WÓJT GMINY W SŁUPNIE
pow. płocki
woj. mazowieckie

ZARZĄDZENIE NR 149/2019
Wójta Gminy Słupno
z dnia 21 października 2019 r.

w sprawie wprowadzenia Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy w Słupnie

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2019 r. poz. 506[1]) w związku z art. 24 ust. 1 i 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. Dz. Urz. UE. L 2016 Nr 119 z dnia 4 maja 2016 r.) zarządzam, co następuje:

§1. 1. Wprowadzam Instrukcję zarządzania systemem informatycznym w Urzędzie Gminy w Słupnie, która stanowi załącznik do niniejszego zarządzenia.

§2. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Marcin Zawadka

[1] Zmiany tekstu jednolitego wymienionej uchwały ogłoszone zostały w Dz. U. z 2019 r. poz. 1309, 1696, 1815.

Załącznik do Zarządzenia Nr 149/2019
Wójta Gminy Słupno z dnia 21 października 2019 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Rozdział 1

§1. 1 Ilekroć w „Instrukcji Zarządzania Systemem Informatycznym" jest mowa o:

1) Administratorze Danych Osobowych (ADO) – osoba decydująca o celach i środkach przetwarzania danych. W Urzędzie Gminy Słupno ul. Miszewska 8A, 09-472 Słupno, funkcję administratora danych pełni wójt;
2) Inspektorze Ochrony Danych Osobowych (IOD) - osoba wyznaczona przez Administratora Danych Osobowych do wypełniania zadań przewidzianych w art. 39 ust. 1 RODO;
3) Administratorze Systemów Informatycznych (ASI) - osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za funkcjonowanie i bezpieczeństwo systemów informatycznych;
4) RODO oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1);
5) osobie upoważnionej - osoba upoważniona przez Administratora Danych Osobowych do przetwarzania danych osobowych w określonym przez niego zakresie;
6) identyfikatorze użytkownika- rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
7) haśle- rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
8) sieci telekomunikacyjnej- rozumie się przez to sieć telekomunikacyjną w rozumieniu Prawa telekomunikacyjnego (Dz.U. z 2018 r. poz. 1954, z późn. zm.)
9) sieci publicznej- rozumie się przez to sieć publiczną w rozumieniu Prawa telekomunikacyjnego (Dz.U. z 2018 r. poz. 1954, z późn. zm.);
10) teletransmisji- rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej

11) rozliczalności- rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
12) integralności danych- rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
13) raporcie- rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
14) poufności danych- rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
15) uwierzytelnianiu- rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu
16) analizie ryzyka - systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka;
17) szacowaniu ryzyka - proces oceny i analizy ryzyka;
18) ocenie ryzyka - proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
19) ryzyku szczątkowym - ryzyko pozostające po procesie postępowania z ryzykiem;
20) bezpieczeństwie informacji - zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność, niezawodność;
21) aktywach - wszystko, co ma wartość dla organizacji;
22) zagrożeniach systemu - to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;
23) incydencie bezpieczeństwa teleinformatycznego - należy przez to rozumieć takie pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności;
24) integralności- należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
25) podatności- należy przez to rozumieć słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie;
26) poufności - należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;

27) zabezpieczeniu- należy przez to rozumieć środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko;
28) zagrożeniu- należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego;
29) zasobach systemu teleinformatycznego - należy przez to rozumieć informacje przetwarzane systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji.

Rozdział 2.
Instrukcja Zarządzania

§ 2. Odpowiedzialność

1. Za bezpieczeństwo danych oraz danych osobowych przetwarzanych w systemach informatycznych urzędu odpowiada Administrator Danych Osobowych (ADO).
2. Nadzór nad realizacją zadań w zakresie zarządzania systemem informatycznym sprawuje Administrator Systemów Informatycznych (ASI).

§ 3. Poziom bezpieczeństwa

1. W urzędzie wprowadza się poziom bezpieczeństwa przetwarzania danych oraz danych osobowych w systemach informatycznych na poziomie wysokim gdyż przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

§ 4. Dostęp do systemów

1. Obszar, w którym są przetwarzane dane, osoba upoważniona do ich przetwarzania zabezpiecza przed dostępem osób nieuprawnionych na czas jej nieobecności.
2. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych oraz danych osobowych.
3. W systemie informatycznym służącym do przetwarzania danych oraz danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Danych Osobowych.

