Zarządzenie nr 46.2021

Wójta Gminy Białowieża

z dnia 28 października 2021

w sprawie wprowadzenia Instrukcji Obsługi Systemu Informatycznego

w Urzędzie Gminy Białowieża

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2021 r. poz. 1372) oraz 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 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 (Dz.U. 2012 poz. 526) zarządza się, co następuje:

§1

Wprowadza się w **Urzędzie Gminy Białowieża** Instrukcję Obsługi Systemu Informatycznego wydanie 3.

§2

Zarządzenie jest adresowane do pracowników **Urzędu Gminy Białowieża** wykonujących czynności określone w przyjmowanych procedurach. Każdy pracownik, zgodnie z wykazem, jest obowiązany zapoznać się z treścią Instrukcji Obsługi Systemu Informatycznego.

§3

Wójt Gminy Białowieża, zobowiązuje wszystkich pracowników Urzędu Gminy Białowieża do przestrzegania zapisów Instrukcji Obsługi Systemu Informatycznego.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT

inż. Albert Waldemar Litwiniuk

.....

(podpis)

Instrukcja obsługi systemu informatycznego

URZĄD GMINY BIAŁOWIEŻA

Tytuł dokumentu	**Instrukcja Obsługi Systemu Informatycznego**		
Wydanie	3	Opracował	Anna Predko-Maliszewska
Data opracowania	28.10.2021	Zatwierdził	Albert Waldemar Litwinowicz

1. WSTĘP

Niniejsza instrukcja stanowi zestaw procedur opisujących zasady postępowania i zabezpieczania danych osobowych przetwarzanych w zbiorach papierowych i w systemach informatycznych.

2. ZABEZPIECZENIA FIZYCZNE

1. Zabezpieczono dostęp do kluczowej infrastruktury w postaci budynków / pomieszczeń biurowych / archiwów / serwerowni, miejsc przechowywania kopii bezpieczeństwa.
2. Obiekt chroniony jest poprzez system alarmowy.
3. Stosowany jest monitoring wizyjny.
4. Dostęp do archiwum zabezpieczony jest drzwiami zamykanymi na klucz.
5. Opracowana i wdrożona została polityka kluczy.
6. Wdrożono zasadę dostępu osób nieupoważnionych do miejsc przetwarzania danych wyłącznie w obecności osoby upoważnionej.
7. Do drukarek / urządzeń kopiujących stosuje się system PIN'ów dostępowych.
8. Dostęp do dokumentacji / danych w pomieszczeniach zabezpieczono w zamkniętych szafach.
9. Składowanie dokumentacji papierowej w archiwum na podwyższeniu.
10. Wdrożono strefy ograniczonego dostępu.

3. ZAPIECZENIA TECHNICZNE

1. Zastosowano UPS podtrzymujący zasilanie serwera oraz kluczowych elementów systemu IT.
2. Serwerownie wyposażone są w gaśnice.
3. W serwerowniach zastosowano klimatyzację.
4. Obiekt chroniony jest poprzez system alarmowy.

4. ZAPIECZENIA ORGANIZACYJNE

1. Opracowano i wdrożono politykę ochrony danych osobowych.
2. Opracowano i wdrożono instrukcję zarządzania systemem informatycznym.
3. Opracowano i wdrożono procedurę nadawania upoważnień do przewarzania danych osobowych.
4. Opracowano i wdrożono procedurę nadawania upoważnień do pracy w systemach informatycznych.

5. PROCEDURY ZARZĄDZANIA UPRAWNIENIAMI W SYSTEMACH INFORMATYCZNYCH I PRZETWARZANIA DANYCH OSOBOWYCH

Procedura opisuje zasady: przyznawania, modyfikacji i cofania uprawnień użytkownika do przetwarzania zbiorów w systemie informatycznym lub w wersji papierowej. Celem procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych poufnych, utraty ich poufności oraz integralności.

5.1. PROCEDURA NADANIA UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Za nadawanie/modyfikację/anulowanie upoważnień do przetwarzania danych osobowych odpowiada ADO.
2. Nadawanie/modyfikację/anulowanie upoważnień odbywa się w oparciu o **załącznik 02a – upoważnienie do przetwarzania danych osobowych.**
3. Przed nadaniem upoważnienia pracownik musi być zapoznany z polityką ochrony danych osobowych.
4. Potwierdzenie zapoznania z przyjętą polityką ochrony danych osobowych wymaga formy pisemnej zgodnie z **załącznikiem nr 01d - Oświadczenie o poufności**.
5. DPO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych zgodnie z **załącznikiem nr 02b – ewidencja osób upoważnionych**.

