**ZARZĄDZENIE NR 35/2019**

**WÓJTA GMNY KOŁACZKOWO**

**z dnia 28.05.2019 r.**

**w sprawie wprowadzenia do stosowania dokumentacji z zakresu ochrony danych osobowych**

Na podstawie art. 24 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 (dalej RODO)

**zarządzam, co następuje:**

**§ 1**

W Urzędzie Gminy w Kołaczkowie wprowadza się do stosowania „Politykę Bezpieczeństwa przetwarzania danych osobowych" stanowiącą załącznik nr 1 do niniejszego Zarządzenia.

**§ 2**

Nadzór nad przestrzeganiem postanowień dokumentacji ochrony danych osobowych oraz stosowania niniejszego Zarządzenia sprawuje Sekretarz Gminy.

**§ 3**

Za prawidłowe działania systemu informatycznego odpowiadają osoby odpowiedzialne za infrastrukturę informatyczną.

**§ 4**

Administratorem jest Wójt Gminy Kołaczkowo.

**§ 5**

Zobowiązuje się pracowników do zapoznania się z postanowieniami niniejszego Zarządzenia i przestrzegania ich realizacji.

**§ 6**

Traci moc zarządzenie nr 22/2015 z dnia 15.06.2015 r.

**§ 7**

Zarządzenie wchodzi w życie z dniem podpisania.

Radca Prawny
Pz - 9360
Paweł Myśliński

WÓJT
Teresa Waszak

# Polityka Ochrony Danych

Niniejsza „Polityka Ochrony Danych" w Urzędzie Gminy w Kołaczkowie (dalej: Urząd) ma na celu opisanie zasad i procedur stosowanych przez Administratora w celu spełnienia wymagań Rozporządzenia PE i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych zwanego w dalszej części polityki RODO.

Administrator deklaruje, że proces przetwarzania danych osobowych uwzględnia zasady, o których mowa w Motywie 39 RODO oraz artykule 5 ust. 1 ppkt a) – e) RODO.

Administrator zaznacza, że niniejsza polityka to jeden ze środków o charakterze organizacyjnym, za pomocą którego wykazuje się zgodność przetwarzania danych osobowych z RODO.

Administrator deklaruje pełną świadomość charakteru, rodzaju i kontekstu przetwarzanych danych osobowych.

**Podstawy prawne:**

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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),
2. Pozostałe przepisy regulujące system ochrony danych osobowych, w tym przepisy wydane na podstawie art. 40 RODO.

## I. Weryfikacja posiadanych danych osobowych i zasady ich przetwarzania

1. Inwentaryzacja danych

1.1 Poprzez dane osobowe, zgodnie z art. 4 pkt 1) RODO należy rozumieć wszystkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można w sposób pośredni lub bezpośredni zidentyfikować, z uwzględnieniem identyfikatorów.

1.2 Dane osobowe są zorganizowane w struktury za pomocą których Administrator może ocenić ryzyko ich przetwarzania oraz ocenić konieczność przeprowadzenia procedury oceny skutków dla systemu ochrony danych, o którym mowa w art. 35 RODO.

1.3 Dane osobowe opisane są z uwzględnieniem, co najmniej poniższych informacji:

a) nazwa przetwarzanych danych osobowych,
b) cele przetwarzania,
c) zakres przetwarzania,
d) odbiorcy danych,
e) zakres czynności przetwarzania,
f) zasoby służące do przetwarzania danych osobowych,
g) informacja o konieczności wpisu do rejestru czynności przetwarzania,
h) informacja o konieczności przeprowadzenia oceny skutków dla ochrony danych na zbiorze,
i) okres przechowywania.

1.4 Szczegółowo opis danych osobowych został przedstawiony w Rejestrze Czynności Przetwarzania Danych. Wzór rejestru stanowi załącznik nr 1.

2. Legalność procesu przetwarzania danych osobowych

2.1 Administrator swoimi działaniami i organizacją Urzędu zapewnia, że:

a) dane osobowe przetwarzane są w sposób legalny, na podstawie art. 6 ust. 1 oraz art. 9 ust. 2,

b) zakres pozyskiwanych danych wynika z przepisów prawa i jest adekwatny do zdefiniowanych celów przetwarzania,

c) określono konkretny czas przez jaki dane są przetwarzane,

d) wobec osób, których dane są przetwarzane wykonano obowiązek informacyjny, zgodnie z art. 13-14 RODO, a wzór klauzul informacyjnych znajduje się w załączniku 2,

e) obowiązek informacyjny wobec osób może być wykonywany poprzez umieszczenie na tablicy informacyjnej w budynku, umieszczeniu go na formularzach lub na stronie internetowej.

f) z wszystkimi współpracującymi podmiotami gospodarczymi podpisano, na mocy art. 28 RODO, umowy powierzenia przetwarzania danych osobowych lub w umowach podstawowych wprowadzono uregulowania odnoszące się do obowiązków zapewnienia przestrzegania przepisów RODO przez te podmioty,

g) jeżeli dane osobowe zostały pozyskane nie bezpośrednio od osób, których dotyczą, administrator musi je o tym powiadomić w sposób umożliwiający im niepodważalne powzięcie takiej wiedzy.

2.2 Dane osobowe są pozyskiwane bezpośrednio od osób lub od innych podmiotów uczestniczących w procesach.

3. Upoważnienia do przetwarzania danych osobowych:

3.1 Administrator do przetwarzania danych osobowych dopuszcza jedynie osoby posiadające stosowne upoważnienia. Wzór stosownych upoważnień stanowi Załącznik nr 3

3.2 Administrator jest odpowiedzialny za proces nadawania i wycofywania upoważnień do przetwarzania danych osobowych.

3.3 Upoważnienia przechowywane są w jednym miejscu.

3.1 Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych, w sposób umożliwiający prawidłową identyfikację historii i prawidłowości procesu przetwarzania danych osobowych. Rejestr jest prowadzony na druku zgodnym z załącznikiem nr 4.

3.2 Ewidencja i upoważnienia prowadzone są przez stanowisko ds. gospodarki odpadami.

3.3 Upoważnienia przechowywane są na stanowisku ds. organizacyjnych i kadrowych.

4. Poufność procesu przetwarzania danych osobowych.

4.1 Każda z osób dopuszczona do przetwarzania danych osobowych lub współpracująca z Urzędem jest zobowiązana do:

a) przetwarzania danych osobowych jedynie w zakresie i jedynie w celu w jakim zostało im wydane upoważnienie lub podpisano umowę powierzenia przetwarzania danych osobowych,

b) zachowania w tajemnicy informacji i danych osobowych, do których posiada dostęp,

c) niewykorzystywania dostępnych danych osobowych do celów sprzecznych z zakresem upoważnienia lub umowy powierzenia przetwarzania danych osobowych,

d) zachowania poufności procesów i metod zabezpieczeń danych osobowych,

e) ochrony informacji i danych osobowych przed przypadkowym, niepożądanym ujawnieniem, modyfikacją, utratą, zniszczeniem danych osobowych czy też nieuprawnionym dostępem osób niepożądanych.

4.2 Osoby dopuszczone do przetwarzania danych osobowych, przed przystąpieniem do pracy, powinny odbyć szkolenie z zasad ochrony danych osobowych, o którym mowa szerzej w Rozdziale VIII.

4.3 Osoby, które zostają dopuszczone do przetwarzania danych osobowych, a które zapoznały się z treścią niniejszej Polityki są zobowiązane do podpisania tzw. oświadczenia o poufności, które jest elementem upoważnienia do przetwarzania danych osobowych.

4.4 Zabronione jest udzielanie wszelkich informacji zawierających dane osobowe osobom, których tożsamości nie można zweryfikować. Weryfikacja tożsamości może odbywać się poprzez żądanie okazania dokumentu tożsamości lub innego dokumentu zawierającego zdjęcie wnioskodawcy lub poprzez wykorzystanie informacji zawartej w dokumentacji, która jest znana jedynie wnioskodawcy. Do tego celu należy wykorzystać metodę pytań bezpośrednich, w których wnioskodawca udzieli poprawnych informacji w co najmniej dwóch zapytaniach.

4.5 Niedopuszczalne jest przekazywanie wszelkich informacji zawierających dane osobowe podmiotom, instytucjom czy też organom, które nie mogą się wykazać prawidłową podstawą prawną dostępu do danych osobowych.

4.6 W przypadku konieczności wydania dokumentów zawierających dane osobowe należy każdorazowo weryfikować tożsamość odbierającego za pomocą mechanizmu, o którym mowa w punkcie 4.4, a w przypadku, kiedy odbierającym nie jest adresat dokumentu należy zażądać upoważnienia.

4.7 Zabrania się eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych np. biurkach, ladach, półkach, parapetach itp.

4.8 Wydruki i inne dokumenty zawierające dane osobowe są przechowywane w pomieszczeniach do tego wyznaczonych. Na stanowiskach pracy mogą być dostępne jedynie dokumenty dotyczące danej sprawy. Stosowana jest zasada tzw. czystego biurka.

4.9 Po zakończeniu pracy wszelka dokumentacja zawierająca dane osobowe jest przechowywana w szafach zamykanych na klucz lub w pomieszczeniach o ograniczonym dostępie osób postronnych, do których dostęp jest utrudniony poprzez zastosowanie zabezpieczeń fizycznych takich jak: zamki w drzwiach, kraty w oknach, systemy kontroli dostępu itp.

