gminy Wiśniewo** zobowiązany jest do zgłoszenia osoby kontaktowej do CSIRT NASK. Zgłoszenie może być zrealizowane listownie lub poprzez stronę internetową: <https://incydent.cert.pl/osoba-kontaktowa#!/lang=pl,entityType=publicInstitution> (załącznik nr 1 do niniejszej Procedury)
3. **Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni** monitoruje w szczególności wystąpienie z poziomu Internetu i/lub domeny przypadków:
 - a) skanowania,
 - b) spamu przesyłanego za pośrednictwem polskich serwerów,
 - c) ataków typu DoS (Denial of Service) i DDoS (Distributed Denial of Service),
 - d) włamań i prób włamania.
4. **Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni** reaguje na każde zgłoszenie dokonane przez pracownika **Urzędu** dotyczące zdarzeń mogących wskazywać na cyberatak lub inną formę ingerencji w systemy eksploatowane w **Urzędzie**, która wskazuje na niekontrolowane działanie osób trzecich oraz weryfikuje zgłoszenie i podejmuje stosowne działania, o których mowa w pkt. 5.
5. Na podstawie opublikowanego raportu CERT Polska z 2018 roku (<https://www.cert.pl/news/single/zgloszenia-i-incydenty-w-2018-roku/>), wykaz incydentów, w tym incydentów występujących najczęściej ze szczegółowym

podziałem na poszczególne kategorie według klasyfikacji eCSIRT.net¹ przedstawia **tabela 1**.

6. Incydent w podmiocie publicznym – **Urząd Gminy Wiśniewo**, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego **Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni** zgłasza niezwłocznie:
 - a) **Wójtowi Gminy Wiśniewo**, w celu umożliwienia realizacji obowiązku wynikającego z art. 22 ust. 1 pkt 2 Ustawy o krajowym systemie cyberbezpieczeństwa tj. zgłoszenia incydentu niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV zawierającego informacje, o których mowa w **załączniku nr 2** do niniejszej Procedury.
 - b) Inspektorowi ochrony danych (**IOD**) w **Gminie Wiśniewo**, na adres poczty elektronicznej: [REDACTED] poprzez przesłanie wypełnionego formularza stanowiącego **załącznik nr 1** do niniejszej instrukcji oraz telefonicznie na numer kom: [REDACTED].
7. **IOD** dokonuje ustalenia czy zidentyfikowany incydent nie stanowi jednocześnie naruszenia ochrony danych osobowych, a w konsekwencji czy nie wymaga podjęcia stosownych działań w tym zakresie tj. oceny wagi ryzyka naruszenia praw i wolności osób fizycznych, oceny zasadności odnotowania incydentu w rejestrze incydentów i naruszeń, zgłoszenia naruszenia do PUODO, i/lub zawiadomienia osób fizycznych których dane dotyczą.
8. W przypadku uzasadnionych podejrzeń, iż doszło do incydentu cyberbezpieczeństwa **Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni** przygotowuje „Raport incydentu cyberbezpieczeństwa” stanowiący **załącznik nr 2** do niniejszej Procedury oraz odnotowuje zdarzenie w „Rejestrze incydentów cyberbezpieczeństwa” stanowiący **załącznik nr 3** do niniejszej Procedury.
9. Obowiązki podmiotów publicznych wynikające z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa przedstawia **załącznik nr 4** do niniejszej Procedury.

¹ Projekt współpracy zespołów CSIRT

Tabela 1. Wykaz incydentów w podziale na kategorie wg klasyfikacji eCSIRT.net

Obrażliwe i nielegalne treści	Spam
	Dyskredytacja, obrażanie
	Pornografia dziecięca, przemoc
	Niesklasyfikowane
Złośliwe oprogramowanie	Wirus
	Robak sieciowy
	Koń trojański
	Oprogramowanie szpiegowskie
	Dialer
	Rootkit
	Niesklasyfikowane
Gromadzenie informacji	Skanowanie
	Podśluch
	Inżynieria społeczna
	Niesklasyfikowane
Próby włamań	Wykorzystanie znanych luk systemowych
	Próby nieuprawnionego logowania
	Wykorzystanie nieznanых luk systemowych
	Niesklasyfikowane
Włamania	Włamanie na konto uprzywilejowane
	Włamanie na konto zwykłe
	Włamanie do aplikacji
	Bot
	Niesklasyfikowane
Dostępność zasobów	Atak blokujący serwis (DoS)
	Rozproszony atak blokujący serwis (DDoS)
	Sabotaż komputerowy
	Przerwa w działaniu usług (niezłośliwe)
	Niesklasyfikowane
Atak na bezpieczeństwo informacji	Nieuprawniony dostęp do informacji
	Nieuprawniona zmiana informacji
	Niesklasyfikowane
Oszustwa komputerowe	Nieuprawnione wykorzystanie zasobów
	Naruszenie praw autorskich
	Kradzież tożsamości, podszycie się
	Phishing
	Niesklasyfikowane
Podatne usługi	Otwarte serwisy podatne na nadużycia
	Niesklasyfikowane
inne	...