5.2. PRZYZNANIE, MODYFIKACJA, COFANIE UPRAWNIEŃ DO PRACY W SYSTEMIE INFORMATYCZNYM

1. Upoważnienie do pracy w systemie informatycznym nadawane jest przez ADO zgodnie z **załącznikiem nr 02d**.
2. ASI nadaje uprawnienia zgodnie z zakresem określonym zakresem w **załączniku nr 02d**.
3. ASI prowadzi rejestr użytkowników systemów informatycznych zgodnie z **załącznikiem 02c – wykaz użytkowników systemów informatycznych**.
4. Każdy użytkownik w systemie informatycznym musi posiadać swój własny, indywidualny identyfikator (login). Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
5. Przy nadawaniu uprawnień do pracy w systemie obowiązuje zasada minimalizacji uprawnień.
6. ADO jest zobowiązany do zlecenia cofnięcia uprawnieniń w systemie informatycznym po ustaniu stosunku zatrudnienia z pracownikiem (**załącznik nr 02d**).
7. ADO jest zobowiązany do zlecenia modyfikacji uprawnieniń w systemie informatycznym w związku z zmianą obowiązków pracownika (**załącznik nr 02d**).

5.3. Uprawnienia szczególne DPO

1. W sytuacji naruszenia bezpieczeństwa danych DPO może zlecić natychmiastową modyfikację nadanych uprawnień lub zawieszenie konta.
2. O tym fakcie DPO niezwłocznie poinformuje ADO.

6. STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

6.1. OGÓLNE ZASADY POSTĘPOWANIA Z HASŁAMI

1. Po utworzeniu konta użytkownika w systemie ASI przekazuje, w sposób poufny, upoważnionemu użytkownikowi hasło pierwszego logowania do systemu.
2. Hasło może być przekazane w postaci wydruku, poprzez SMS, ustnie.
3. Hasło musi być przekazane innym kanałem niż pozostałe dane niezbędne do uwierzytelnienia.

4. Jeśli system nie wymusi zmiany hasła pierwszego logowania, użytkownik zobowiązany jest do niezwłocznej zmiany tego hasła.
5. Hasło powinno się składać z minimum 8 znaków, zawierać małe i duże litery, cyfry lub znaki specjalne.
6. Hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury.
7. Hasło nie może być jednakowe z identyfikatorem użytkownika.
8. Hasło nie może być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
9. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
10. Zabronione jest przekazywanie innym użytkownikom danych dostępowych (loginu i hasła).
11. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
12. W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie ASI oraz DPO.
13. Hasło powinno być zmieniane nie rzadziej niż co 6 miesięcy. Jeśli dany system informatyczny nie wymusza hasła, użytkownik jest zobowiązany do samodzielnej zmiany hasła co 6 miesięcy.

6.2. HASŁA DO SYSTEMÓW OPERACYJNYCH

1. Z hasłami uwierzytelniającymi w systemach operacyjnych należy postępować w sposób opisany w punkcie „Ogólne zasady postępowania z hasłami".

6.3. HASŁA DO APLIKACJI PRZETWARZAJĄCYCH DANE OSOBOWE

1. Z hasłami do aplikacji przetwarzających dane osobowe należy postępować w sposób opisany w punkcie „Ogólne zasady postępowania z hasłami".

7. PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

7.1. PROCEDURA ROZPOCZĘCIA PRACY

1. Przed rozpoczęciem pracy użytkownik powinien dokonać oględzin stanowiska pracy pod kątem możliwego dostępu do stanowiska osób trzecich. Jeśli wystąpią podejrzenia, iż doszło do ingerencji osób trzecich należy powiadomić ASI. Szczególną uwagę należy zwrócić na to czy w portach USB nie są umieszczone nośniki danych.
2. W celu rozpoczęcia pracy z systemem informatycznym użytkownik musi posłużyć się identyfikatorem oraz hasłem. Zabrania się pracy wielu użytkowników na wspólnym koncie.
3. Jeśli system sygnalizuje o próbach logowania osoby nieupoważnionej użytkownik jest zobowiązany do powiadomienia o tym fakcie ASI.

4. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi.
5. W celu redukcji ryzyka nieautoryzowanego i nieuprawnionego dostępu do danych należy stosować politykę czystego ekranu polegającą na uniemożliwieniu osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach komputerowych.

7.2. PROCEDURA ZAWIESZENIA PRACY

1. W przypadku chwilowego opuszczenia stanowiska pracy użytkownik zobowiązany jest uruchomić wygaszacz ekranu blokowany hasłem (skrót klawiaturowy w systemach Windows: ⊞ + L) lub wylogować się z konta użytkownika. Jeśli użytkownik nie wykona tej czynności system po upływie 5 minut nieaktywności użytkownika powinien automatycznie aktywować wygaszacz ekranu.

7.3. PROCEDURA ZAKOŃCZENIA PRACY

1. Kończąc pracę użytkownik zobowiązany jest do:
   a) zamknięcia wszystkich aplikacji;
   b) zamknięcia systemu operacyjnego;
   c) wyłączenia stacji roboczej / laptopa;
   d) wyłączenia listwy zasilającej.
2. Przed opuszczeniem stanowiska pracy należy zabezpieczyć nośniki danych, wydruki i inne dokumenty znajdujące się na stanowisku pracy.

