Załącznik do Zarządzenie Nr 19/2022
Burmistrza Gminy i Miasta Gryfów Śląski
z dnia 22 lutego 2022 r.

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

URZĄD GMINY I MIASTA W GRYFOWIE ŚLĄSKIM

RYNEK 1, 59-620 GRYFÓW ŚLĄSKI

SPIS TREŚCI

ROZDZIAŁ I

Postanowienia ogólne

§ 1

Podstawa prawna

Niniejszy System Zarządzania Bezpieczeństwem Informacji został sporządzony na podstawie międzynarodowych standardów bezpieczeństwa informacji i jest zgodny z obowiązującymi normami prawnymi, w szczególności z:

1. Konstytucją Rzeczypospolitej Polskiej (Dz.U. Nr 78, poz. 483), zwaną dalej „Konstytucja RP”;
2. Rozporządzeniem 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. Urz. UE L 119 z 2016 r.), zwanym dalej: „RODO”;
3. Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r.poz. 1781), zwana dalej: „ustawa uodo”;
4. Ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2019 r. poz. 742), zwana dalej: „ustawa o informacjach niejawnych”;
5. Ustawą z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2020 r. poz. 1913), zwana dalej: „ustawą znk”;
6. Ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2020 r. poz. 2176), zwana dalej: „dostęp do informacji publicznej”;
7. Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 poz. 1369), zwana dalej: „ustawa o cyberbezpieczeństwie”;
8. Rozporządzeniem 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 (Dz.U. z 2017 r. poz. 2247), zwane dalej: „rozporządzenie KRI”;
9. Normą ISO/IEC 27001, zwana dalej: „norma ISO”.

§ 2

Cel SZBI

Celem wdrożonego Systemu Zarządzania Bezpieczeństwa Informacji w Urzędzie Gminy i Miasta w Gryfowie Śląskim w skrócie „SZBI" jest zapewnienie zachowania poufności, integralności i dostępności informacji w wyniku stosowania procesu zarządzania ryzykiem, a także:

1. Zagwarantowania właściwej ochrony informacji, w tym odpowiedniego poziomu bezpieczeństwa informacji bez względu na jakim nośniku została ona zapisana;
2. Zapewnienia ciągłości procesów przetwarzania informacji;
3. Ograniczenia występowania zagrożeń dla bezpieczeństwa informacji;
4. Zapewnienia właściwego funkcjonowania wszystkich systemów informatycznych;
5. Właściwego reagowania na incydenty bezpieczeństwa informacji.

§ 3

Skład SZBI

System Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy i Miasta Gryfów Śląski zapewnia kompleksową regulację w zakresie bezpieczeństwa informacji, w której skład wchodzą następujące dokumenty:

1. **Polityka Ochrony Danych Osobowych** wprowadzona Zarządzeniem nr 96/2019 Burmistrza Gminy i Miasta Gryfów Śląski z dnia 10 października 2019 r.
2. **Plan Ochrony Informacji Niejawnych** wprowadzony Zarządzeniem nr 18/2022 Burmistrza Gminy i Miasta Gryfów Śląski z dnia 18 lutego 2022 r.
3. **Polityka Bezpieczeństwa Informacji** wprowadzona w rozdziale II niniejszego dokumentu jakim jest System Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy i Miasta Gryfów Śląski.

§ 4

Zasady postępowania z określonymi informacjami

W Urzędzie Gminy i Miasta w Gryfowie Śląskim poszczególne informacje są chronione na podstawie przepisów prawa. W oparciu o wymagania prawne nakładane na ochronę aktywów

informacyjnych dokonano podziału na właściwe klasy chronionych informacji. Najważniejsze grupy informacji objęte wymaganiami to:

1. Dane osobowe.
2. Informacje niejawne.
3. Informacje objęte tajemnicą skarbową.
4. Informacje publiczne.
5. Informacje finansowe.
6. Informacje stanowiące tajemnice przedsiębiorstwa, w szczególności informacje występujące w umowach zawartych z dostawcami usług zewnętrznych.