Załącznik nr 1

Zgłaszanie osób kontaktowych do CSIRT NASK

Obowiązkowi zgłoszenia osób kontaktowych właściwemu CSIRT podlegają wg ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) **operatorzy usług kluczowych** (art 9 ust 1) oraz **podmioty publiczne** (art 22 ust 1 pkt 5).

Jeżeli chcą Państwo zgłosić incydent proszę użyć poniższego odnośnika:

Zgłaszanie incydentu do CSIRT NASK.

Aby zgłosić osoby kontaktowe do CSIRT NASK lub zaktualizować ich dane należy:

- wypełnić poniższy formularz,
- wygenerowane pismo opatrzyć podpisem, elektronicznym lub tradycyjnym kierownika instytucji,
- przesłać pismo na skrzynkę ePUAP (Naukowa i Akademicka Sieć Komputerowa PIB; adres skrzynki: /NASK-Instytut/SkrytkaESP, w tytule proszę wpisać "Zgłoszenie osoby kontaktowej do CSIRT NASK") lub na adres NASK-PIB wskazany w dokumencie (w przypadku operatora usługi kluczowej załączając skan decyzji administracyjnej uznającej podmiot za operatora usługi kluczowej).

Przed wypełnieniem poniższego formularza polecamy zapoznać się ze wspólnymi rekomendacjami CSIRT NASK oraz CSIRT GOV w zakresie wyznaczania osób kontaktowych.

Zgłoszenie osoby kontaktowej – Jaki podmiot Państwo reprezentują?

 Operator usługi kluczowej Wypełnienie obowiązku wynikającego z art 9 ust 1 ustawy o KSC	 Podmiot publiczny Wypełnienie obowiązku wynikającego z art 22 ust 1 pkt 5 ustawy o KSC	 Inny podmiot Dobrowolne zgłoszenie niezobowiązanego podmiotu
---	--	--

Prosimy o wypełnienie poniższego formularza

Dane podmiotu zgłaszającego
Pełna nazwa instytucji |
Nazwa skrócona |

☐ Czy reprezentowany przez Państwa podmiot publiczny jest jednocześnie operatorem usługi kluczowej?

NIP

Numer REGON

Numer KRS

Ogólny adres e-mail

Adres siedziby (ulica, numer budynku, numer lokalu)

Kod pocztowy siedziby

Miasto siedziby

Informacje o zakresie sieciowym

Adres e-mail, na który mają być wysyłane informacje o nowych zdarzeniach wykrytych w Państwa sieci

Numer systemu autonomicznego lub adresy sieci w notacji CIDR (po jednym w linii)

Nazwy domen należących do Państwa instytucji (po jednej w linii)

Osoby kontaktowe

Przynajmniej jedna osoba musi być uplasowana w wewnętrznych strukturach odpowiedzialnych za cyberbezpieczeństwo.

Umieszczenie osoby kontaktowej

☐ Wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo

☐ Zewnętrzny podmiot świadczący usługi z zakresu cyberbezpieczeństwa

Imię i nazwisko

Stanowisko lub funkcja

Adres e-mail

Numer telefonu

Dostępność

8-16

8-22

24h

Jednostki organizacyjne

Zgodnie z art 21 pkt 3 ustawy o KSC, "jednostka samorządu terytorialnego może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne".

Nazwa jednostki organizacyjnej	
Pełny adres jednostki organizacyjnej	
Informacje dodatkowe	
Informacje dodatkowe	

Załączniki i wysyłanie zgłoszenia

Dołączenie plików lub wysłanie formularza jest możliwe po kliknięciu "Nie jestem robotem" poniżej.