4.10 Wszelkie dokumenty zawierające dane osobowe niszczone są z użyciem niszczarek.

4.11 Zaleca się zwrócenie szczególnej uwagi pracownikom na sytuację przypadkowego pozostawienia dokumentów zawierających dane osobowe w miejscach ogólnodostępnych, przy kopiarkach, przy drukarkach itp.

4.12 Administrator jest zobowiązany do corocznej weryfikacji posiadanych zbiorów danych osobowych, które mają na celu wyeliminowanie danych, do których ustały podstawy przetwarzania.

5. Współpraca z podmiotami zewnętrznymi

5.1 W działalności Urzędu jest dopuszczalna współpraca z podmiotami zewnętrznymi, którym udostępnia się dane osobowe.

5.2 Powierzenie przetwarzania danych osobowych może odbywać się jedynie na podstawie umowy lub innego instrumentu prawnego, zgodnie z zasadami określonymi w art. 28 RODO.

5.3 Wzór umowy powierzenia stanowi załącznik nr 5.

5.4 Prowadzona jest ewidencja podmiotów, z którymi podpisano umowy powierzenia, którego wzór stanowi Załącznik nr 6.

5.5 Ewidencja prowadzona jest przez stanowisko ds. gospodarki odpadami.

6. Udostępnianie danych

6.1 Urząd udostępnia dane osobowe jedynie na podstawie obowiązujących przepisów prawa i w granicach prawa.

6.2 Wzór ewidencji udostępnionych danych w trybie, o którym mowa w punkcie 6.1 stanowi załącznik nr 7.

6.3 Każdy referat lub samodzielne stanowisko prowadzi ewidencję, o której mowa w pkt 6.2.

6.4 Urząd przekazując dane drogą pocztową przekazuje je listem poleconym za potwierdzeniem odbioru.

6.5 W przypadku udostępniania dokumentów za pomocą korespondencji mailowej pracownik ma obowiązek szyfrować przekazywane pliki.

7. Uprawnienia osób, których dane osobowe są przetwarzane

7.1 Urząd zapewnia osobom, których dane osobowe przetwarza, realizację wszystkich przysługujących im praw.

7.2 W przypadku zastosowania ograniczenia praw osób, należy taką sytuację pisemnie wyjaśnić osobie, która wniosła sprawę w zakresie realizacji jej praw.

7.3 Prawa realizowane są zgodnie z przyjętą procedurą, która stanowi załącznik do Polityki.

## II. Ryzyko

1. Analiza ryzyka

1.1. W Urzędzie przeprowadzana jest analiza ryzyka. Analiza ryzyka może odbywać się dla procesów przetwarzania oraz sprzętu mającego istotny wpływ na bezpieczeństwo jednostki.

1.2. Analiza ryzyka przeprowadzana jest w celu określenia, oceny i minimalizacji zagrożeń, których efektem ma być wdrożenie optymalnych i adekwatnych zabezpieczeń.

1.3. Analiza ryzyka przeprowadzona jest corocznie, nie później niż do dnia 31 marca lub w przypadku wprowadzenia nowych procedur lub rozwiązań organizacyjnych, zgodnie z procedurą analizy ryzyka opisaną w dokumencie Metodyka Analizy Ryzyka

2. Ocena skutków dla ochrony danych osobowych

2.1. Dla zbiorów danych osobowych, w których znajdują się dane osobowe, których nieuprawnione ujawnienie wiąże się z wysokim ryzykiem uszczerbku dla osób, których dane dotyczą przeprowadzana jest ocena skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO.

2.2. Ocena skutków dla ochrony danych osobowych polega na:

a) opisie planowanych operacji i celów przetwarzania,

b) opisie i ocenie przez administratora czy planowane operacje przetwarzania są niezbędne i proporcjonalne w stosunku do celów,

c) ocenie ryzyka naruszenia praw lub wolności osób, których dane dotyczą,

d) opisie środków planowanych w celu zaradzenia ryzykiem, w tym określeniu mechanizmów, zabezpieczeń i środków technicznych, mających zapewnić bezpieczeństwo procesu,

2.3. Ocena skutków dla ochrony danych może być wykonywana przy pomocy dedykowanego oprogramowania.

3. Polityka zarządzania ryzykiem

3.1. Czynności, o których mowa w punkcie II stanowią politykę zarządzania ryzykiem

3.2. Za nadzór nad realizacją polityki zarządzania ryzykiem odpowiada Administrator.

3.3. Polityką zarządzania ryzykiem administruje wyznaczony pracownik. Analiza ryzyka i ocena skutków dla systemu ochrony danych może odbywać się przy udziale Inspektora Ochrony Danych.

3.4. Wyznaczony pracownik ma obowiązek sporządzenia corocznego raportu związanego z ryzykiem w nie później niż do 30 kwietnia.

## III. Inspektor Ochrony Danych Osobowych

Inspektor Ochrony Danych wyznaczany jest dla celu zarządzania bezpieczeństwem danych osobowych w Urzędzie.

1. Za wyznaczenie Inspektora Ochrony Danych odpowiada Administrator.
2. Inspektorem Ochrony Danych może być jedynie osoba, która posiada fachową wiedzę na temat prawa i praktyki w ochronie danych osobowych.
3. Inspektor Danych Osobowych nie musi być pracownikiem Urzędu.
4. Administrator jest zobowiązany do udostępnienia danych kontaktowych Inspektora Ochrony Danych w sposób umożliwiający jego identyfikację i kontakt oraz jest zobowiązany powiadomić o nich organ nadzorczy.

4.1 Poprzez udostępnienie danych Inspektora Ochrony Danych należy rozumieć, co najmniej ich publikację na stronie internetowej administratora oraz w widocznym miejscu, w siedzibie administratora.

5. Administrator ma obowiązek zapewnić Inspektorowi Ochrony Danych możliwość wykonywania jego obowiązków w sposób niezależny i zapewnić mu status, o którym mowa w art. 38 RODO.
6. Zadania Inspektora Ochrony Danych:
   6.1 informowanie administratora podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i innych przepisów regulujących tą materię,
   6.2 monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów,
   6.3 podejmowanie działań zwiększających świadomość personelu, inicjowanie i organizowanie szkoleń personelu uczestniczącego w operacjach przetwarzania,
   6.4 przeprowadzanie wewnętrznych audytów,
   6.5 udzielanie na żądanie administratora zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z rozdziałem II niniejszego dokumentu,
   6.6 współpraca z organem nadzorczym,
   6.7 pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
7. Dane kontaktowe Inspektora Ochrony Danych są przekazywane organowi nadzorczemu według trybu i za pomocą narzędzi opracowanych i wdrożonych przez organ nadzoru.

## IV. Rejestr czynności przetwarzania

1. W Urzędzie prowadzony jest Rejestr czynności przetwarzania danych osobowych.
2. Rejestr czynności przetwarzania winien zawierać co najmniej informacje, o których mowa w art. 30 RODO.
3. Rejestr czynności przetwarzania jest prowadzony w oparciu o załącznik nr 1.
4. W przypadku gdy Urząd staje się podmiotem przetwarzającym prowadzony jest Rejestr kategorii czynności przetwarzania w oparciu o załącznik nr 1A.

## V. Zasady postępowania w przypadku naruszenia systemu ochrony danych

1. Każda osoba, której Administrator wydał upoważnienie do przetwarzania danych osobowych, ma obowiązek natychmiastowego powiadamiania o występującym zagrożeniu lub wystąpieniu incydentu związanego z systemem ochrony danych osobowych.
2. Powiadomienie to może mieć charakter ustny lub pisemny.
3. Adresatem takiego powiadomienia jest Inspektor Ochrony Danych.

4. Po otrzymaniu takiego powiadomienia Inspektor Ochrony Danych podejmuje niezwłocznie czynności w celu ustalenia stanu faktycznego.
5. W przypadku uzasadnionego podejrzenia wystąpienia incydentu lub naruszenia systemu ochrony danych osobowych podejmuje działania mające zapobiec dalszym skutkom oraz powiadamia administratora.
6. Po dokonaniu czynności zabezpieczających, Inspektor Ochrony Danych, ma za zadanie przeprowadzić postępowanie wyjaśniające, które:
   6.1 ustali ostateczny zakres, przyczyny wystąpienia oraz skutki, zarówno dla Urzędu, jak i osób, których dane dotyczyły,
   6.2 podejmuje niezbędne czynności mające na celu przywrócenie prawidłowości działania systemu ochrony danych osobowych w Urzędzie,
   6.3 opracowuje działania naprawcze i zapobiegawcze, których zadaniem jest wyeliminowanie niepożądanych zdarzeń w przyszłości,
   6.4 wskazuje osoby odpowiedzialne za wystąpienie sytuacji.
7. Powyższe czynności są dokumentowane przez Inspektora Ochrony Danych Osobowych za pomocą formularza, którego wzór stanowi załącznik nr 8.
8. Rejestr formularzy, o których mowa w punkcie 7 niniejszego rozdziału prowadzi Inspektor Ochrony Danych przy pomocy ewidencji, która stanowi załącznik nr 8A.
9. Inspektor Ochrony Danych Osobowych ma obowiązek przedstawienia raportu Administratorowi w czasie umożliwiającym Administratorowi powiadomienie o incydencie lub naruszeniu systemu ochrony danych osobowych organu nadzorczego nie później niż na 72 godziny od czasu jego wykrycia.
10. Dla szczegółowego wyjaśnienia stworzona została Instrukcja postępowania w sytuacji naruszenia ochrony danych.