ROZDZIAŁ II

Polityka Bezpieczeństwa Informacji - PBI

§ 5

Podejście do bezpieczeństwa informacji

Podejście do bezpieczeństwa informacji w Urzędzie Gminy i Miasta w Gryfowie Śląskim zostało oparte na kluczowych regułach dla funkcjonowania organizacji w zakresie zarządzania szeroko pojętym aktywem jakim jest informacja.

1. **Reguła poufności informacji** - zapewniająca, że informacja jest udostępniana jedynie osobom upoważnionym do jej przetwarzania.
2. **Reguła integralności informacji** - zapewniająca zupełną dokładność i kompletność informacji oraz metod jakimi jest ona przetwarzana.
3. **Reguła dostępności informacji** - zapewniająca, że osoby upoważnione do przetwarzania posiadają dostęp do oznaczonej informacji wówczas, gdy istnieje taka potrzeba.

§ 6

Bezpieczeństwo organizacyjne

1. Dostęp do aktywów oraz zasobów informacyjnych w Urzędzie Gminy i Miasta w Gryfowie Śląskim jest realizowany za pomocą zatwierdzonych sposobów postępowania oraz mechanizmów kontrolnych w obszarach fizycznego dostępu do informacji oraz danych przetwarzanych w systemach informatycznych zastosowanych w Urzędzie.

2. Procedura bezpiecznego postępowania z kluczami dostępu do pomieszczeń w Urzędzie Gminy i Miasta w Gryfowie Śląskim stanowi załącznik nr 1 do Systemu Zarządzania Bezpieczeństwem Informacji.

§ 7

Odpowiedzialność za aktywa

1. Odpowiedzialność za aktywa w postaci informacji oraz urządzeń i kluczy dostępu spoczywa na każdym z zobowiązanych uczestników SZBI. Ponadto odpowiedzialność za bezpieczeństwo informacji spoczywa na każdym uczestniczącym w procesie przetwarzania informacji na mocy udzielonego upoważnienia do przetwarzania danych osobowych oraz regulacji wynikających z przetwarzania informacji niejawnych w Urzędzie Gminy i Miasta w Gryfowie Śląskim.
2. Oświadczenie o zapoznaniu pracownika z Systemem Zarządzania Bezpieczeństwem Informacji stanowi załącznik nr 2 do Systemu Zarządzania Bezpieczeństwem Informacji.

§ 8

Analiza ryzyka bezpieczeństwa informacji

Szacowanie ryzyka dla bezpieczeństwa informacji przetwarzanych w Urzędzie Gminy i Miasta Gryfów Śląski zostało określone w załączniku nr 3 do Systemu Zarządzania Bezpieczeństwem Informacji. Analiza ryzyka dokonywana jest przy wykorzystaniu ryzyk określonych w polityce ochrony danych osobowych z uwzględnieniem ryzyk dla bezpieczeństwa informacji wskazanych w powyżej wymienionym załączniku.

§ 9

Organizacja bezpieczeństwa informacji przy pracy
z wykorzystaniem urządzeń mobilnych

Wykorzystanie urządzeń mobilnych w Urzędzie Gminy i Miasta w Gryfowie Śląskim kompleksowo reguluje procedura w postaci regulaminu korzystania z urządzeń mobilnych stanowiącego załącznik nr 4 do Systemu Zarządzania Bezpieczeństwem Informacji.

§ 10

Bezpieczeństwo określonych informacji

1. Dane osobowe – w przypadku informacji stanowiących dane osobowe należy każdorazowo odnieść się do zapisów wdrożonej polityki ochrony danych osobowych oraz procedur z niej wynikających.
2. Informacje niejawne – stanowią wszelkie informacje, dla których przetwarzania ustanowiono plan ochrony informacji niejawnych.
3. Informacje publiczne – informacje podlegające ochronie do momentu ich upublicznienia przez Urząd Gminy i Miasta w Gryfowie Śląskim. Dostęp do informacji publicznych pozostaje ograniczony w zakresie prawnie chronionych informacji, których ochrona wynika bezpośrednio z przepisów obowiązującego prawa. Upublicznieniu mogą podlegać jedynie informacje, które zostały podane uprzedniej analizie udostępnienia. Informacje w postaci potencjalnych podatności, incydentów, zagrożeń dla cyberbezpieczeństwa oraz ryzyku wystąpienia incydentów nie podlegają udostępnieniu w trybie ustawy o dostępie publicznym zgodnie z art. 37 ust. 1 ustawy o cyberbezpieczeństwie.
4. Informacje objęte tajemnicą skarbową – informacje chronione na mocy art. 293 ustawy z dnia 29 sierpnia 1993 r. Ordynacja podatkowa.
5. Informacje finansowe – informacje chronione na mocy art. 99 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.
6. Informacje stanowiące tajemnice przedsiębiorstwa – informacje należy przetwarzać zgodnie z przepisami o zwalczaniu nieuczciwej konkurencji, przepisami o dostępie do informacji publicznej, warunkami umowy lub porozumienia, w szczególności wymaganiami określonymi w zapisach umownych dotyczących zachowania poufności.