7.4. WZNOWIENIE PRACY PO AWARII

1. W sytuacji nagłego przerwania pracy (np. będącego wynikiem zaniku napięcia) użytkownik jest zobowiązany do sprawdzenia czy nie doszło do utraty danych w aplikacjach, które były użytkowane przed wystąpieniem sytuacji awaryjnej.
2. W przypadku zaistnienia podejrzenia utraty danych lub uszkodzenia stacji roboczej użytkownik zobowiązany jest niezwłocznie powiadomić ASI.

8. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ WYDRUKÓW

8.1. ZABEZPIECZENIE ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

1. Nośniki danych, płyty CD/DVD, pendrive, itd., należy przechowywać w sposób uniemożliwiający dostęp osób nieuprawnionych.
2. Po zakończeniu pracy z nośnikiem danych należy zamknąć go w zamykanej na klucz szafce lub biurku.

3. Nośniki powinny być chronione przed działaniem czynników takich jak: pożar, zalanie, pola elektromagnetyczne (np. głośniki), zbyt niska lub zbyt wysoka temperatura.
4. Bez wiedzy i zgody ADO nie można kopiować na nośniki danych informacje zawierające jakiekolwiek dane osobowe lub inne poufne dane dotyczące UG Białowieża.
5. Bez wiedzy ADO nie można wynosić poza obszar UG Białowieża nośniki zawierające dane osobowe oraz dane poufne.
6. W przypadku wynoszenia poza obszar UG Białowieża nośników zawierających dane należy je uprzednio zaszyfrować.
7. W sytuacji przekazywania (przesyłania) nośników z danymi osobowymi poza obszar UG Białowieża należy stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce;
    b. dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą;
    c. należy stosować bezpieczne koperty depozytowe;
    d. przesyłkę należy przesyłać przez kuriera.
8. Użytkownik jest zobowiązany do niezwłocznego, trwałego usuwana danych z nośników po ustaniu okresu ich przydatności.
9. Nośniki, które nie będą już wykorzystywane należy niszczyć w sposób trwały.
10. Przed przekazaniem sprzętu informatycznego poza UG Białowieża (np. sprzedaż, darowizna, utylizacja) należy zdemontować nośniki (dyski twarde z komputerów i drukarek) lub wyczyścić specjalistycznym oprogramowaniem.

8.2. ZABEZPIECZENIE DOKUMENTÓW I WYDRUKÓW

1. Zbędne wydruki i dokumenty zawierające dane osobowe oraz dane poufne powinny być niezwłocznie zniszczone po ustaniu czasu ich przydatności.
2. W celu redukcji ryzyka nieautoryzowanego i nieuprawnionego dostępu lub uszkodzenia danych osobowych znajdujących się na wydrukach należy stosować politykę czystego biurka polegającą na zamykaniu dokumentów w szafkach oraz biurkach podczas nieobecności w pomieszczeniu lub zakończeniu pracy. Ponadto należy zadbać o to, by osoby trzecie nie miały możliwości wglądu w zawartość dokumentów znajdujących się na stanowisku pracy.
3. Dokumenty i wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.
4. Zabrania się pozostawiania wydruków oraz ksero na drukarkach, skanerach i kserokopiarkach bez nadzoru.
5. Wydruki powinny być niezwłocznie zabierane z podajnika drukarki.
6. Do niszczenia dokumentów zawierających dane osobowe należy wykorzystywać niszczarki.
7. Kserokopiarki, drukarki oraz niszczarki muszą być zabezpieczone przed dostępem osób trzecich.
8. Za zapewnienie bezpieczeństwa dokumentów i wydruków odpowiedzialni są kierownicy właściwych jednostek lub komórek organizacyjnych oraz podległe im osoby przetwarzające dane, w tym dane osobowe.

9. ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

9.1. OCHRONA ANTYWIRUSOWA

1. Przez oprogramowanie szkodliwe rozumie się: robaki, wirusy, konie trojańskie, rootkity.
2. Każda stacja robocza oraz serwer muszą być zabezpieczone oprogramowaniem antywirusowym. Za zapewnienie ochrony antywirusowej odpowiada ASI, w tym za zapewnienie odpowiedniej ilości licencji dla użytkowników.
3. Aktualizacja definicji wirusów odbywa się automatycznie, zabronione jest wyłączanie automatycznych aktualizacji bazy.
4. Użytkownicy są zobowiązani do skanowania oprogramowaniem antywirusowym wszystkich danych przychodzących (e-mail, nośniki danych, Internet).
5. Zabrania się wyłączania programu antywirusowego.
6. O każdym przypadku wykrycia wirusa należy powiadomić ASI.

9.2. OCHRONA PRZED NIEAUTORYZOWANYM DOSTĘPEM DO SIECI LOKALNEJ

1. W celu zabezpieczenia sieci lokalnej przed nieautoryzowanym dostępem stosuje się firewall.
2. Za zapewnienie działania oprogramowania typu firewall odpowiada ASI.
3. Zabrania się użytkownikom wyłączania oprogramowania typu firewall.
4. Firewall jest zainstalowany na serwerach i na stacjach roboczych.