§ 5. Ogólne zasady eksploatacji systemów

1. ADO wraz z IOD i ASI podejmują działania mające na celu zapewnienia jak najwyższego stopnia bezpieczeństwa dla danych i informacji podczas eksploatacji.
2. ASI jest upoważniony do wydawania zaleceń użytkownikom do obszaru w którym przetwarzają dane oraz dane osobowe.
3. Użytkownikom nie wolno samodzielnie podłączać do infrastruktury informatycznej urzędu jakichkolwiek urządzeń prywatnych lub niezautoryzowanych przez ASI.
4. Podłączenie urządzeń prywatnych może nastąpić wyłącznie za zgodą ASI.
5. Użytkownikom nie wolno samodzielnie instalować jakiegokolwiek oprogramowania,

używać nośników pamięci nieznanego pochodzenia oraz podejmować czynności jakie mogą nieść za sobą ryzyko utraty danych oraz danych osobowych.

6. Użytkownik jest uprawniony do wykorzystywania systemu informatycznego wyłącznie dla celów i realizowania swoich obowiązków służbowych.

§ 6. Urządzenia do przetwarzania danych

1. Sprzęt wykorzystywany w urzędzie jest dobierany adekwatnie do celu jego wykorzystania.
2. Użytkownik jest zobowiązany zgłaszać ASI wszelkie nieprawidłowości w działaniu wykorzystywanego przez niego sprzętu.
3. Ekrany monitorów powinny być ustawione w sposób uniemożliwiający podejrzenie danych dla osób nieuprawnionych, szczególnie dla osób postronnych wchodzących do pomieszczenia.
4. Pomieszczenia serwerowni są zabezpieczone przed dostępem dla osób nieupoważnionych. Dostęp do serwerowni mają jedynie osoby upoważnione przez ADO.
5. Wszystkie urządzenia teletechniczne są podłączone wyłącznie do dedykowanej sieci elektrycznej posiadającej uziemienia i odpowiednie parametry.

§ 7. Nośniki danych

1. Podstawowym nośnikiem, na których są przetwarzane dane osobowe są dyski twarde stacji roboczych oraz serwerów.
2. W szczególnych przypadkach gdy wymaga tego specyfika realizowanych zadań, dane mogą być przechowywane na nośnikach mobilnych takich jak płyty CD/DVD/ karty pamięci.
3. Nośniki zawierające kopie zapasowe danych które uległy przedawnieniu należy trwale i skutecznie zniszczyć. Usunięcie danych powinno spełniać wymogi definicji tego pojęcia zawartej w przepisach o ochronie danych osobowych.
4. Nośniki zawierające kopie zapasowe danych przechowuje się w bezpiecznych miejscach, zabezpieczonych przed uszkodzeniem lub zniszczeniem oraz dostępem osób niepowołanych z zachowaniem wszystkich uregulowań dotyczących bezpieczeństwa przy przetwarzaniu danych.
5. Dostęp do kopii zapasowych posiada jedynie ASI.

6. Dane przechowywane na nośnikach mobilnych powinny być usuwane niezwłocznie po ustaniu powodów, dla których podjęto decyzję o wykorzystaniu nośnika mobilnego wyłącznie przez ASI.

§ 8. Procedura naprawy i aktualizacji systemów oraz oprogramowania

1. Naprawa sprzętu i oprogramowania w systemach informatycznych odbywa się wyłącznie przez ASI, informatyka lub osoby uprawnione posiadające niezbędną wiedzę i doświadczenie.
2. Naprawa odbywa się każdorazowo w budynku urzędu pod nadzorem ASI lub informatyka oraz w obecności uprawnionego pracownika urzędu.
3. W szczególnych sytuacjach naprawy poza siedzibą urzędu powinny być wykonywane wyłącznie na sprzęcie pozbawionym jakichkolwiek danych osobowych lub należy zastosować dodatkowe środki w postaci kryptografii.
4. Aktualizacja oprogramowania służącego do przetwarzania danych, w szczególności danych osobowych odbywa się wyłącznie w siedzibie urzędu. Wykonywana jest przez ASI, informatyka lub serwisanta dedykowanego oprogramowania pod nadzorem ASI.

§ 9. Procedura nadawania i cofania uprawnień

1. ADO nadaje upoważnienie do przetwarzania danych oraz danych osobowych w obszarze określonym przez bezpośredniego przełożonego osoby upoważnionej.
2. IOD prowadzi ewidencje osób upoważnionych przez ADO do przetwarzania wszystkich danych osobowych.
3. IOD na podstawie upoważnienia informuje ASI o konieczności stworzenia nowego dostępu do systemów informatycznych przetwarzających dane osobowe.
4. Użytkownik przetwarzający dane po otrzymaniu upoważnienia od IOD oraz loginu i hasła od ASI jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy.
5. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia bezpiecznym hasłem.