## VI. Kontrole wewnętrzne i audyty bezpieczeństwa

1. Kontrolą systemów służących do przetwarzania danych osobowych zajmuje się Inspektor Ochrony Danych.
2. Kontrole przeprowadzane są regularnie, co najmniej raz do roku, a w przypadku wystąpienia incydentu , kompleksową kontrolę obejmującą wszystkie aspekty działalności rozpoczyna się nie później niż 7 dni po zakończeniu działań związanych z incydentem, który wystąpił.
3. Kontrola przeprowadzana jest z zastrzeżeniem wymogów i terminów określonych w RODO.
4. Kontrola przeprowadzana jest przy uwzględnieniu minimalnych wytycznych jakimi są: badanie pod względem zgodności z prawem, branżowymi standardami postępowania, normami i przepisami wewnętrznymi.
5. Inspektor Ochrony Danych może wykonywać kontrole osobiście, może, przy aprobacie Administratora wyznaczyć do tego inną osobę lub podmiot.
6. Kontrole przeprowadzane są na podstawie programów kontroli, w których opisywany jest ich zakres, termin, cele oraz metody ich przeprowadzania oraz doraźnie.

7. Proces kontroli musi być dokumentowany i uzupełniony pozyskaniem obiektywnych dowodów na prawidłowość procesu kontrolnego.
8. Jeśli podczas kontroli stwierdzone zostają nieprawidłowości zagrażające systemowi ochrony danych osobowych, kontroler musi niezwłocznie powiadomić o tym fakcie administratora.
9. Wynik kontroli musi być udokumentowany i przekazany administratorowi.
10. Administrator może zlecić badanie audytowe niezależnemu podmiotowi, po poinformowaniu o tym fakcie Inspektora Ochrony Danych.

## VII. Postępowanie dyscyplinarne

1. Pracownicy i podmioty współpracujące mają bezwzględny obowiązek stosowania przepisów prawa i przepisów wewnętrznych obowiązujących w Urzędzie w zakresie ochrony danych osobowych.
2. W przypadku wystąpienia incydentu, naruszenia procedur czy też zaniechania czynności wynikających z obowiązków w zakresie ochrony danych osobowych, wszystkie takie czynności będą traktowane jako ciężkie naruszenie zasad i stosunków formalnych panujących w Urzędzie.
3. Administrator, jako Pracodawca, ma prawo do potraktowania działań, o których mowa w punkcie 2 powyżej jako działań podlegającej sankcjom karnym wynikającym z RODO lub innych przepisów krajowych w zakresie organizacji procesu ochrony danych osobowych i jest uprawniony do złożenia stosownych doniesień do organów nadzorczych.

## VIII. Szkolenia personelu

1. Każdy pracownik/współpracownik Urzędu, przed przystąpieniem do pracy na zbiorach danych osobowych musi zostać przeszkolony w zakresie przepisów związanych z ochroną danych osobowych.
2. Za przeprowadzenie szkoleń odpowiada Inspektor Ochrony Danych.
3. Szkolenie może być przeprowadzone za pomocą szkolenia multimedialnego.
4. Inspektor Ochrony Danych przeprowadza szkolenia w miarę potrzeb, po każdej zmianie przepisów mających znaczenie dla procesów ochrony danych osobowych oraz nie rzadziej niż raz na 24 miesięce.

## IX. Wykaz zabezpieczeń

1. W Urzędzie prowadzony jest wykaz zabezpieczeń organizacyjnych, technicznych, fizycznych i personalnych, w którym w sposób usystematyzowany opisano procedury zabezpieczeń.
2. Wykaz, o którym mowa w punkcie powyżej prowadzi Administrator.
3. Wykaz prowadzony jest w formie papierowej i elektronicznej, zgodnie z załącznikiem nr 9.
4. Wykaz winien być aktualizowany każdorazowo po wprowadzeniu nowych rozwiązań oraz po analizie ryzyka, o ile jej wynik tego wymaga.
5. Procedura postępowania z kluczami wprowadzona została oddzielnym dokumentem.

## X. Wykaz załączników

1. Wzór rejestru czynności przetwarzania danych osobowych
   1A. Wzór rejestru kategorii czynności przetwarzania
2. Wzór obowiązku informacyjnego
3. Wzór upoważnienia do przetwarzania danych osobowych
4. Wzór ewidencji osób upoważnionych do przetwarzania danych
5. Wzór umowy powierzenia przetwarzania danych
6. Wzór ewidencji umów powierzenia
7. Wzór ewidencji udostępnienia danych
8. Wzór raportu z naruszenia ochrony danych
   8A. Wzór ewidencji incydentów
9. Wykaz zabezpieczeń
   9A. Lista potencjalnych zabezpieczeń
10. Instrukcja zarządzania systemami informatycznymi
11. Procedura postępowania z prawami osób
    11A Wzór ewidencji realizacji prawa osób
12. Metodyka analizy ryzyka
    12A Arkusz analizy ryzyka

Załącznik nr 1

**Wzór**
**Rejestru czynności przetwarzania danych osobowych**

| **Nazwa czynności przetwarzania** (1) | |
|---|---|
| **Jednostka organizacyjna**<br>(departament, dział itp.) | |
| **Cel przetwarzania**<br>art. 30 ust. 1 pkt b | |
| **Kategorie osób**<br>art. 30 ust. 1 pkt c | |
| **Kategorie danych osobowych**<br>art. 30 ust. 1 pkt c | |
| **Podstawa prawna** | |
| **Źródło danych** | |
| **Planowany termin usunięcia kategorii danych**<br>(jeżeli jest to możliwe)<br>**art. 30 ust. 1 pkt f** | |
| **Nazwa współadministratora i dane kontaktowe**<br>(jeśli dotyczy)<br>**art. 30 ust. 1 pkt d** | |
| **Nazwa podmiotu przetwarzającego i dane kontaktowe**<br>(jeśli dotyczy)<br>**art. 30 ust. 1 pkt d** | |
| **Kategorie odbiorców**<br>(innych niż podmiot przetwarzający)<br>**art. 30 ust. 1 pkt d** | |
| **Nazwa systemu lub oprogramowania** | |
| **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa**<br>**zgodnie z art. 32 ust. 1**<br>(jeżeli jest to możliwe)<br>**art. 30 ust. 1 pkt g** | |
| **DPIA – Ocena skutków**<br>(jeśli tak, lokalizacja raportu) | |
| **Transfer do kraju trzeciego lub organizacji międzynarodowej**<br>(nazwa kraju i podmiotu)<br>**Art. 30 ust. 1 pkt e** | |
| **Jeśli transfer i art. 49 ust. 1 akapit drugi – dokumentacja odpowiednich zabezpieczeń**<br>**art. 30 ust. 1 pkt e** | |

Załącznik nr 1A

**Wzór**
**Rejestru kategorii czynności przetwarzania danych osobowych**

| | | |
|---|---|---|
| Kategorie przetwarzań<br>Art. 30 ust. 2 lit. b | | |
| Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)<br>Art. 30 ust. 2 lit. d, art. 32 ust. 1 | | |
| Administrator<br>Art. 30 ust. 2 lit. a | Nazwa i dane kontaktowe administratora | |
| | Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)" | |
| | Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono) | |
| | Inspektor ochrony danych administratora (jeśli powołano) | |
| Czas trwania przetwarzania | | |
| Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane<br>Art. 30 ust. 2 lit. c | | |
| Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi<br>Art. 30 ust. 2 lit. c | | |
| Podprzetwarzający (podwykonawca) - jeśli dotyczy | | |
| Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy) | | |

Załącznik nr 2

**Wzór**
**obowiązku informacyjnego**

## KLAUZULA INFORMACYJNA DLA KLIENTÓW URZĘDU GMINY W KOŁACZKOWIE

W związku z realizacją wymogów 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 „RODO"), informujemy o zasadach przetwarzania Pani/Pana danych osobowych oraz o przysługujących Pani/Panu prawach z tym związanych.