9.3. ZABEZPIECZENIA INFRASTRUKTURY TELEINFORMATYCZNEJ

1. Elementy infrastruktury informatycznej (komputery, terminale, drukarki, skanery, kserokopiarki, elementy sieciowe) są zabezpieczone przed dostępem osób niepowołanych.
2. Monitory są ustawione w sposób uniemożliwiający osobom trzecim śledzenie pracy użytkownika.
3. W celu minimalizacji ryzyka utraty danych oraz w celu podtrzymaniu ciągłości pracy zastosowano UPS do wybranych stacji roboczych.
4. W stacjach roboczych BIOS chroniony jest hasłem.
5. Użytkownicy nie pracują na kontach z uprawnieniami administratora.

9.4. ZABEZPIECZENIA PROGRAMÓW I BAZ PRZETWARZAJĄCYCH DANE OSOBOWE

1. Stosowana jest zasada minimalnych uprawnień.
2. Systemy informatyczne automatycznie odnotowuje datę wprowadzenia danych osobowych do aplikacji oraz identyfikator osoby dokonującej wpisu.
3. Systemy informatyczne rejestrują zmiany dokonywane na zbiorze danych osobowych (login oraz datę dokonania zmian).
4. Systemy informatyczne pozwalają na określenie uprawnień każdego użytkownika.
5. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru.

10. ZASADY PRACY W ŚRODOWISKU INFORMATYCZNYM

10.1. OGÓLNE ZASADY PRACY W ŚRODOWISKU INFORMATYCZNYM

1. Urządzenia teleinformatyczne należące do ADO mogą być wykorzystywane jedynie w celach służbowych.
2. Urządzenia służące do przetwarzania danych osobowych należy przechowywać w bezpieczny i nadzorowany sposób.
3. Użytkownik jest zobowiązany do dbania i szanowania elementów infrastruktury teleinformatycznej.
4. O wszelkich zniszczeniach, utracie, lub prawdopodobieństwie zniszczenia elementów infrastruktury teleinformatycznej należy niezwłocznie powiadomić ASI.
5. Zabrania się instalowania aplikacji bez wiedzy ASI.
6. Niedozwolone jest instalowanie oprogramowania niezgodnego z warunkami licencjonowania.
7. Za szkody wywołane przez oprogramowanie zainstalowane samowolnie odpowiada użytkownik.
8. Zabrania się modyfikowania ustawień systemu operacyjnego oraz innych aplikacji bez wiedzy ASI.
9. Zabrania się udostępniania osobom trzecim urządzeń należących do ADO.
10. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadają licencje.
11. ASI odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki).

10.2. PROCEDURA KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się pobierania i instalowania z Internetu jakichkolwiek aplikacji, oraz pobierania z nieznanych źródeł plików.
3. W opcjach przeglądarki zabrania się zapamiętywania haseł oraz korzystania z opcji autouzupełniania formularzy.
4. Zabrania się przesyłania przez sieć Internet informacji poufnych bez zgody ADO.
5. Zabrania się korzystania ze stron / serwisów służących do wymiany i pobierania plików.
6. Zabrania się odwiedzania stron zawierających treści o charakterze pornograficznym, hackerskim, terrorystycznym lub innym zakazanym przez prawo.
7. ASI może zablokować dostęp do wybranych stron internetowych lub grupy stron o określonym charakterze.

10.3. PROCEDURA KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. W celu prowadzenia korespondencji elektronicznej stosowane są służbowe skrzynki pocztowe.
2. Zabrania się przesyłania informacji poufnych za pomocą środków korespondencji prywatnej.
3. Należy zadbać o prawidłowy wybór adresata korespondencji elektronicznej.
4. Przesyłając informacje poufne należy zabezpieczyć je kryptograficznie (np. do pliku dodać hasło, które powinno być przekazane innym kanałem niż wiadomość email – sms, ustnie). Dla

stosowanych haseł do plików obwiązują zasady opisane w rozdziale Ogólne zasady postępowania z hasłami.

5. Wysyłając korespondencję do co najmniej dwóch adresatów spoza UG Białowieża należy adresy email wprowadzać do pola UDW (Ukryte Do Wiadomości).
6. Należy dokonywać okresowych przeglądów poczty i usuwać korespondencję już niepotrzebną.
7. Nie należy otwierać załączników znajdujących się z mailach pochodzących od nieznanych osób.
8. Otwarcie każdego załącznika powinno być poprzedzone analizą treści maila, wszelkie wątpliwości dotyczące treści lub pochodzenia maila należy potraktować jako potencjalne zagrożenie, o którym należy powiadomić ASI.