6. Identyfikator może zostać przydzielony tylko raz i jednoznacznie powinien identyfikować użytkownika systemu teleinformatycznego.
7. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
8. Ewidencję osób upoważnionych do przetwarzania danych, w tym danych osobowych w systemach informatycznych wraz z identyfikatorami prowadzi ASI.
9. W przypadku cofnięcia upoważnienia osobie przetwarzające dane oraz dane osobowe, do korzystania z systemu informatycznego lub/i do przetwarzania danych osobowych, bezpośredni przełożony jest zobowiązany powiadomić o tym fakcie ASI oraz IOD.
10. IOD wyrejestrowuje niezwłocznie użytkownika i zleca ASI unieważnienie bądź zablokowanie identyfikatora i hasła użytkownika oraz podejmuje inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

§ 10. Procedura zabezpieczenia systemów

1. System informatyczny służący do przetwarzania danych oraz danych osobowych zabezpiecza się, w szczególności przed:
   1) działaniem złośliwego oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego poprzez zainstalowanie programu antywirusowego na każdej stacji roboczej;
   2) poprzez stosowanie routerów brzegowych separujących prace wewnętrzną sieci LAN;
   3) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego ups.
2. ASI we współpracy z ADO określa zasady podłączania lokalnej infrastruktury informatycznej do sieci publicznej, określając użytkowników oraz ich uprawnienia dostępu.
3. ASI jest zobowiązany do zastosowania zabezpieczeń chroniących lokalną sieć komputerową przed niepowołanym dostępem z zewnątrz.
4. Stosuje się metody zapewniające poufność transmisji i ograniczony krąg użytkowników mających dostęp do sieci zdefiniowanej, kontrolowanej przez ASI i informatyka.

5. Przesyłanie danych podlegających ochronie w sieci publicznej może odbywać się wyłącznie z zastosowaniem środków kryptograficznych.
6. Wykorzystywanie w transmisji sieci bezprzewodowych (Wi-Fi) jest możliwe tylko poprzez mechanizmy kryptograficzne. Każda osoba uprawniona, wykorzystująca do komunikacji sieć bezprzewodową jest monitorowana w celu bezpieczeństwa transmisji danych.
7. Do sieci teletechnicznej mają możliwość podłączyć się urządzenia jedynie wcześniej zgłoszone do ASI które po nadaniu uprawnień zostają opisane w systemie logów routerów brzegowych.
8. ADO zabrania wykorzystywania sprzętu prywatnego do celów służbowych oraz prób podłączania się do lokalnej infrastruktury. W szczególnych i uzasadnionych na piśmie przypadkach na podłączenie może zezwolić ADO lub ASI.
9. Każda próba ingerencji w lokalna infrastrukturę, w tym podłączanie urządzeń niezatwierdzonych przez ASI lub ADO może zostać uznana za próbę naruszenia bezpieczeństwa danych oraz systemów teleinformatycznych.
10. Osoby wykorzystujące w swojej pracy komputery przenośne zobowiązane są do zachowania szczególnej ostrożności w trakcie wykorzystywania go, zwłaszcza poza siedzibą urzędu.
11. Szczególną ostrożność należy zachowywać w zakresie transportu komputera, przechowywania oraz użytkowania.
12. ASI lub zastępujący go informatyk jest zobowiązany przed przekazaniem sprzętu mobilnego do odpowiedniego zabezpieczenia kryptograficznego, adekwatnego do przetwarzanych danych.
13. W trakcie doboru zabezpieczeń ASI jest zobowiązany rozważyć zastosowanie:
    1) zabezpieczenie dostępu do komputera hasłem na poziomie sprzętowym;
    2) zabezpieczenie dostępu do systemu za pomocą mechanizmów uwierzytelniania;
    3) zastosowanie kryptograficznych środków ochrony danych przetwarzanych na nośnikach danych wchodzących w skład komputera;
    4) zastosowanie narzędzi programowych ograniczających dostęp do chronionych danych.
14. Osoba użytkująca komputer przenośny jest zobowiązana do zachowania szczególnej ostrożności przy podłączaniu go do sieci publicznej.
15. Za wszelkie działania podejmowane z użyciem urządzeń mobilnych

wykorzystywanych poza obszarem siedziby urzędu oraz wszelkie konsekwencje z tego wynikające ponosi użytkownik urządzeń mobilnych.