1. **Administratorem** Pani/Pana danych osobowych przetwarzanych w Urzędzie Gminy w Kołaczkowie jest: **Wójt Gminy Kołaczkowo** z siedzibą w Urzędzie Gminy, Plac Reymonta 3, 62-306 Kołaczkowo.
2. Jeśli ma Pani/Pan pytania dotyczące sposobu i zakresu przetwarzania Pani/Pana danych osobowych w zakresie działania Urzędu Gminy w Kołaczkowie, a także przysługujących Pani/Panu uprawnień, może się Pani/Pan skontaktować się z Inspektorem Ochrony Danych Osobowych za pomocą adresu .....
3. Administrator danych osobowych – Wójt Gminy Kołaczkowo - przetwarza Pani/Pana dane osobowe na podstawie obowiązujących przepisów prawa, zawartych umów oraz na podstawie udzielonej zgody.
4. Pani/Pana dane osobowe przetwarzane są w celu/celach:
   a) wypełnienia obowiązków prawnych ciążących na Urzędzie Gminy w Kołaczkowie,
   b) realizacji umów zawartych z kontrahentami Gminy Kołaczkowo.
   W pozostałych przypadkach Pani/Pana dane osobowe przetwarzane są wyłącznie na podstawie wcześniej udzielonej zgody w zakresie i celu określonym w treści zgody.
5. Odbiorcami Pani/Pana danych osobowych będą wyłącznie organy władzy publicznej oraz podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów powszechnie obowiązującego prawa, a także inne podmioty, które na podstawie stosownych umów podpisanych z Gminą Kołaczkowo przetwarzają dane osobowe, dla których Administratorem jest Wójt Gminy Kołaczkowo.
6. Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do realizacji celów określonych w pkt 4, a po tym czasie przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa.
7. W związku z przetwarzaniem Pani/Pana danych osobowych przysługują Pani/Panu następujące uprawnienia:
   a) prawo dostępu do swoich danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, chyba że przepisy szczegółowe stanowią inaczej,
   b) prawo do wniesienia sprzeciwu wobec przetwarzania, chyba że przepisy szczegółowe stanowią inaczej,
   c) cofnięcia zgody w dowolnym momencie (ma zastosowanie, jedynie gdy przetwarzanie odbywa się na podstawie zgody, skorzystanie z prawa do cofnięcia zgody nie ma wpływu na przetwarzanie, które miało miejsce do momentu wycofania zgody),
   d) przenoszenia danych (ma zastosowanie, jedynie, gdy przetwarzanie odbywa się na podstawie zgody wyrażonej przez osobę, której dane dotyczą lub umowy, której jest stroną),
8. Przysługuje Pani/Panu prawo **wniesienia skargi** do organu nadzorczego, którym jest **Prezes Urzędu Ochrony Danych Osobowych**, gdy stwierdzi Pani/Pan naruszenie przetwarzania danych osobowych Pani/Pana dotyczących.
9. Pani/Pana dane nie będą podlegać zautomatyzowanemu podejmowaniu decyzji w tym profilowaniu.
10. W sytuacji, gdy przetwarzanie danych osobowych odbywa się na podstawie zgody osoby, której dane dotyczą, podanie przez Panią/Pana danych osobowych Administratorowi ma charakter dobrowolny.
11. Podanie przez Panią/Pana danych osobowych jest obowiązkowe, w sytuacji gdy przesłankę przetwarzania danych osobowych stanowi przepis prawa lub zawarta między stronami umowa.

Załącznik nr 3

**Wzór**
**Upoważnienia do przetwarzania danych osobowych**

## UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 ogólnego rozporządzenia o ochronie danych * z dniem _____ upoważniam Panią/Pana _____

*podać imię i nazwisko osoby upoważnionej*

do przetwarzania danych osobowych, administrowanych lub/i powierzonych do przetwarzania Administratorowi, w postaci papierowej oraz w ramach nadanych dostępów do systemów informatycznych, zgodnie z zajmowanym stanowiskiem.
Polecam Pani / Panu przetwarzanie danych osobowych zgodnie z nadanym upoważnieniem.
Jednocześnie, wraz z nadanym upoważnieniem, zobowiązuję Panią/Pana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz regulacji wewnętrznych wprowadzonych i wdrożonych do stosowania przez Administratora.

**Niniejsze upoważnienie traci moc:**
najpóźniej z dniem odwołania albo rozwiązania lub wygaśnięcia umowy o pracę, a także z chwilą zmiany stanowiska pracy i zmiany danych osobowych pracownika.
* ROZPORZĄDZENIA 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

### OŚWIADCZENIE

Oświadczam, iż zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych oraz regulacjami wewnętrznymi wprowadzonymi i wdrożonymi do stosowania przez Administratora, także w zakresie dotyczącym bezpieczeństwa informacji.

Zobowiązuję się do:

- zachowania w tajemnicy danych osobowych jak również innych informacji prawnie chronionych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych,
- niewykorzystywania danych osobowych oraz innych informacji w celach pozasłużbowych o ile nie są one jawne,
- zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia oraz innych informacji o ile nie są one jawne, także po ustaniu zatrudnienia,
- korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora,
- należytej dbałości o sprzęt i oprogramowanie zgodnie z regulacjami wewnętrznymi,
- nieudostępniania sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu postanowień Kodeksu Pracy lub za naruszenie przepisów karnych w rozumieniu przepisów dziedzinowych o ochronie informacji prawnie chronionych.

---
Podpis pracownika

---
Podpis Administratora

Załącznik nr 4

**Wzór**
**Ewidencji osób upoważnionych**

| *Lp.* | *Nazwisko i Imię* | *Identyfikator (login do systemów)* | *Data nadania upoważnienia* | *Data odebrania upoważnienia* | *Zakres* | *Uwagi* |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |
| 6 | | | | | | |

**Wzór**
**umowy powierzenia przetwarzania danych**

**Umowa powierzenia przetwarzania danych osobowych**

zawarta dnia _____ pomiędzy:

(zwana dalej „**Umową**")

_____

zwany w dalszej części „**Administratorem**"

reprezentowanym przez:

_____

a

_____

zwany w dalszej części „**Podmiotem przetwarzającym**"

(*dane podmiotu, który będzie przetwarzać dane osobowe w imieniu Administratora*)

reprezentowanym przez:

_____

zwane też w dalszej części „**Stronami**"

Niniejsza umowa została zawarta na podstawie przepisów dotyczących 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) zwane w dalszej części „**Rozporządzeniem**".

§ 1

**Powierzenie przetwarzania danych osobowych**

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 Rozporządzenia, dane osobowe do przetwarzania na zasadach i w celu określonym w niniejszej Umowie.
2. Administrator oświadcza, że jest Administratorem danych, które powierza Podmiotowi przetwarzającemu.
3. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Podmiot przetwarzający oświadcza, że stosuje środki bezpieczeństwa spełniające wymogi RODO określone w § 3 ust. 1 niniejszej Umowy.

§ 2

**Zakres i cel przetwarzania danych**

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie niniejszej Umowy dane. Dane te zostały określone w załączniku 1 do umowy.
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu określonym w załączniku nr 1.

## § 3

### Obowiązki i prawa Stron

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających odpowiedni stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający określa ogólny opis zabezpieczeń w załączniku nr 1.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej Umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust. 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem zobowiązany jest do działania określonego w załączniku 1.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych niezwłocznie zgłasza je Administratorowi nie później niż w ciągu 48 godzin.
8. Administrator zgodnie z art. 28 ust. 3 pkt h Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy.
9. Administrator realizować będzie prawo kontroli zgodnie z załącznikiem 1.
10. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora.
11. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

## § 4

### Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Podmiot przetwarzający zobowiązuje się do korzystania z usług wyłącznie takich podwykonawców, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie przez tych podwykonawców danych osobowych, spełniało wymogi Rozporządzenia.
3. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
4. Podwykonawca winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
5. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.
6. Podmioty, którym dane Administratora zostały powierzone przez Podmiot przetwarzający wymienia się w załączniku 1.

## § 5

### Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie, a także:
   a) o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego,
   b) o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczą-

cych przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez organ nadzorczy. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

## § 6

## Czas obowiązywania Umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas określony w załącznik 1.
2. Każda ze stron może wypowiedzieć niniejszą Umowę z zachowaniem okresu opisanego w załączniku 1.

## § 7

## Rozwiązanie umowy

1. Administrator może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z Umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.

## § 8

## Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne"). Podjęte zobowiązanie pozostaje w mocy w czasie trwania i po zakończeniu przetwarzania w ramach powierzenia danych osobowych.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonania Umowy, chyba że konieczność ujawnienia informacji wynika z obowiązujących przepisów prawa lub Umowy.

## § 9

## Postanowienia końcowe

1. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze Stron.
3. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
4. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy Administratora przetwarzającego.