10.4. Praca na odległość, wykorzystywanie urządzeń przenośnych

1. Użytkownicy komputerów przenośnych wynoszonych poza obszar UG Białowieża zobowiązani są do:
   a) Stosowania loginu i hasła w celu uwierzytelnienia;
   b) Szyfrowania danych osobowych oraz poufnych znajdujących się na komputerze przenośnym (szyfrowanie partycji, szyfrowanie plików);
   c) Do zachowania szczególnej ostrożności podczas transportu komputera przenośnego.
2. Dostęp zdalny do systemu jest możliwy wyłącznie poprzez wykorzystanie uwierzytelnionego połączenia VPN. Uzyskanie przez użytkownika dostępu zdalnego musi być zaakceptowane przez ADO.
3. Użytkownik korzystający z urządzeń przenośnych jest zobowiązany do zachowania szczególnej ostrożności, aby urządzenie nie zostało zagubione, skradzione, pozostawione bez opieki. Np. komputery przenośne zawsze powinny być wożone w bagażu podręcznym i jeśli to możliwe maskowane podczas transportu.
4. Dane znajdujące się na urządzeniu przenośnym powinny być zaszyfrowane, za wdrożenie mechanizmów szyfrowania odpowiada ASI.
5. Każdy użytkownik komputerów przenośnych / terminali musi być zapoznany z **zał. 02i Regulamin komputerów przenośnych.**

10.5. Kopie bezpieczeństwa stacji roboczych

1. Kopie bezpieczeństwa stacji roboczych wykonywane są przez użytkowników.
2. Użytkownik zobowiązany jest nie rzadziej niż raz w miesiącu wykonać kopię bezpieczeństwa danych na nośnik zewnętrzny.
3. Użytkownik zobowiązany jest do zabezpieczenia nośnika przed dostępem osób trzecich.

11. Strefy bezpieczeństwa

W Urzędzie Gminy Białowieża obowiązuje system podziału na strefy bezpieczeństwa.

11.1. Strefa bezpieczeństwa klasy I

1. Obejmuje serwerownię oraz archiwum.

2. Wykaz osób upoważnionych do przebywania w obszarze strefy I znajduje się w **załączniku nr 02e**.
3. Osoby nieuprawnione do przebywania w obszarze strefy I (nieuprawnieni pracownicy, osoby postronne) mogą przebywać w obszarze strefy pod warunkiem obecności osób upoważnionych.
4. Prace konserwacyjne oraz prace mające na celu utrzymanie czystości mogę odbywać się jedynie w obecności osób upoważnionych do przebywania w strefie I.

11.2. STREFA BEZPIECZEŃSTWA KLASY II

1. Obejmuje wszystkie pomieszczenia Urzędu Gminy Białowieża, w których przetwarzane są dane osobowe, za wyjątkiem obszarów należących do strefy bezpieczeństwa klasy I.
2. Wykaz osób upoważnionych do przebywania w obszarze strefy II znajduje się w **załączniku nr 02e**.
3. Osoby postronne mogą przebywać w obszarze strefy II pod warunkiem obecności osób upoważnionych.
4. Prace konserwacyjne oraz prace mające na celu utrzymanie czystości mogę odbywać się pod nieobecność osób upoważnionych do przebywania w strefie II – pod warunkiem uzyskania pisemnego upoważnienia stanowiącego **załącznik nr 02j – upoważnienie do przebywania w strefie przetwarzania danych.**

11.3. STREFA BEZPIECZEŃSTWA KLASY III

1. Do strefy bezpieczeństwa klasy III należą pomieszczenia, w których nie są przetwarzane dane osobowe, stanowiące przestrzeń komunikacji w urzędzie.
2. Do przebywania w obszarze strefy III nie wprowadza się ograniczeń.

12. POLITYKA KLUCZY

12.1. ZASADY DOSTĘPU DO BUDYNKU

1. Polityka kluczy obejmuje siedzibę ADO zlokalizowaną przy ulicy Sportowej 1, 17-230 Białowieża.
2. Wejście do siedziby jest zabezpieczone systemem alarmowym.
3. Decyzją ADO wydawane są kody dostępu do systemu alarmowego.
4. Decyzją ADO wydawane są klucze do siedziby.
5. Klucze do siedziby znajdują się pod osobistym nadzorem osób upoważnionych. Ewidencja przydziału kluczy znajduje się w **załączniku nr 02e**.
6. Zadaniem osób upoważnionych jest odpowiednie zabezpieczenie powierzonych kluczy oraz zachowanie w poufności kodu do systemu alarmowego.
7. Podejrzenie utraty poufności kodu alarmowego należy niezwłocznie zgłosić ADO oraz DPO.
8. Utratę klucza do budynku lub podejrzenie możliwości skopiowania klucza należy niezwłocznie zgłosić ADO oraz DPO.

12.2. ZABEZPIECZENIE POMIESZCZEŃ

1. Pomieszczenia, w których są przetwarzane dane osobowe zabezpieczone są poprzez drzwi zamykane na klucz.
2. Klucze do pomieszczeń przechowywane są w zamykanej klucznicy.
3. Utratę kluczy, lub podejrzenie ich skopiowania należy niezwłocznie zgłosić ADO oraz DPO.