16. W przypadku zaistnienia konieczności wykorzystania sprzętu komputerowego poza siedzibą urzędu użytkownik każdorazowo musi uzyskać zgodę ADO lub ASI. Urządzenia opuszczające siedzibę urzędu nie posiadają możliwości połączenia się z bazami danych oraz danych osobowych. Wniosek należy zgłosić droga elektroniczną(mail) lub papierową.
17. Zabrania się samowolnego wynoszenia przez pracowników sprzętu poza siedzibę urzędu.
18. Z obowiązku tego zwolnione są osoby pełniące funkcję: Wójta, Zastępcy Wójta, Sekretarza oraz Skarbnika.

§ 11. Polityka stosowania haseł

1. Hasła dostępu do systemów informatycznych są objęte tajemnicą służbową i związane z spersonalizowanym identyfikatorem.
2. Zabrania się ujawniania, przekazywania lub zapisywania haseł.
3. Zabrania się stosowania automatycznych mechanizmów logowania poprzez zapisywanie haseł w systemach.
4. Możliwe jest stosowanie certyfikatu umieszczonego na karcie elektronicznej tj. karta kryptograficzna/chipowa wykorzystującej kod pin w celu uwierzytelnienia.
5. Hasło nie może być takie samo jak identyfikator przydzielony przez ASI.
6. Hasło nie może być używane więcej niż raz.
7. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni, jeśli system w którym są przetwarzane dane nie wymusi tego automatycznie.
8. Hasło nadane przez użytkownika musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
9. Hasła nadane przez ASI do pierwszego zalogowania, użytkownik musi niezwłocznie zmienić według powyżej określonych kryteriów.
10. Użytkownik nie może zapisywać haseł ani przekazywać ich innym. Stanowi ono w połączeniu z spersonalizowanym identyfikatorem dowód wykonywanych operacji na danych przez uprawnionego użytkownika.
11. Użytkownik, który utracił hasło lub klucz prywatny, nie może za pomocą spersonalizowanego identyfikatora uzyskać dostępu do Systemu Informatycznego,

zobowiązany jest zgłosić bezzwłocznie ten fakt ASI.

§ 12. Tworzenie kopii bezpieczeństwa

1. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
2. Kopie wszystkich danych oraz danych osobowych muszą być tworzone nie rzadziej niż raz na 30 dni.
3. Kopie zapasowe:
   1) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu serwerowni z ograniczonym dostępem;
   2) usuwa się niezwłocznie po ustaniu ich użyteczności.
4. Kopie baz danych są wykonywane wyłącznie przez ASI i przechowywane w obu serwerowniach na dwóch niezależnych serwerach równocześnie.
5. Kopie danych zgromadzonych na stacjach roboczych użytkowników wykonywane są bezpośrednio przez użytkowników na zabezpieczony hasłem dla każdego udział na serwerze plików, który jest zlokalizowany w pomieszczeniu serwerowni.
6. Kopie baz danych powinny być opisane w sposób jednoznacznie identyfikujący zbiór wraz z podaniem daty wykonywania kopi.
7. ASI uczestniczy w procesie tworzenia kopii zapasowych oraz ma prawo do wprowadzania doraźnych zmian dotyczących czasu wykonywania kopii.
8. W przypadku przekazywania nośników informacji zawierających kopie zapasowe danych osobowych podmiotom zewnętrznym na podstawie zawartych umów celem usunięcia błędów lub naprawy zbiorów, stosownie wcześniej każdorazowo musi zostać określona procedura przekazywania oraz metody zabezpieczenia nośników informacji przed dostępem osób nieupoważnionych z zastosowaniem środków ochrony kryptograficznej.

§ 13. Postępowanie przy likwidacji lub przekazaniu urządzeń

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   1) likwidacji- pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to

możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych- pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
3) naprawy- pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez ADO.

§ 14. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed rozpoczęciem pracy w systemie każdy pracownik jest zobowiązany sprawdzić stan urządzeń oraz swojego stanowiska pracy pod kątem potencjalnych działań stanowiących naruszenie zasad bezpieczeństwa lub próby uzyskania nielegalnego dostępu do danych.
2. W sytuacji stwierdzenia naruszenia zasad bezpieczeństwa użytkownik jest zobowiązany bezzwłocznie poinformować o tym fakcie ASI oraz przerwać dalszą procedurę logowania do systemu.
3. W przypadku jakichkolwiek wątpliwości dotyczącej bezpieczeństwa systemu, użytkownik powinien poinformować swojego przełożonego lub osobę zastępującą go oraz ASI.
4. Jeśli stan urządzeń oraz stanowisko pracy nie budzi zastrzeżeń, użytkownik może rozpocząć procedurę uwierzytelniania go w systemach.
5. Jeżeli pracownik zamierza chwilowo opuścić stanowisko pracy to jest zobowiązany każdorazowo zawiesić prace w systemach uniemożliwiając w ten sposób dostęp do danych dla niepowołanych osób.
6. Użytkownik jest zobowiązany do zapisania danych na których pracuje, a następnie do zablokowania stacji roboczej poprzez wylogowanie z systemów.
7. Bezwzględnie zabrania się opuszczania stanowiska pracy bez zablokowania dostępu do stacji roboczej.
8. Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek zapisać dane na których pracował, zamknąć programy oraz wylogować się z systemu.
9. W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 10 min, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.
10. Przed opuszczeniem stanowiska pracy użytkownik jest zobowiązany upewnić się, że komputer został prawidłowo zamknięty.