Administrator

Podmiot przetwarzający

Załącznik nr 1 do **Umowy powierzenia przetwarzania danych osobowych**

1. Zakres powierzonych danych:

*(rodzaje danych osobowych: zwykłe/szczególnej kategorii/dotyczące wyroków skazujących i naruszeń prawa, przykładowe kategorie osób, których dane dotyczą: pracownicy/klienci/kontrahenci Administratora w postaci np. imion i nazwisk/adresów zamieszkania/PESEL)*

2. *Cel przetwarzania powierzonych danych*

*(np. w celu realizacji umowy z dnia ..... w zakresie świadczenia usług kadrowo-płacowych)*

3. *Zastosowane zabezpieczenia – ogólny opis.*

4. *Rodzaj działania z danymi po zakończeniu umowy*

*(zwrot/usunięcie, określenie czasu na wykonanie działania)*

5. *Kontrola podmiotu przetwarzającego*

*(określenie godzin kontroli, określenie czasu na poinformowanie podmiotu przetwarzającego o zamiarze kontroli)*

6. *Podmioty podpowierzenia*

*(należy wskazać podmioty, pełne nazwy wraz z adresem, którym dane powierzył podmiot przetwarzający)*

7. *Okres ważności umowy*

*(data obowiązywania umowy)*

8. *Okres wypowiedzenia*

*(należy określić okres wypowiedzenia)*

Załącznik nr 6

**Wzór**
**ewidencji umów powierzenia**

| *Lp.* | *Podmiot przetwarzający* | *Kategorie danych* | *Data podpisania* | *Data obowiązywania* | *Czynności powierzenia* | *Osoba kontaktowa* |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |
| 6 | | | | | | |

Załącznik nr 7

**Wzór**
**Ewidencji udostępnienia danych**

| *Lp.* | *Podmiot wnioskujący* | *Osoba, które wniosek dotyczy* | *Podstawa udostępnienia* | *Data udostępnienia* | *Uwagi* |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| 6 | | | | | |

Załącznik nr 8

**Wzór**
**Raportu z naruszenia ochrony danych osobowych**

| **Raport nr ... z naruszenia ochrony danych osobowych** | | | |
|---|---|---|---|
| *Data poinformowania o naruszeniu* | | *Godzina* | |
| *Data wystąpienia naruszenia* | | *Godzina wystąpienia naruszenia* | |
| *Osoba powiadamiająca o zaistniałym zdarzeniu (Imię i nazwisko, stanowisko służbowe)* | | | |
| *Lokalizacja zdarzenia ( okoju, nazwa pomieszczenia lub nazwa i dane kontaktowe podmiotu przetwarzającego u którego doszło do naruszenia)* | | | |
| *Rodzaj naruszenia bezpieczeństwa, oraz okoliczności towarzyszące* | | | |
| *Podjęte działania (korekcja)* | | | |
| *Przyczyny wystąpienia zdarzenia* | | | |
| *Działania korygujące* | | | |
| *Decyzja co do zgłoszenia naruszenia do Organu Nadzorczego oraz jej adnienie* | | | |
| *Data zawiadomienia* | | *Godzina zawiadomienia* | |
| *Decyzja co do poinformowania osób których dane dotyczą i jej uzasadnienie* | | | |
| *Data zawiadomienia* | | *Forma zawiadomienia* | |
| *Data i podpis Inspektora Ochrony Danych lub osoby upoważnionej* | | | |

Załącznik nr 8A

**Wzór**
**Ewidencji incydentów**

| LP. | DATA ZGŁOSZENIA | OSOBA ZGŁASZAJĄCA DO IOD | OPIS | DATA WYSTĄPIENIA | KOREKCJA | DZIAŁANIA KORYGUJĄCE |
|---|---|---|---|---|---|---|
| 1. | | | | | | |
| 2. | | | | | | |
| 3. | | | | | | |
| 4. | | | | | | |
| 5. | | | | | | |
| 6. | | | | | | |
| 7. | | | | | | |
| 8. | | | | | | |

Załącznik nr 9

*Należy wykorzystać materiał z Załącznika nr 9A*

## Wykaz zabezpieczeń

**Wykaz zabezpieczeń w .....**

**Rodzaje stosowanych zabezpieczeń:**

| **Rodzaj zabezpieczenia** | **Organizacyjne** |
|---|---|
| | |
| | |
| | |
| **Rodzaj zabezpieczenia** | **Personalne** |
| | |
| | |
| | |
| **Rodzaj zabezpieczenia** | **Fizyczne** |
| | |
| | |
| | |
| | |
| **Rodzaj zabezpieczenia** | **Techniczne** |
| | |
| | |

| RODZAJ ZABEZPIECZENIA | Lista potencjalnych zabezpieczeń |
|---|---|
| Organizacyjne | Zabezpieczenie odpowiednich środków finansowych zapewniających wymianę sprzętu (zgodnie z obowiązującą w Izbie strategią rozwoju informatyzacji) |
| Organizacyjne | Zapory sieciowe skonfigurowane według zasady "wszystko jest zabronione, z wyjątkiem tego na co wyrażono zgodę" |
| Personalne | Umowy serwisowe (powierzenia, SLA, kary umowne) |
| Personalne | Bezpieczeństwo informacji w zarządzaniu projektami - bezpieczeństwo informacji należy uwzględniać w każdym projekcie (obowiązkowa współpraca z IOD) |
| Personalne | Aktualizacja zakresów odpowiedzialności i obowiązków w zakresie bezpieczeństwa informacji |
| Personalne | Zwrot aktywów - wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia, powinni zwrócić wszystkie posiadane aktywa Izby |
| Personalne | Sformalizowany proces rejestrowania i wyrejestrowywania użytkowników |
| Personalne | Sformalizowany proces przydzielania dostępu użytkownikom do wszystkich systemów i usług |
| Personalne | Ograniczenie i nadzorowanie przyznawania praw uprzywilejowanego dostępu |
| Personalne | Sformalizowany proces przydzielania poufnych informacji uwierzytelniającymi użytkowników |
| Personalne | Przeglądy praw dostępu użytkowników, odbywające się regularnych odstępach czasu |
| Personalne | Odbieranie praw dostępu - wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia, powinni mieć odebrane wszystkie prawa dostępu |
| Techniczne | System kontroli dostępu (karty wejścia/wyjścia, czytniki biometryczne) |
| Techniczne | Monitoring środowiskowy (czujki wilgotności, pomiary temperatury, ...) |
| Techniczne | Systemy UPS i/lub agregaty prądotwórcze |
| Techniczne | Monitorowanie zużycia - systemy monitorujące stan usług i zasobów krytycznych, serwerów, baz danych i urządzeń technicznych, dla zapewnienia właściwej wydajności systemu |
| Techniczne | System przeciwpożarowy |
| Techniczne | System zarządzania hasłami - interaktywny i zapewniający wybór haseł dobrej jakości |
| Techniczne | Ograniczenie i nadzór nad wykorzystywaniem programów narzędziowych, umożliwiających obejście zabezpieczeń systemowych |
| Techniczne | Ograniczenie / uniemożliwienie dostępu do kodów źródłowych programów |
| Techniczne | Aktualizacje systemu |
| Techniczne | Analityczny system do wykrywania zagrożeń (SIEM) |
| Techniczne | Klimatyzacja |
| Techniczne | Redundancja krytycznych zasobów (macierz dyskowa RAID3, redundancja łącz, ...) |
| Techniczne | Sondy IDS / IPS do ochrony dostępności do sieci komputerowej |
| Techniczne | System wykrywania słabości i podatności (skanery podatności) |
| Techniczne | Systemy do inwentaryzacji sprzętu, zarządzania licencjami, monitoring użytkowników |
| Techniczne | Systemy firewall, NG firewall, UTM |
| Techniczne | Szyfrowanie (poczty SSL, połączeń internetowych SSl/VPN, Pendrive, dysków komputerowych przenośnych (BitLocker), plików (7zip) itp. |
| Techniczne | Testy penetracyjne |
| Techniczne | Utwardzanie systemów (hardening) - kompleksowe działania zmierzające do optymalizacji działania i poprawy stanu zabezpieczeń systemów operacyjnych serwerów oraz urządzeń końcowych pracujących w |
| Techniczne | Wirtualizacja - uruchamianie wielu systemów operacyjnych na tej samej platformie sprzętowej i systemowej |
| Techniczne | Autoryzacja dostępu do serwera DHCP |
| Techniczne | Blokowanie możliwości instalowania oprogramowania przez użytkownika |
| Techniczne | Blokowanie portów USB na stacjach roboczych |
| Techniczne | Blokowanie ruchu sieciowego z określonych adresów IP |
| Techniczne | Budowanie topologii sieci z uwzględnieniem obszarów bezpiecznych i zdemilitaryzowanych (DMZ) |
| Techniczne | Monitorowanie ruchu sieci |
| Techniczne | Nadzór nad ruchem wychodzącym |
| Techniczne | Okresowe przeglądanie logów stacji roboczej przez administratorów |
| Techniczne | Oprogramowanie klasy AV na stacjach roboczych |
| Techniczne | Oprogramowanie klasy AV na styku sieci WAN z LAN |
| Techniczne | Przejście na statyczne wersje serwisu po wykryciu ataku typu DDoS/DoS |
| Techniczne | Serwery PROXY (w tym utrzymywanie czarnej listy adresów URL oraz adresów IP) |
| Techniczne | Stosowanie strefowania |
| Techniczne | Stosowanie techniki rozpraszania danych (CDN - conten delivery network) |
| Techniczne | Systemy klasy IDS/IPS |
| Techniczne | Translacja adresów sieciowych |
| Techniczne | Weryfikacja, czy na stacji roboczej znajduje się wyłącznie dopuszczalne oprogramowanie |
| Techniczne | Wykrycie nielegalnych działań ze strony użytkowników wewnętrznych systemu |
| Techniczne | Wykrywanie i blokowanie spamu |
| Techniczne | Rozliczalność operacji |