12.3. KLUCZE DO BIUREK / SZAF

1. Dokumenty, elektroniczne nośniki danych powinny być zamykane na klucz w szafkach i biurkach.
2. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
3. Klucze powinny być jednoznacznie opisane.
4. Po zakończeniu pracy szafy oraz biurka są zamykane na klucz, klucze zamykane są w wybranej szafie / szufladzie.
5. Klucz zamykający szafę / szufladę wybraną do przechowania klucz deponowany jest w klucznicy wraz z kluczami do pomieszczenia.

12.4. ARCHIWUM

1. Archiwum zabezpieczone jest drzwiami zamykanymi na klucz.
2. Wykaz osób upoważnionych do dostępu do archiwum znajduje się w **załączniku nr 02e.**

12.5. POMIESZCZENIA DZIAŁU IT / SERWEROWNIA

1. Pomieszczenia działu IT / serwerownia zabezpieczone są drzwiami zamykanymi na klucz.
2. Wykaz osób upoważnionych do dostępu do pomieszczeń działu IT / serwerowni znajduje się w **załączniku nr 02e.**

13. PROCEDURA DOSTĘPU PODMIOTÓW ZEWNĘTRZNYCH

1. Przed dopuszczeniem podmiotów zewnętrznych do pracy polegającej na przetwarzaniu danych osobowych stosowane są umowy powierzenia przetwarzania danych osobowych.
2. ADO lub osoba przez niego upoważniona prowadzi rejestr podmiotów zewnętrznych, którym powierza lub udostępnia dane osobowe w postaci usługi zewnętrznej, rejestr prowadzony jest w **załączniku 01a Rejestr czynności przetwarzania.**

14. CIĄGŁOŚĆ DZIAŁANIA

14.1. KOPIE BEZPIECZEŃSTWA

14.1.1. KOPIE BEZPIECZEŃSTWA STACJI ROBOCZYCH

1. Zasady tworzenia kopii bezpieczeństwa stacji roboczych opisane są w punkcie 10.5.

14.1.2. KOPIE BEZPIECZEŃSTWA SERWERÓW ORAZ BAZ DANYCH

1. Za proces wykonywania kopii bezpieczeństwa serwerów oraz baz danych odpowiada ASI.
2. Dla aktyw informatycznych ASI prowadzi **załącznik nr 02f procedury tworzenia kopii**.
3. Procedury tworzenia kopii bezpieczeństwa są regularnie aktualizowane przez ASI.
4. Kopie bezpieczeństwa podlegają testom odtworzeniowym nie rzadziej niż raz na 6 miesięcy.
5. Każde ze zidentyfikowanych aktyw posiada instrukcję odtworzenia z kopii bezpieczeństwa opisaną w załączniku nr 02f.

14.1.3. TESTOWANIE KOPII BEZPIECZEŃSTWA

1. ASI dokonuje testów odtworzeniowych kopii bezpieczeństwa.
2. Testy kopii bezpieczeństwa odbywają się nie rzadziej niż raz na 6 miesięcy.
3. ASI w dzienniku administratora (załącznik 02k) odnotowuje przeprowadzenie testu oraz jego przebieg.

14.2. HASŁA ADMINISTRATORA

1. Hasło administratora składa się co najmniej z 8 znaków, zawiera małe i duże litery, cyfry oraz znaki specjalne.
2. Hasła administratora przechowywane są w zamkniętej kopercie – **załącznik nr 02g - metryka hasła.**
3. Osoby przechowujące koperty wyznaczone są przez ADO.
4. W przypadku zmiany administratora systemów informatycznych należy niezwłocznie zmienić hasła do systemów, którymi dany ASI zarządzał oraz zaktualizować metrykę hasła zdeponowaną jest w zamykanej skrytce.
5. W przypadkach awaryjnych (np. nieobecność ASI) hasło może być przekazane decyzją ADO osobie zastępującej ASI.
6. Po ustaniu sytuacji awaryjnej, ASI jest zobowiązany do zmiany hasła oraz zaktualizowania metryki hasła.

14.3. KONSERWACJA SPRZĘTU IT

1. Osobą odpowiedzialną za przeglądy i konserwację systemów informatycznych oraz nośników informacji służących przetwarzania danych jest ASI.
2. Przeglądy i konserwacja sprzętu odbywać się powinna zgodnie z zaleceniami dostawcy w zakresie częstotliwości i zakresu.
3. Usługi serwisowe świadczone w siedzibie ADO powinny odbywać się w obecności i pod nadzorem osób upoważnionych.
4. Usługi serwisowe odbywające się poza siedzibą ADO poprzedzone muszą być usunięciem nośników danych.
5. Przed przekazaniem sprzętu informatycznego poza obszar UG Białowieża należy zdemontować nośniki (dyski twarde z komputerów i drukarek) lub dane trwale usunąć w sposób uniemożliwiający odtworzenie lub proces naprawy powinien odbywać się pod kontrolą ASI.