11. Dodatkowo opuszczając stanowisko pracy użytkownik jest zobowiązany do zabezpieczenia przed dostępem osób nieupoważnionych wszystkich dokumentów papierowych oraz nośników danych zawierających informacje podlegające ochronie.

§ 15. Zasady korzystania z poczty elektronicznej

1. Dostęp do systemu poczty elektronicznej przydzielany jest na wniosek przełożonego nowego użytkownika.
2. ASI tworzy nowe konto, określa zakres przestrzeni wirtualnej oraz przydziela hasło tymczasowe umożliwiające użytkownikowi pierwsze logowanie.
3. Użytkownik po podpisaniu protokołu odbioru powinien zalogować się do systemu pocztowego i niezwłocznie zmienić hasło.
4. Schemat tworzenia bezpiecznych haseł opisuje punkt 10 niniejszej instrukcji.
5. Zabrania się wykorzystywania służbowej poczty elektronicznej do celów innych niż związane z realizacją zadań wynikających z zatrudnienia.
6. Obowiązuje zakaz przekazywania jakichkolwiek informacji służbowych, w tym danych osobowych , poprzez niezatwierdzone przez ADO kanały informacyjne.
7. ADO oraz ASI mając zasadne podejrzenia wykorzystywania poczty elektronicznej do celów innych niż służbowe w porozumieniu z bezpośrednim przełożonym użytkownika mogą przeprowadzić kontrolę korespondencji znajdującej się na serwerach pocztowych użytkownika.

§ 16. Zasady korzystania z telefonów służbowych

1. ASI w porozumieniu z ADO na podstawie wniosku przełożonego użytkownika przekazuje do wykorzystania w celach służbowych numer telefonu dla pracownika urzędu.
2. Zabrania się wykorzystywania służbowego telefonu oraz numer do celów innych niż związane z realizacją zadań wynikających z zatrudnienia.
3. Obowiązuje zakaz przekazywania jakichkolwiek informacji służbowych, w tym danych osobowych, poprzez niezatwierdzone przez ADO kanały informacyjne.

§ 17. Wykonywanie kontroli oraz przeglądów systemów

1. ASI może dokonywać przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbać o ich dobry stan techniczny bez uprzedniego informowania użytkownika

systemu.

2. Informatyk wraz z ASI wykonuje przeglądy okresowe raz na kwartał oraz przegląd generalny raz na rok.
3. W przypadku stwierdzenia usterek technicznych ASI ma obowiązek niezwłocznie powiadomić o tym fakcie ADO.
4. ASI w przypadku stwierdzenia uchybień, dotyczących przetwarzania danych w podmiocie powinien o tym fakcie niezwłocznie powiadomić ADO oraz wprowadzić takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.
5. Zgodnie z zasadą ograniczonego przechowywania określoną w art. 5 ust. 1lit. E RODO Asi wraz ADO przeprowadzi
6. Naczelnicy wydziałów, dyrektorzy biur, osoby na samodzielnych stanowiskach do 31 stycznia są zobligowani do przekazania ASI szczegółowego wykazu dokumentów opublikowanych na stronach urzędu , które zgodnie z Rozporządzeniem Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, powinny zostać zniszczone w procesie brakowania dokumentów niearchiwalnych.

Rozdział 2.
Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych

§ 18. Wymogi ogólne bezpieczeństwa przetwarzanych danych osobowych, wprowadzone przez ADO.

1. W czasie przetwarzania danych osobowych informacje mogą występować w postaci plików lub informacji przechowywanych na dysku twardym komputera, plikach lub informacjach zapisanych na nośnikach komputerowych lub w wersjach roboczych/ gotowych dokumentów wydrukowanych na papierze.
2. Bezpieczeństwo przetwarzanych lub przechowywanych informacji zawierające dane osobowe wymaga:
   1) zapewnienia ochrony fizycznej stanowiska komputerowego przed nieuprawnionym dostępem;
   2) ochrony nośników technicznych i wydruków dokumentów wytwarzanych przy pomocy sprzętu komputerowego, w tym określenia zasad postępowania z nimi przed nieuprawnionym dostępem;
   3) zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego;
   4) zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników;
   5) zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności;
   6) zapewnienia możliwości kontroli nośników, na których przetwarzano lub przechowywano dane osobowe.