Załącznik nr 9A

| RODZAJ ZABEZPIECZENIA | Lista potencjalnych zabezpieczeń |
|---|---|
| Fizyczne | Strefy dostępu określające obszar, w którym przetwarzane są dane wrażliwe lub krytyczne |
| Fizyczne | Zabezpieczenie dostępu do serwerowni (drzwi zamykane na klucz, wejście kodowane, czytnik biometryczny itp.) |
| Fizyczne | Zabezpieczenie dostępu do archiwum (drzwi zamykane na klucz, drzwi ognioodporne, drzwi antywłamaniowe itp.) |
| Fizyczne | Ochrona fizyczna obiektu i/lub pomieszczeń |
| Fizyczne | Systemy alarmowe / zabezpieczenia antywłamaniowe |
| Fizyczne | Monitoring wizyjny |
| Fizyczne | Zabezpieczenia dostępu do lokalu i pomieszczeń (drzwi zamykane na klucz, drzwi ognioodporne, drzwi antywłamaniowe itp.) |
| Fizyczne | Regularne wykonywanie i testowanie kopii informacji, oprogramowania i obrazów systemów zgodnie z procedurą kopi zapasowych |
| Fizyczne | Bezpieczne wycofywanie nośników - nośniki, które nie będą dalej wykorzystywane, należy bezpiecznie wycofać, zgodnie z formalnymi procedurami |
| Fizyczne | Bezpieczne przekazywanie nośników - nośniki zawierające informacje należy chronić przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu |
| Fizyczne | Ograniczenie dostępu do pomieszczeń i sprzętu |
| Fizyczne | Zabezpieczenie dokumentacji w pomieszczeniach (zamknięte metalowe/niemetalowe szafy, sejf, skrytki itp.) |
| Fizyczne | Ekranowanie pomieszczeń |
| Fizyczne | Nadzór nad niewykorzystywanymi zakończeniami sieci LAN |
| Fizyczne | Nadzór nad niewykorzystywanymi zakończeniami sieci LAN (odłączenie niewykorzystanych zakończeń na krosownicach) |
| Fizyczne | prowadzenie okablowania sieciowego w zamkniętych kanałach, nadzór nad krosownicami |
| Fizyczne | Stosowanie światłowodów w miejsce połączeń galwanicznych |
| Organizacyjne | Polityka stosowania zabezpieczeń kryptograficznych |
| Organizacyjne | Polityka dotycząca korzystania, ochrony i okresów ważności kluczy kryptograficznych |
| Organizacyjne | Umowy na serwis i konserwację sprzętu w celu zapewnienia jego ciągłej dostępności i integralności |
| Organizacyjne | Nadawanie i nadzór nad udzielonymi zezwoleniami dotyczącymi wynoszenia poza Izbę sprzętu, informacji i programów |
| Organizacyjne | Polityka czystego biurka i ekranu |
| Organizacyjne | Procedury eksploatacyjne |
| Organizacyjne | Procedura kopii zapasowych |
| Organizacyjne | Zasady instalowania oprogramowania przez użytkowników |
| Organizacyjne | Klauzule w umowach dotyczących wszystkich usług sieciowych, zawierające zidentyfikowane mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania dotyczące zarządzania |
| Organizacyjne | Polityka przesyłania informacji, procedery i zabezpieczenia w celu ochrony wymiany informacji przesyłanych z użyciem wszystkich rodzajów środków łączności |
| Organizacyjne | Polityka bezpieczeństwa informacji - zatwierdzona przez prezesa, opublikowana i zakomunikowana pracownikom i właściwym stronom zewnętrznym |
| Organizacyjne | Przegląd polityk bezpieczeństwa informacji - przeglądy cykliczne oraz, gdy wystąpią istotne zmiany, w celu zapewnienia, że nadal są właściwe, adekwatne i skuteczne |
| Organizacyjne | Polityka stosowania urządzeń mobilnych |
| Organizacyjne | Warunki zatrudnienia - umowy z pracownikami i kontrahentami powinny określać odpowiedzialność stron w obszarze bezpieczeństwa informacji |
| Organizacyjne | Szkolenia wstępne dla pracowników nowozatrudnionych |
| Organizacyjne | Okresowe szkolenia dla pracowników już zatrudnionych |
| Organizacyjne | Procedury zarządzania nośnikami wymiennymi |
| Organizacyjne | Polityka kontroli dostępu - ustanowiona, udokumentowana i poddawana cyklicznym przeglądom |
| Organizacyjne | Dostęp do sieci i usług sieciowych, tylko do zasobów, do których otrzymali wyraźne upoważnienie |
| Organizacyjne | Ograniczenie dostępu do informacji zgodnie z polityką kontroli dostępu |
| Organizacyjne | Procedura bezpiecznego logowania |
| Organizacyjne | Regulamin Ochrony Danych Osobowych dla pracowników i współpracowników |
| Organizacyjne | Outsourcing |
| Organizacyjne | Polityka kluczy (kontrola kluczy zapasowych, kontrola wydawania kluczy, kontrola przechowywania kluczy) |
| Organizacyjne | Procedura audytów |
| Organizacyjne | Procedura korzystania z zasobów sieci (poczta elektroniczna, Internet, ...) |
| Organizacyjne | Procedura postepowania z nośnikami i sprzętem poza Izbą |
| Organizacyjne | Procedury nadawania i odbierania uprawnień |
| Organizacyjne | Procedury postępowania na wypadek wykrycia ataków DDoS/DoS |
| Organizacyjne | Procedury postępowania w przypadku wykrycia anomalii i sposoby dokumentowania takiego postępowania |
| Organizacyjne | Procedury przeglądania uprawnień w systemach |
| Organizacyjne | Procedury reagowania na wykrycie botnet w sieci Izby |
| Organizacyjne | Procedury reagowania na wykryte incydenty / Plan ciągłości działania |
| Organizacyjne | Procedury uaktualnienia oprogramowania (instalacja łat) |
| Organizacyjne | Rozpraszanie uprawnień (zasada "czterech par oczu") |
| Organizacyjne | Stosowanie zasady wiedzy koniecznej (need to know) |
| Organizacyjne | Umowy z dostawcami usługi dostępu do Internetu zawierające klauzule przenoszące działania przeciw atakowi na dostawcę |

# Instrukcja
# Zarządzania Systemem Informatycznym

## I. Postanowienia ogólne

1. Do pracy w systemie informatycznym służącym do przetwarzania danych osobowych może zostać dopuszczona tylko i wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych wydane przez Administratora.
2. Administratorowi Systemu Informatycznego w pracach związanych z zarządzaniem infrastrukturą informatyczną może pomagać inny użytkownik (użytkownik uprzywilejowany).
3. Użytkownik uprzywilejowany, o którym mowa w pkt 2 pomaga Administratorowi Systemu Informatycznego w obowiązkach dotyczących infrastruktury informatycznej i wynikających z niniejszego dokumentu.
4. Użytkownik uprzywilejowany posiada takie uprawnienia by mógł wykonywać zadania związane z procedurami zapisanymi w niniejszym dokumencie.

## II. Przetwarzanie danych osobowych

1. Praca na komputerach może odbywać się tylko w miejscach do tego wyznaczonych. Każdy pracownik posiada wydzielone miejsce pracy.
2. Za umożliwienie korzystania z komputera przez osobę nieupoważnioną odpowiada pracownik, któremu sprzęt ten został przydzielony.
3. Na każdym użytkowniku systemu informatycznego spoczywa odpowiedzialność za rodzaj i zakres danych przetwarzanych przez niego w ramach przydzielonych mu uprawnień systemowych i programowych, oraz odpowiedzialność za ochronę tych danych przed niepowołanym dostępem, niepowołaną modyfikacją, zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.

## III. Procedury zarządzania systemem informatycznym

### III.1. Nadawanie uprawnień

#### III.1.1. Rejestrowanie użytkownika

1. Za rejestrację użytkownika w systemie informatycznym odpowiedzialny jest Administrator Systemu Informatycznego.
2. Osoba zajmująca się sprawami kadrowymi zobowiązana jest do powiadomienia Administratora Systemu Informatycznego o nowo zatrudnionym pracowniku, stażyście, praktykancie.
3. Upoważnienie do przetwarzania danych osobowych przygotowywane jest przez osobę zajmującą się gospodarką odpadami komunalnymi.
4. Zakres dostępu do systemu informatycznego przygotowuje bezpośredni przełożony.

5. Administrator Systemu Informatycznego zakłada konto w systemie informatycznym zgodne z przekazanymi mu informacjami.
6. Administrator Systemu Informatycznego nadaje takie uprawnienia, które są niezbędne do codziennej pracy użytkownika.

### III.1.2. Wyrejestrowanie użytkownika

1. Osoba zajmująca się sprawami kadrowymi jest zobowiązana do niezwłocznego poinformowania Administratora Systemu Informatycznego o zakończeniu stosunku pracy, stażu, praktyki z użytkownikiem systemu informatycznego.
2. Administrator Systemu Informatycznego blokuje identyfikator użytkownika, któremu upłynął termin lub zostało odebrane upoważnienie do przetwarzania danych osobowych, zgodnie z przekazanymi mu informacjami przez pracownika zajmującego stanowisko do spraw kadrowych.
3. Administrator Systemu Informatycznego wyrejestrowuje użytkowników z systemu informatycznego na wniosek przełożonego.
4. Wyrejestrowanie może mieć charakter czasowy lub trwały.
5. Wyrejestrowanie następuje poprzez zablokowanie konta użytkownika do czasu ustania przyczyn uzasadniających blokadę (wyrejestrowanie czasowe).
6. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach, którego zatrudniony był użytkownik.