§ 11

Bezpieczeństwo w relacji z dostawcami usług zewnętrznych

Umowy zawierane z firmami świadczącymi usługi zewnętrzne, powinny zawierać zapisy odnośnie kwestii bezpieczeństwa informacji z szczególnym uwzględnieniem ochrony danych osobowych w przypadku niezbędności ich przetwarzania przy realizacji umowy.

1. Zapisy umowy powierzenia wynikają wprost z polityki ochrony danych osobowych przyjętej w Urzędzie Gminy i Miasta w Gryfowie Śląskim.

2. Należy stosować zapisy zobowiązujące do zachowania w poufności informacji ujawnionych w ramach realizacji poszczególnych umów.

§ 12

Zarządzanie incydentami bezpieczeństwa informacji

Wystąpienie incydentu informatycznego spowodowanego ingerencją podmiotu zewnętrznego w systemy mające zastosowanie w Urzędzie Gminy i Miasta w Gryfowie Śląskim powoduje konieczność podjęcia zgłoszenia do krajowego zespołu reagowania na incydenty bezpieczeństwa komputerowego pod adresem e-mail: cert@cert.pl przy pomocy formularza online dostępnego na stronie internetowej: https://incydent.cert.pl

1. Osobą odpowiedzialną za dokonanie zgłoszenia jest pracownik na stanowisku do spraw informatyzacji urzędu, wyznaczony w Urzędzie Gminy i Miasta w Gryfowie Śląskim.
2. Zgłoszenie należy dokonać w terminie nie późniejszym, aniżeli w ciągu 24 godzin od momentu wykrycia incydentu.
3. Zgłoszenie incydentu bezpieczeństwa informatycznego do CERT Polska, nie zwalnia z obowiązku zgłoszenia naruszeń wynikających z wdrożonej w Urzędzie Gminy i Miasta w Gryfowie Śląskim dokumentacji z zakresu ochrony danych osobowych czy informacji niejawnych.

§ 13

Plan ciągłości działania

Celem planu ciągłości działania jest minimalizacja zakłóceń w trakcie realizacji działalności przez Urząd Gminy i Miasta w Gryfowie Śląskim w związku z sytuacją ingerującą bezpośrednio na prawidłowość pracy jednostki.

1. Zaistnienie dysfunkcji systemu informatycznego uniemożliwiającego dalszą pracę w systemie powoduje odniesienie się do zdefiniowanych działań koniecznych do podjęcia w danym przypadku, określonych w poniższej tabeli:

Lp.	Funkcja	Opis działań	Zasoby
1.	Weryfikacja zasadności zgłoszenia od użytkownika.	Weryfikacja, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego.	- dostęp do infrastruktury informatycznej na stanowisku, skąd pochodzi zgłoszenie.
2.	Ustalenie źródła awarii.	Ustalenie, co jest przyczyną awarii: - przerwa w zasilaniu prądem, - brak połączenia z siecią Internet, - wadliwe działanie sprzętu, - wadliwe działanie aplikacji, - wadliwe działanie systemu, na którym uruchomiona jest aplikacja.	- dostęp do serwerowni oraz do sprzętu, który uległ awarii, - kontakt z osobą, która może w porze nocnej pobrać klucze od ośrodka, - w przypadku zablokowania zamka wezwać ślusarza, - w przypadku awarii zasilania elektrycznego wezwać elektryka.
3.	Określenie skali awarii.	Ustalenie, czy awaria powoduje zatrzymanie pracy: - jednego pomieszczenia pracy lub działu (od 1 do 10 osób); - kilku wydziałów; - całego budynku jednostki.	- kontakt z kluczowymi pracownikami działów oraz listę z numerami telefonów.
4.	Ustalenie czy wznawianie usługi może odbywać się w dotychczasowej lokalizacji.	Działanie ma na celu zweryfikowanie, czy wznawiane usługi uruchamiane będą w dotychczasowej lokalizacji, czy w lokalizacjach alternatywnych.	- możliwość uruchomienia dowolnych usług w lokalizacji, - infrastrukturę sieciową, zasilanie prądem.
5.	Zakup niezbędnych elementów wyposażenia, dokonanie naprawy bądź wymiany urządzeń, uruchomienie aplikacji.	W przypadku braku możliwości zakupu należy znaleźć rozwiązanie alternatywne (np. zdecydować o przeniesieniu aplikacji na stałe na inny serwer).	- środki na zakup elementów niezbędnych do ponownego uruchomienia systemu.
6.	Weryfikacja możliwości przeniesienia aplikacji na inny serwer.	Sprawdzenie, czy aplikacja może być uruchomiona na którymś z działających poprawnie w jednostce serwerów.	- dostęp do alternatywnego serwer.
7.	Przygotowanie serwera zastępczego.	Serwerem zastępczym można ustanowić np. komputer typu stacja robocza, który należy odpowiednio skonfigurować. Po uruchomieniu aplikacji na serwerze zastępczym należy przetestować jej działanie.	- maszynę dowolnego typu, która w podstawowym zakresie pozwoli na uruchomienie podstawowych usług.
8.	Podjęcie decyzji o terminie odtworzenia maszyny.	W razie konieczności należy skontaktować się z kluczowymi pracownikami wydziałów.	- kontakt z kluczowymi pracownikami wydziałów Urzędu Gminy i Miasta w Gryfowie Śląskim.
9.	Przywrócenie funkcjonowania systemu.	Usunięcie przyczyny nieprawidłowego działania systemu. W razie konieczności należy odtworzyć aplikację korzystając z kopii zapasowych.	- dostęp do najbardziej aktualnej wersji aplikacji, - dostęp do aktualnej bazy danych.
10.	Sprawdzenie systemu bądź aplikacji.	Przeniesienie bądź uruchomienie należy potwierdzić weryfikacją prawidłowego funkcjonowania systemów zainstalowanych na serwerze bądź aplikacji.	- dostęp do serwera i stacji roboczych.
11.	Uruchomienie usługi w systemie informatycznym Urzędu Gminy i Miasta w Gryfowie Śląskim.	Uruchomienie usługi należy zakomunikować zainteresowanym użytkownikom jednostki.	- kontakt z kluczowymi pracownikami wydziałów Urzędu Gminy i Miasta w Gryfowie Śląskim.

2. Osobą odpowiedzialną za funkcjonowanie planu ciągłości działania pozostaje Sekretarz przy udziale Informatyka.
3. Test planu ciągłości działania polega na wykonaniu symulacji wyłączenia serwera danej aplikacji, uniemożliwiając tym samym możliwość wykonywania usług. Rezultatem oczekiwanym testu jest możliwość wznowienia działania usługi na nowej maszynie. Symulacji należy dokonać z udokumentowaniem czynności w protokole, którego wzór stanowi załącznik nr 5 do niniejszego Systemu Zarządzania Bezpieczeństwem Informacji.
4. Zakłócenia działalności mogące wystąpić w wyniku klęski żywiołowej na wypadek, której zostało ustanowione postępowanie w rozdziale 6 wdrożonej polityki ochrony danych osobowych w Urzędzie Gminy i Miasta w Gryfowie Śląskim.

ROZDZIAŁ III

Tabela zmian Systemu Zarządzania Bezpieczeństwa Informacji (SZBI)

Lp.	Paragraf/punkt	Data wprowadzonej zmiany	Opis dokonanej zmiany w SZBI