§ 19. 1. W myśl ustawy o ochronie danych osobowych, każdy Administrator Danych Osobowych powinien zapewnić takie warunki pracy w systemie, aby cechował się on poufnością, integralnością i rozliczalnością.

2. Każde zauważone zagrożenie związane z poufnością, integralnością lub rozliczalnością, powinno być niezwłocznie zgłoszone ADO oraz ASI.

§ 20. 1. Poufność to zapewnienie danym osobowym niemożności ich udostępniania nieupoważnionym osobom czy podmiotom.

2. Zagrożenia, jakie można wyróżnić ze względu na utratę poufności w systemie informatycznym:
   1)kradzież urządzenia lub nośnika;
   2)pozostawienie urządzenia lub nośnika w miejscu ogólnie dostępnym;
   3)nieprawidłowa obsługa urządzenia;
   4)manipulowanie przy urządzeniu lub nośniku;
   5)awaria oprogramowania;
   6)niewłaściwe funkcjonowanie oprogramowania;
   7)nieumiejętność obsługi oprogramowania przez użytkownika;
   8)instalowanie nieautoryzowanego oprogramowania;
   9)naruszenie praw autorskich (używanie pirackiego oprogramowania);
   10)kradzież dokumentów przez zatrudnionych lub osoby trzecie;
   11)brak motywacji do pracy;
   12)skopiowanie danych przez zatrudnionych lub osoby trzecie;
   13)nieświadome przekazanie danych osobom trzecim;
   14)brak znajomości obowiązujących procedur;
   15)katastrofa budowlana;
   16)wejście osoby nieuprawnionej na teren organizacji, do budynku lub pomieszczeń;
   17)brak możliwości identyfikacji osoby nieuprawnionej;
   18)brak prądu;
   19)szpiegostwo zdalne;
   20)przejęcie kontroli nad siecią;
   21)przeciążenie sieci;
   22)awaria serwerów;
   23)podłączanie nieautoryzowanych urządzeń lub nośników;
   24)niejasny podział zadań i obowiązków, dublowanie kompetencji;
   25)brak wyraźnego podziału odpowiedzialności;
   26)brak skutecznych procedur.

3. Skala identyfikacji skutków utraty zasobów dla atrybutu poufności danych osobowych.

Wartość	**Skutki**
0	Brak skutków utraty poufności
1-3	Niski skutek utraty poufności
4-7	Średni skutek utraty poufności
8-9	Wysoki skutek utraty poufności
10	Całkowita utrata poufności

§ 21. 1. Integralność to zapewnienie, aby wszelkie modyfikacje wykonywane w systemie informatycznym, w systemie jego katalogów oraz indywidualnych plikach posiadające w sobie dane osobowe były skutkiem rozważnych i zaplanowanych działań użytkowników systemu.

2. Dane nie mogą zostać zmodyfikowane lub zniszczone w sposób nieautoryzowany. Integralność danych dotyczy przede wszystkim wartości informacyjnych przetwarzanych w postaci elektronicznej. Ważne jest zachowanie integralności dla bezpieczeństwa systemu i sieci.
3. Zagrożenia, jakie można wyróżnić ze względu na utratę integralności przez system informatyczny:
   1) nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego;
   2) błędy, pomyłki;
   3) brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika;
   4) wadliwe działanie systemu operacyjnego;
   5) brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych.
   6) uszkodzenie, celowe lub przypadkowe systemu operacyjnego lub urządzeń sieciowych;
   7) celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych,
   8) działanie złośliwego oprogramowania (wirusy);

9) pożar, zalanie, ekstremalna temperatura, itp.;

10)zagrożenia zewnętrzne (np. klęski żywiołowe, atak terrorystyczny).

4. Skala identyfikacji skutków utraty zasobów dla atrybutu integralności danych osobowych

Wartość	**Skutki**
1	Utrata integralności nie występuje
2	Niski skutek utraty integralności
3	Średni skutek utraty integralności
4	Wysoki skutek utraty integralności
5	Bezwzględny skutek utraty integralności

§ 22. 1. Rozliczalność to cecha zapewniająca działanie podmiotu przetwarzającego dane osobowe, która może być przypisana w sposób jednoznaczny tylko temu, jednemu podmiotowi.