## III.2. Metody i środki uwierzytelnienia oraz procedury związane z ich użytkowaniem i zarządzaniem

### III.2.1. Hasła użytkowników

1. W Urzędzie stosuje się dwustopniowe uwierzytelnienie.
2. Pierwsze uwierzytelnienie następuje do stacji roboczej, drugie uwierzytelnienie do programu, na którym przetwarzane są dane osobowe.
3. Metodą uwierzytelniania jest identyfikator użytkownika (login) oraz hasło logowania.
4. Loginy nadawane są przez Administratora Systemu Informatycznego.
5. Login użytkownika powinien jednoznacznie identyfikować użytkownika.
6. Przy budowaniu loginu i hasła nie stosuje się polskich znaków diakrytycznych.
7. Hasło pierwszego logowania może być nadawane przez Administratora Systemu Informatycznego.
8. Użytkownik zobowiązany jest do zmiany hasła.
9. Hasło powinno zawierać minimum 8 znaków.

10. Hasło powinno zawierać małe i duże litery.
11. Hasło powinno zawierać cyfry lub znak specjalny.
12. Hasła powinny być zmieniane nie rzadziej niż co 30 dni.
13. Jeżeli system informatyczny nie wymusi zmiany hasła, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
14. Hasło powinno być znane tylko i wyłącznie użytkownikowi.
15. Nie wolno podawać hasła osobom trzecim.
16. Hasło nie może być widoczne na ekranie podczas jego wpisywania.
17. Zabrania się zapisywania hasła w łatwo dostępnym miejscu.
18. Jeżeli, nadawanie uprawnień, w którymś z systemów informatycznych odbiega od zasad zapisanych powyżej tworzona jest oddzielna instrukcja nadawania uprawnień do systemu.

### III.2.2. Hasło administracyjne

1. Administrator Systemu Informatycznego ustala hasła administracyjne.
2. Hasła administracyjne do systemu informatycznego powinna znać tylko osoba upoważniona.
3. Hasło administracyjne powinno być zapisane w bezpieczny sposób i zdeponowane w miejscu, do którego jest ograniczony dostęp.
4. Otwarcie hasła może zostać dokonane tylko i wyłącznie, gdy Administrator Systemu Informatycznego i osoba przez niego upoważniona nie jest dostępna.
5. Inspektor Ochrony Danych może przeprowadzać weryfikację zgodności haseł.
6. Badanie zgodności przeprowadza się nie rzadziej niż raz na rok.

## III.3. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Administrator Systemu Informatycznego zobowiązany jest do sprawdzenia poprawności uruchomienia systemu informatycznego oraz urządzeń wspomagających w razie zauważenia nieprawidłowości w uruchomieniu systemu powinien zablokować dostęp użytkowników do systemu i jak najszybciej usunąć usterkę.
2. Administrator Systemu Informatycznego w razie pojawienia się problemów z poprawnym działaniem systemu lub brakiem zasilania elektrycznego, zobowiązany jest do sprawdzenia przyczyn awarii.
3. Po awaryjnym przerwaniu pracy komputera, np. zanik napięcia w sieci energetycznej, należy sprawdzić czy zostały zapisane ostatnio wprowadzane dane do używanych w tym czasie programów.

### III.3.1. Rozpoczęcie pracy

1. Każdy użytkownik musi BEZWZGLĘDNIE stosować się do wyznaczonego czasu dostępu do systemu informatycznego i jego zasobów.

2. Przed rozpoczęciem pracy użytkownik zobowiązany jest do zweryfikowania stanowiska pracy w celu sprawdzenia, czy stanowisko pracy nie zostało naruszone, lub wykorzystane przez osobę niebędącą użytkownikiem tego systemu.
3. W razie podejrzenia prób włamania do systemu, pomieszczenia użytkownik zobowiązany jest niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego.
4. Rozpoczęcie pracy na stacji roboczej następuje po jej włączeniu.
5. Bezpośredni dostęp do systemu przetwarzania danych osobowych może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
6. W przypadku pojawienia się trudności w autoryzacji, pomimo prawidłowo wpisanej nazwy użytkownika i hasła, użytkownik zobowiązany jest skontaktować się z Administratorem Systemu Informatycznego.
7. Jeżeli proces autoryzacji przebiegł prawidłowo, użytkownik może przystąpić do pracy.

### III.3.2. Przerywanie pracy

1. Przerywając pracę użytkownik, który opuszcza swoje stanowisko i pomieszczenie pracy zobowiązany jest do zablokowania systemu.
2. Na stacjach roboczych zostały skonfigurowane wygaszacze ekranu w taki sposób by po określonym czasie bezczynności blokowana była stacja robocza.
3. Użytkownik udostępniający stanowisko pracy innej upoważnionej osobie musi wylogować się z systemu.

### III.3.3. Zakończenie pracy w systemie

1. Zakończenie pracy polega na wylogowaniu użytkownika i zakończeniu pracy systemu.
2. Wyłączenie komputera może nastąpić wyłącznie po uprzednim zamknięciu wszystkich aktywnych aplikacji (programów).
3. Kategorycznie zabrania się wyłączać komputery w czasie działania programu przyciskiem „POWER" lub „RESET" (bez wyraźnej przyczyny), gdyż takie działanie może spowodować trwałe uszkodzenie zbiorów danych oraz uszkodzić oprogramowanie komputera. Nie należy wyłączać przewodów zasilających i sieciowych z gniazda elektrycznych i gniazd sieci komputerowej.

## III.4. Procedura tworzenia kopii zapasowych

1. Za sporządzanie i bezpieczeństwo kopii danych elektronicznych, przetwarzanych w Urzędzie odpowiedzialny jest Administrator Systemu Informatycznego oraz wyznaczeni pracownicy zgodnie z zakresem obowiązków.
2. Kopie należy wykonywać poprzez przegrywanie całej bazy danych lub katalogów.
3. Kopie bezpieczeństwa powinny być wykonywane regularnie zgodnie z określonym planem tworzenia kopii zapasowych.

4. Plan, o którym mowa w pkt 3 tworzy Administrator Systemu Informatycznego.
5. Kopie bezpieczeństwa powinny być wykonywane automatycznie.
6. Kopie bezpieczeństwa wykonywane są na osobne nośniki danych.
7. Podstawowym modelem wykonywania kopii bezpieczeństwa są kopie dzienne.
8. Dzienne kopie bezpieczeństwa wykonywane są z programów mający istotne znaczenie dla działalności Urzędu.

### III.5. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe

1. Kopie bezpieczeństwa przechowywane są w zabezpieczonych miejscach, do których jest ograniczony dostęp.
2. Do zabezpieczenia danych w Urzędzie można zastosować program szyfrujący całościowo lub częściowo partycje.
3. Elektroniczne nośniki danych (pamięci flash, nośniki optyczne, itp.), na których znajdują się dane osobowe muszą być przechowywane w miejscach, do których dostęp jest ograniczony.
4. Po wykorzystaniu danych z elektronicznego nośnika informacji, nośnik ten należy zniszczyć lub trwale usunąć z niego dane.
5. Zabrania się wnoszenia i używania jakichkolwiek prywatnych lub innych „nie służbowych" nośników magnetycznych, optycznych oraz pamięci przenośnych bez zgody Inspektora Ochrony Danych.
6. Pracownik jest zobowiązany do odpowiedniego zabezpieczenia danych przechowywanych na powierzonym mu sprzęcie.

### III.6. Procedura przekazywania danych poza teren Urzędu

1. Dane przekazywane poza teren Urzędu za pomocą łączy internetowych muszą być odpowiednio zabezpieczone.
2. Przekazywane informacje muszą być zabezpieczone w taki sposób by ich nieuprawnione odczytanie było niemożliwe.
3. Dane muszą być zabezpieczone poprzez hasła dostępu.
4. Haseł dostępu, czy kluczy aktywacyjnych do danych nie można przekazywać tą samą droga, co danych.
5. Przekazywanie danych w formie elektronicznej na nośnikach zewnętrznych musi odbywać się przy zachowaniu szczególnych względów bezpieczeństwa.
6. Dane na nośnikach zewnętrznych muszą być zabezpieczone przed nieuprawnionym dostępem.
7. Dane na nośnikach muszą być zabezpieczone programem szyfrującym.
8. Sam przenoszony, przekazywany nośnik musi być zabezpieczony w taki sposób by jego nieuprawnione otwarcie było widoczne.
9. Niedopuszczalne jest przekazywanie jakichkolwiek danych osobowych drogą telefoniczną.

### III.7. Ochrona przed złośliwym oprogramowaniem

1. Na wszystkich komputerach będących w posiadaniu Urzędu powinien być zainstalowany program antywirusowy, który chroni je przed zagrożeniami wynikającymi z działania złośliwego kodu.
2. Za instalacje programu odpowiedzialny jest Administrator Systemu Informatycznego.
3. Program antywirusowy, który został zainstalowany na komputerach pracuje „w tle" i na bieżąco monitoruje próby zainfekowania przez złośliwy kod.
4. Program zainstalowany na komputerach Urzędu działa na zasadzie „klient - serwer".
5. Końcówki zarządzane są za pomocą konsoli administracyjnej, do której dostęp ma Administrator Systemu Informatycznego.
6. Końcówki zainstalowane na stacjach roboczych, aktualizacje i szczepionki pobierają przez konsolę administracyjną.
7. Przy każdym uruchomieniu komputera program skanuje zawartość dysków w celu wykrycia złośliwego kodu.
8. Na styku sieci publicznej z siecią wewnętrzną został zamontowany firewall klasy UTM, który odpowiednio zabezpiecza przed atakami z zewnątrz.