14.4. UTYLIZACJA SPRZĘTU IT

1. Zbędne urządzenia i elementy infrastruktury teleinformatycznej powinny być poddane utylizacji i złomowaniu.
2. Przed oddaniem sprzętu IT do złomowania / utylizacji należy zdemontować wszelkie nośniki danych.
3. Kopie zapasowe, które uległy uszkodzeniu lub stały się zbędnymi w dalszej działalności pozbawia się bezpowrotnie zapisu danych, a w przypadku gdy nie jest to możliwe, niszczy w stopniu uniemożliwiającym ich odtworzenie. Przedmiotowe czynności wykonuje się komisyjnie pod kierownictwem ADO lub osoby przez niego upoważnionej i potwierdza się sporządzeniem protokołu komisyjnego zniszczenia kopii zapasowych.
4. Przeznaczone do utylizacji nośniki danych niszczy w stopniu uniemożliwiającym ich odtworzenie. Przedmiotowe czynności wykonuje się komisyjnie pod kierownictwem ADO lub osobę przez niego upoważnionej i potwierdza się sporządzeniem protokołu komisyjnego zniszczenia kopii zapasowych.
5. Jeżeli ww. czynności są zlecane podmiotom zewnętrznym, wykonawca zobowiązany jest do przedstawienia protokołu zniszczenia przedmiotowych nośników informatycznych.

14.5. Dziennik administratora

1. ASI prowadzi dziennik administratora (**załącznik nr 02k**) w którym odnotowuje:
   - Prace serwisowe i administracyjne dotyczące serwerów i elementów infrastruktury teleinformatycznej,
   - Przeprowadzenie testów kopii bezpieczeństwa,
   - Przeglądy logów systemowych.
2. Dziennik administratora prowadzony jest w postaci elektronicznej.

14.6. Logi systemowe

1. ASI raz w tygodniu dokonuje przeglądu logów systemowych stacji roboczych i serwerów.
2. ASI potwierdza wykonanie przeglądu logów systemowych w dzienniku administratora (**załącznik 02k**).

15. Procedura postępowania podczas braku dopływu energii elektrycznej

1. Celem procedury jest zabezpieczenie Urzędu Gminy Białowieża na wypadek okresowego zaniku elektrycznej w taki sposób, aby zabezpieczyć minimalne funkcjonowanie Urzędu w zakresie komunikacji z mieszkańcami oraz innymi podmiotami.
2. W przypadku wystąpienia przerw lub braku dopływu energii elektrycznej należy uruchomić agregat prądotwórczy.
3. Agregat prądotwórczy zlokalizowany jest w piwnicy budynku przy ul. Sportowej 1. Klucze do pomieszczenia zawierającego agregat prądotwórczy znajdują się w sekretariacie.
4. Agregat prądotwórczy należy umieścić na zewnątrz budynku przy parkingu na terenie siedziby Urzędu. Agregat podczas pracy powinien być nadzorowany przez pracownika wskazanego przez ADO (Wójta Gminy Białowieża lub przez zastępcę Wójta).

5. Zasilanie wygenerowane przez agregat prądotwórczy przeznaczone jest do zasilania laptopa użytkowanego przez Zastępcę Wójta oraz do zasilenia serwera telekomunikacyjnego.

16. PROCEDURA POSTĘPOWANIA PODCZAS BRAKU DOSTĘPU SIECI INTERNET

1. Celem procedury jest zabezpieczenie Urzędu Gminy Białowieża na wypadek braku dostępu sieci Internet w taki sposób, aby zachować komunikację elektroniczną z mieszkańcami oraz innymi podmiotami.
2. W przypadku wystąpienia przerw lub braku dostępu sieci Internet należy do Sekretariatu Urzędu Gminy przenieść modem DSL z serwerowni oraz wpiąć istniejąca linię telefoniczną do modemu.

UPOWAŻNIENIE
do przetwarzania danych osobowych

Z dniem Kliknij tutaj, aby wprowadzić datę.

☐ nadaję upoważnienie	☐ modyfikuję upoważnienie	☐ cofam upoważnienie

do przetwarzania danych osobowych Pani/Panu *) Kliknij tutaj, aby wprowadzić imię i nazwisko.

zatrudnionej / zatrudnionemu *) na stanowisku Kliknij tutaj, aby wprowadzić nazwę stanowiska.

W zakresie:

1. Czynność przetwarzania danych
2. Czynność przetwarzania danych
3. Czynność przetwarzania danych

*) niepotrzebne skreślić

Dodatkowe uwagi: Kliknij tutaj, aby wprowadzić tekst.

Data Kliknij tutaj, aby wprowadzić datę.

Imię i nazwisko upoważniającego Kliknij tutaj, aby wprowadzić tekst.

Podpis upoważniającego .....

URZĄD GMINY BIAŁOWIEŻA	**Ewidencja osób upoważnionych do przetwarzania danych osobowych**	Załącznik 02b wydanie 1
		Strona **1** z **1**

Nr upoważnienia	**Imię i nazwisko**	**Stanowisko**	**Data nadania**	**Data odebrania**	**Zakres upoważnienia**

URZĄD GMINY BIAŁOWIEŻA	**Ewidencja użytkowników systemów informatycznych**	Załącznik 02c wydanie 2
		Strona **1** z **1**

LP	Imię i nazwisko	Pokój	Nazwa komputera	Login do systemu operacyjnego	Program dziedzinowy	Login w systemie	Data nadania	Data cofnięcia
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								
11.								