2. Zagrożenia, jakie można wyróżnić ze względu na utratę rozliczalności systemu informatycznego:
   1) brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania;
   2) wyparcie się pracy na stanowisku komputerowym, gdzie przetwarza się dane osobowe;
   3) wprowadzenie zmian w treści dokumentu zawierającego dane osobowe;
   4) błędy oprogramowania lub sprzętu;
   5) nieprzydzielenie użytkownikom indywidualnych identyfikatorów;
   6) niewłaściwa administracja systemem informatycznym;
   7) niewłaściwa konfiguracja systemu informatycznego;
   8) zniszczenie lub sfałszowanie logów systemowych;
   9) brak rejestracji udostępnienia danych osobowych;
   10) podszywanie się pod innego użytkownika;
   11) niespełnienie przez system wymagań ustawowych.

3. Skala identyfikacji skutków utraty zasobów dla atrybutu rozliczalności danych osobowych.

Wartość	Skutki
1	Utrata dostępności nie występuje
2	Niski skutek utraty rozliczalności
3	Średni skutek utraty rozliczalności
4	Wysoki skutek utraty rozliczalności
5	Ekstremalny skutek utraty rozliczalności

§ 23. 1. Szczególnie niebezpieczne dla systemów informatycznych są zagrożenia ze względu na ingerencję:

1) siły natury takie jak uderzenie pioruna a w konsekwencji pożar, starzenie się sprzętu, nośników pamięci, katastrofy budowlane, ulewny deszcz;
2) ludzi takie jak błędy i pomyłki użytkowników i administratorów, błędy utrzymania systemu w poufności, integralności i rozliczalności, zaniedbania użytkowników przy przesyłaniu, udostępnianiu i kopiowaniu, zagubienie nośnika zawierającego dane osobowe, nielegalne użycie oprogramowania, nieuprawnione zastępstwo, podpalenie obiektu, zakłócenia elektromagnetyczne i radiotechniczne, zmiany napięcia w sieci, defekty oprogramowania, szpiegostwo i kradzież, użycie złośliwego oprogramowania.

§ 24. Podatność systemu na zagrożenia

1. Podatność systemu na zagrożenia może wynikać z dostępności systemu dla znacznej liczby personelu, mającego potencjalnie dostęp do systemu oraz wiedzę, jak obsługiwać system. Osoba przetwarzająca dane osobowe powinna przestrzegać „zasady czystego biurka". Ponadto, tylko i wyłącznie osoby upoważnione do przetwarzania danych osobowych powinny posiadać wiedzę o tym, w jaki sposób obsługiwać system informatyczny, będący integralnym elementem placówki.
2. Dostępność informacji znajdujących się w systemie za pośrednictwem połączeń zewnętrznych. System informatyczny w placówce powinien być odpowiednio zabezpieczony, to znaczy wystarczająco odporny na wszelkiego rodzaju zewnętrzne zagrożenia.
3. Możliwość celowego wprowadzania luk w sprzęcie i oprogramowaniu lub wprowadzania wirusów komputerowych. Kadra powinna być odpowiednio

uwrażliwiona na otrzymywanie korespondencji mailowej, co do której zaistnieje podejrzenie, że została przesłana w celu wprowadzenia wirusa komputerowego.

4. Możliwość awarii sprzętu lub oprogramowania ze względu na uszkodzenia, błędy projektowe lub umyślną interwencję. Sprzęt informatyczny powinien być cyklicznie odpowiednio serwisowany, tak by wyeliminować zagrożenia.
5. Przesyłanie informacji przez niezabezpieczone łącza telekomunikacyjne również stanowi zagrożenie utraty poufności danych osobowych.
6. Podatność systemu na zagrożenia została ograniczona poprzez:
   1)ochronę fizyczną stanowisk komputerowych;
   2)kontrolę dostępu do pomieszczeń, gdzie przetwarzane są dane osobowe;
   3)ograniczenie liczby personelu, mającego potencjalnie dostęp do stanowisk komputerowych oraz wiedzę, jak je obsługiwać;
   4)zbudowanie stabilnej sieci zasilającej;
   5)audyt;
   6)zabezpieczanie haseł;
   7)użycie oprogramowania antywirusowego;
   8)backupy.
7. Identyfikacja podatności systemu informatycznego na określone zagrożenia.