Załącznik nr 2

RAPORT INCYDENTU CYBERBEZPIECZEŃSTWA

I. WSTĘPNY OPIS INCYDENTU

1. Data Godzina
2. Osoba powiadamiająca o incydencie oraz inne osoby zaangażowane lub odpytane w związku z incydem (imię, nazwisko, stanowisko służbowe, dane kontaktowe):
.....
3. Lokalizacja zdarzenia (*nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.*):
.....

II. WSTĘPNA ANALIZA INCYDENTU

4. Zadanie publiczne, którego dotyczy zgłoszenie:
.....
5. Liczba osób, na które incydent miał wpływ
.....
6. Moment wystąpienia i wykrycia incydemu oraz czas jego trwania
.....
7. Zasięg geograficzny obszaru, którego incydent dotyczy
.....
8. Przyczyna zaistnienia incydemu:

☐ Podejrzana wiadomość e-mail	☐ Podatności
☐ Próba oszustwa	☐ Złośliwe oprogramowanie
☐ Nielegalne treści	☐ Inny
9. Źródło incydemu
.....
10. Sposób jego przebiegu
.....
11. Skutki jego oddziaływania na systemy informacyjne podmiotu publicznego
.....
12. Informacja o podjętych działaniach zapobiegawczych
.....

13. Informacja o podjętych działaniach naprawczych - jeśli charakter incydentu pozwala podjąć je od razu.

14. Czy doszło do naruszenia danych osobowych

☐ TAK

☐ NIE

W przypadku naruszenia danych osobowych należy dodatkowo uruchomić procedurę zgłaszania naruszeń związanych z ochroną danych osobowych.

W przypadku naruszenia danych osobowych podać nr zgłoszenia z rejestru incydentów -
.....

.....
(podpisy osób obsługujących incydent)

** Do Raportu należy dołączyć kopię zgłoszenia do CSIRT NASK.*

REJESTR INCYDENTÓW CYBERBEZPIECZEŃSTWA
w Urzędzie Gminy Wiśniewo

Lp.	Data zgłoszenia	Zadanie publiczne, którego dotyczy zgłoszenie	Opis zdarzenia	Kategoria incydentu	Podjęte działania zapobiegawcze	Podjęte działania naprawcze
1	2	3	4	5	6	7
1.						
2.						
3.						
4.						
5.						
6.						

Kategorie incydentu (kolumna nr 7):

A – Podejrzana wiadomość e-mail B – Próba oszustwa

C – Podatności

D – Złośliwe oprogramowanie E – Nielegalne treści

F - Inny incydent

Załącznik nr 4

Wyciąg z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Rozdział 5

Obowiązki podmiotów publicznych

Art. 21.

1. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
2. Organ administracji publicznej może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki jemu podległe lub przez niego nadzorowane.
3. Jednostka samorządu terytorialnego może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne.

Art. 22.

1. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego:
 - 1) zapewnia zarządzanie incydem w podmiocie publicznym;
 - 2) zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
 - 3) zapewnia obsługę incydem w podmiocie publicznym i incydem krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;
 - 4) zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;
 - 5) przekazuje do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby, o której mowa w art. 21, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.
2. Zgłoszenie, o którym mowa w ust. 1 pkt 2, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

Art. 23.

1. Zgłoszenie, o którym mowa w art. 22 ust. 1 pkt 2, zawiera:

- 1) dane podmiotu zgłaszającego, w tym nazwę podmiotu, numer we właściwym rejestrze, siedzibę i adres;
 - 2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby składającej zgłoszenie;
 - 3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
 - 4) opis wpływu incydem w podmiocie publicznym na realizowane zadanie publiczne, w tym:
 - a) wskazanie zadania publicznego, na które incydent miał wpływ,
 - b) liczbę osób, na które incydent miał wpływ,
 - c) moment wystąpienia i wykrycia incydem oraz czas jego trwania,
 - d) zasięg geograficzny obszaru, którego dotyczy incydent,
 - e) przyczynę zaistnienia incydem i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;
 - 5) informacje o przyczynie i źródle incydem;
 - 6) informacje o podjętych działaniach zapobiegawczych;
 - 7) informacje o podjętych działaniach naprawczych;
 - 8) inne istotne informacje.
2. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydem w podmiocie publicznym.