Upoważnienie
do pracy w systemach informatycznych

A. Dane podstawowe

Imię i nazwisko osoby upoważnionej:		
☐ upoważniam	☐ modyfikuję upoważnienie	☐ anuluję upoważnienie
Imię i nazwisko upoważniającego		
Data:		
Uwagi:		

B. Zakres

Program dziedzinowy

Dodatkowe uwagi: Kliknij tutaj, aby wprowadzić tekst.

Data Kliknij tutaj, aby wprowadzić datę.

Imię i nazwisko upoważniającego Kliknij tutaj, aby wprowadzić tekst.

Podpis upoważaniającego .....

Ewidencja przydziału kluczy

LP	Nazwa, numer, rodzaj pomieszczenia i wydanego do niego klucza	Wydanie				Zwrot	
		Data	Imię i nazwisko przyjmującego	Podpis otrzymującego	K – klucz A – alarm	Data	Podpis odbierającego

Załącznik 02f wydanie 1

Procedury tworzenia kopii bezpieczeń

LP	Nazwa	Rodzaj	Przeznaczenie / opis	Adres systemu / aplikacji
		serwer fizyczny		
		serwer wirtualny		
		aplikacja		
		stacja robocza		

ıstwa

Lokalizacja fizyczna	Harmonogram kopii bezpieczeństwa (całościowa, przyrostowa)	Retencja	Lokalizacja kopii bezpieczeństwa	Testy odtworzeniowe (częstotliwość)

Gestor (właściciel merytoryczny) - dział	Instrukcja odtworzenia z kopii bezpieczeństwa

Załącznik 02h wydanie 1

Rejestr testów kopii bezpieczeństwa

LP	Data	Nazwa odtwarzanego systemu	Opis przebiegu procedury odtworzenia, w tym napotkane trudności i błędny	Planowana data kolejnego testu

Regulamin użytkowania komputerów przenośnych

1. Pracownicy upoważnieni do przetwarzania danych osobowych i pracujący na komputerach przenośnych muszą być zapoznani z Regulaminem użytkowania komputerów przenośnych oraz pisemnego zobowiązania się do jego przestrzegania.
2. Dane osobowe lub danych poufne znajdujące się na komputerach przenośnych muszą zostać zaszyfrowane na dysku i zabezpieczone co najmniej 8-znakowym hasłem (duże, małe litery i cyfry).
3. Komputery przenośne są wykorzystywane do prac służbowych.
4. W przypadku kradzieży/zgubienia lub naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest niezwłocznie zgłosić zdarzenie/problem administratorowi danych osobowych oraz inspektorowi ochrony danych.
5. Osoba upoważniona zobowiązana jest do zabezpieczenia komputera przenośnego w czasie transportu, a przede wszystkim:
   1) zaleca się przenoszenie komputera przenośnego w zwykłej teczce, aktówce,
   2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas nieobecności osoby upoważnionej,
   3) zabrania się pozostawiania komputera przenośnego poza miejscem pracy bez nadzoru.
6. System operacyjny, jak i inne aplikacje dziedzinowe, w ramach których przetwarzane są dane osobowe muszą być zabezpieczenie hasłem.
7. Pracując na komputerze przenośnym w miejscach publicznych lub w obecności osób nieuprawnionych, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Zapoznałam/em się z treścią Regulaminu użytkowania komputerów przenośnych i zobowiązuje się do przestrzegania zasad w nim zawartych.

Data: .....

Imię i nazwisko użytkownika .....

Podpis użytkownika .....

UPOWAŻNIENIE
do przebywania w strefie przetwarzania danych

Z dniem Kliknij tutaj, aby wprowadzić datę. upoważniam Panią/Pana *) Kliknij tutaj, aby wprowadzić imię i nazwisko.

do przebywania w strefie obszaru przetwarzania danych osobowych w celu wykonywania czynności zleconych, przez które rozumie się w szczególności: sprzątanie pomieszczeń, ochronę obiektów i pomieszczeń, konserwację infrastruktury znajdującej się w obszarze przetwarzania danych osobowych.

Zobowiązuję Panią / Pana *) do:

- zachowania w tajemnicy danych osobowych w sytuacji dostępu do nich podczas wykonywania czynności zleconych;
- zabezpieczenia tych danych przed dostępem osób nieupoważnionych, a następnie przekazanie ich do dyspozycji osób upoważnionych;
- zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych Inspektorowi Ochrony Danych lub bezpośredniemu przełożonemu.

Data Kliknij tutaj, aby wprowadzić datę.

Imię i nazwisko upoważniającego Kliknij tutaj, aby wprowadzić tekst.

Podpis upoważniającego .....

URZĄD GMINY BIAŁOWIEŻA	**Dziennik administratora**	Załącznik 02k wydanie 1
		Strona **1** z **1**

LP	Data	Opis działań	Imię i nazwisko administratora