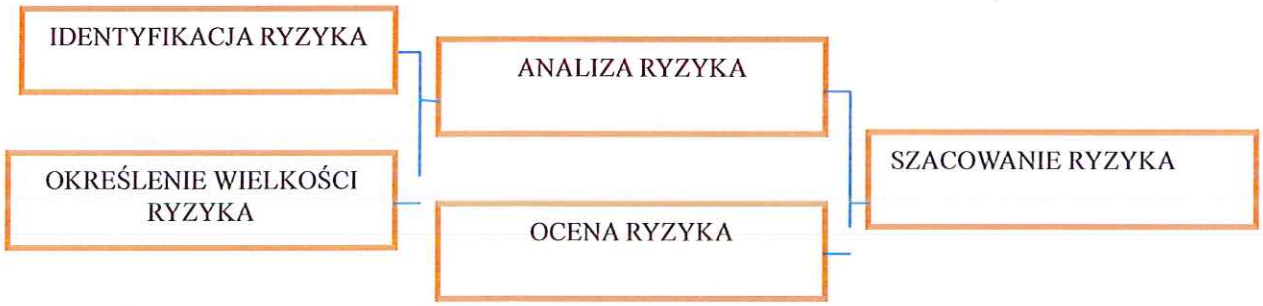
Wartość	**Skutki**
1	Brak podatności
2	Niski poziom
3	Średni poziom
4	Wysoki poziom
5	Ekstremalny poziom

§ 25. 1. Administrator Danych Osobowych przygotowując analizę zagrożeń i szacowanie ryzyka określa:

1) zasoby - które będzie chronić: sprzęt komputerowy przechowujący dane - dysk twardy, dane osobowe przetwarzane w formie papierowej i elektronicznej, aplikacje, w których przetwarzane są dane osobowe, pomieszczenia, w których pracują osoby przetwarzające dane osobowe;
2) zagrożenia - czynnik, który może powodować wystąpienie incydentu;

3) podatność - słabość zasobów, która może być wykorzystana przez potencjalne zagrożenie;
4) skutki - jaki wpływ będzie miał zaistniały incydent na utratę danych osobowych.

2. Poniższy schemat obrazuje prawidłowy tok szacowania i postępowania z ryzykiem, jakie podejmuje Administrator Danych Osobowych.



1) Analiza ryzyka jest częścią szacowania ryzyka. Jest ona pojęciem węższym niż szacowanie ryzyka, nie zawiera bowiem oceny ryzyka.
2) Ocena ryzyka, czyli określenie, które ryzyka są akceptowalne poprzez porównanie wyznaczonych poziomów ryzyka z tymi, które można zaakceptować.
3) Szacowanie ryzyka obejmuje analizę ryzyka i ocenę ryzyka.

§ 26. 1. Administrator Danych Osobowych szacuje wynik ryzyka, wyciąga wnioski oraz podejmuje działania naprawcze, mające na celu obniżenie wartości ryzyka akceptowalnego.

RYZYKO = wartość skutków x podatność zasobów systemu (max. = 375)

Wartość	**Poziom Ryzyka**
1- 39	Bardzo niskie ryzyko
40-99	Niskie ryzyko
100- 149	Średnie ryzyko
150 -249	Wysokie ryzyko
250-375	Bardzo wysokie ryzyko

§ 27. 1. Proces zarządzania ryzykiem związany z bezpieczeństwem informacji zapewnia:

1) identyfikowanie zagrożeń dla przetwarzanych informacji;
2) oszacowanie ryzyka w kategoriach konsekwencji dla funkcjonowania biznesowego oraz prawdopodobieństwa wystąpienia zagrożeń;
3) odpowiednie przedstawienie oraz zrozumienie prawdopodobieństwa oraz konsekwencji materializacji ryzyka;
4) ustanowienie priorytetów dotyczących postępowania z ryzykiem;
5) wprowadzanie priorytetowych działań mających na celu redukcję ryzyka;
6) zaangażowanie kierownictwa podczas podejmowania decyzji związanych z zarządzaniem ryzykiem oraz bieżące informowanie go o postępach realizowanych działań minimalizujących;
7) monitorowanie i regularne przeglądanie ryzyka oraz procesu zarządzania nimi;
8) kształcenie pracowników w zakresie ryzyka oraz działań mających na celu obniżenie poziomu prawdopodobieństwa ich wystąpienia.

§ 28. 1. Administrator Danych Osobowych w Urzędzie Gminy w Słupnie wraz z ASI, przeprowadził analizę dla wszystkich chronionych zasobów oraz wszystkich możliwych zagrożeń.

2. Administrator Danych Osobowych wraz z ASI jest zobowiązany dostosować środki bezpieczeństwa, zarówno techniczne, jak i fizyczne oraz organizacyjne, do wyników, jakie oddała przeprowadzona analiza.
3. Administrator Danych Osobowych określa postępowania z ryzykiem.