### III.8. Procedury korzystania z oprogramowania

1. Pracownicy mogą korzystać jedynie z oprogramowania, na które Urząd posiada aktualne licencje. Pracownik jest odpowiedzialny za stan oprogramowania zainstalowanego na komputerze.
2. W przypadku komputerów wolnostojących, do których nie jest przypisany na stałe konkretny użytkownik, wyznacza się osobę odpowiedzialną za ten komputer. Osobą odpowiedzialną może być w szczególności kierownik komórki organizacyjnej, która wykorzystuje taki komputer.
3. Wszyscy pracownicy przyjmują do wiadomości informację o konieczności pracy wyłącznie na oprogramowaniu wymienionym w „metryce komputera".
4. Każda zmiana stanu zainstalowanego na danym komputerze oprogramowania musi znaleźć potwierdzenie w metryce tego komputera.
5. Pracownicy Urzędu nie mogą za pomocą komputerów firmowych pobierać z Internetu lub przesyłać nielicencjonowanego oprogramowania oraz innych utworów, w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, chronionych prawem autorskim (w tym w szczególności utworów muzycznych, filmów, grafiki, gier komputerowych i tym podobnych).
6. Pracownicy nie mogą wnosić na teren Urzędu ani instalować na firmowych komputerach prywatnych kopii oprogramowania, plików muzycznych i video, z żadnego nośnika i z żadnego innego urządzenia.
7. Pracownicy Urzędu mogą korzystać z komputerów, Internetu oraz poczty elektronicznej wyłącznie w celu wykonywania obowiązków służbowych oraz dla samokształcenia, w tym szczególnie dla podnoszenia swoich kwalifikacji na zajmowanym stanowisku.

8. Instalacji oprogramowania w Urzędzie mogą dokonywać wyłącznie osoby do tego upoważnione.
9. Zakupu oprogramowania w Urzędzie mogą dokonywać wyłącznie osoby do tego upoważnione.
10. Osoby biorące udział w nielegalnym kopiowaniu oprogramowania mogą zostać zgodnie z prawem polskim pociągnięte do odpowiedzialności karnej i cywilnej, w tym do odpowiedzialności odszkodowawczej z tytułu odpowiedzialności cywilnej, oraz ukarane grzywną i/lub karą pozbawienia wolności w ramach odpowiedzialności karnej. Wobec takich osób zostaną również zastosowane sankcje przewidziane w Kodeksie Pracy.

### III.9. Procedury przechowywania dokumentacji licencyjnej

1. W Urzędzie przechowuje się kompletną dokumentację licencyjną - wszystkie atrybuty legalności oprogramowania, które towarzyszyły mu przy zakupie.
2. Oryginalna dokumentacja licencyjna oraz podpisane metryki komputera przechowywane są w zamkniętym pomieszczeniu, do którego dostęp mają wyłącznie osoby upoważnione.
3. Za certyfikaty autentyczności systemów operacyjnych naklejone na obudowie komputerów odpowiedzialny jest informatyk oraz osoby odpowiedzialne za dany komputer. O wszelkich przypadkach braku lub uszkodzenia certyfikatu należy niezwłocznie poinformować informatyka.
4. Za dokumentację licencyjną oraz za jej właściwe przechowywanie odpowiedzialny jest informatyk oraz osoby przez niego upoważnione.
5. Dokumentacja licencyjna traktowana jest jak majątek Urzędu.
6. Przyjęcie na stan dokumentacji licencyjnej przez informatyka potwierdzane jest wpisem do książki ewidencji majątku.
7. Dostęp do oryginalnej dokumentacji licencyjnej ma wyłącznie informatyk zarządzający oprogramowaniem oraz osoby przez niego upoważnione.
8. Nośniki z materiałami szkoleniowymi dla Urzędu, nośniki zakupione wraz z gazetami i czasopismami oraz nośniki zawierające oprogramowanie pochodzące z innych legalnych źródeł przechowywane są w pomieszczeniu razem z całą dokumentacją licencyjną i mogą być używane i użyczane osobom trzecim wyłącznie przez informatyka oraz osoby przez niego upoważnione.
9. Nośniki zawierające materiały przygotowane przez Urząd powinny być oznaczone, jako własność Urzędu.

### III.10. Procedury instalacji oprogramowania

1. Osobą odpowiedzialną za instalację oprogramowania w Urzędu jest Administrator Systemu Informatycznego.
2. Instalacji może dokonywać wyłącznie informatyk oraz osoby przez niego upoważnione.
3. Przed zainstalowaniem oprogramowania osoba odpowiedzialna za instalację musi zapoznać się z warunkami licencji i podjąć decyzję czy je akceptuje oraz czy Urząd spełnia wymogi tej licencji.

4. Instalacji należy dokonywać wyłącznie zgodnie z ilością posiadanych przez Urząd licencji.
5. Pobieranie i instalowanie oprogramowania z Internetu dopuszcza się wyłącznie w sytuacji, gdy licencja na to zezwala, a oprogramowanie jest niezbędne do wykonywania obowiązków służbowych przez pracownika. Mogą tego dokonywać wyłącznie osoby upoważnione.
6. W odniesieniu do aplikacji klient/serwer oraz aplikacji sieciowych, pracownicy Urzędu mogą używać oprogramowania wyłącznie na warunkach określonych w stosownej umowie licencyjnej na to oprogramowanie.
7. Oprogramowanie w wersjach testowych lub jakikolwiek inny sposób ograniczone umowami licencyjnymi może być użytkowane w Urzędzie wyłącznie zgodnie z jego przeznaczeniem, tylko przez czas i w zakresie określonym w licencji oraz jedynie przez osoby upoważnione.
8. Każdorazowa instalacja oprogramowania na komputerze musi mieć odzwierciedlenie w metryce konkretnego komputera oraz w rejestrze sprzętu i oprogramowania.
9. Osoba odpowiedzialna za nadzór nad rejestrem sprzętu i oprogramowania po każdej instalacji nowego oprogramowania zobowiązana jest do uaktualnienia rejestru, stworzenia aktualnej metryki i przedstawienia jej do podpisu przez pracownika użytkującego komputer lub będącego za niego odpowiedzialnym.
10. Nie wolno dokonywać kopii oryginalnych nośników, jeśli umowa licencyjna na to nie zezwala. Jeżeli umowa licencyjna na to pozwala kopii takich może dokonywać wyłącznie informatyk.

### III.11. Procedura korzystania z Internetu

1. Użytkownikom zabrania się dostępu do Internetu za pośrednictwem łączy, które nie są autoryzowane przez osoby upoważnione. Osobą upoważnioną jest w tym wypadku Administratora Systemu Informatycznego.
2. Zabrania się korzystania z Internetu w sposób mogący narazić Urząd na jakiekolwiek straty finansowe lub inne.
3. Pracownicy, którzy posiadają dostęp do łączy internetowych, zobowiązani są do ich wykorzystywania wyłącznie w celach służbowych z jednoczesnym zachowaniem dobrych obyczajów i poszanowania praw autorskich i ich dzieł udostępnianych przez sieć Internet.
4. Niedozwolone dla pracownika jest:
   1) udostępnianie osobom trzecim nazw kont i haseł,
   2) samodzielna zmiana konfiguracji stacji roboczych związanych ściśle z przyłączem internetowym,
   3) ściąganie i instalowanie oprogramowania z Internetu bez zgody Administratora Systemu Informatycznego nawet w przypadkach, gdy w/w oprogramowanie jest darmowe.
5. Nie przestrzeganie zasad określonych w pkt. 4 będzie traktowane jak naruszenie obowiązków pracowniczych. O zaistniałym fakcie Administrator Systemu Informatycznego powiadamia Administratora.

6. Uzyskiwanie dostępu, przeglądanie lub rozprowadzanie niewłaściwych materiałów (np. rozrywkowych, pornografii) poprzez sieć wewnętrzną Urzędu lub sieć Internet jest surowo zabronione.
7. Uzyskiwanie nieautoryzowanego dostępu do sieci Internet oraz do chronionych systemów lub plików jest zakazane. W przypadku stwierdzenia lub powiadomienia o nieupoważnionych działaniach, Administrator Systemu Informatycznego Administratora Danych, który wszczyna postępowanie wyjaśniające i podejmuje stosowne działania.
8. Korzystanie z czasu wyznaczonego na wykonywanie obowiązków służbowych i zasobów Urzędu w celu osiągnięcia osobistych korzyści jest zakazane.
9. Niedopuszczalne jest ujawnianie za pośrednictwem Internetu informacji prawnie chronionych.

### III.12. Procedura dotycząca pracy na komputerach przenośnych

1. O ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji.
2. Użytkownik, któremu został powierzony komputer przenośny, powinien chronić go przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas transportu takiego urządzenia.
3. Obowiązuje zakaz używania komputera przenośnego przez osoby inne niż użytkownicy, któremu został on powierzony.
4. Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora.
5. Użytkownicy zobowiązani są zmieniać hasło na komputerze przenośnym nie rzadziej, niż co 30 dni.
6. Pliki zawierające dane osobowe i przechowywane na komputerach przenośnych muszą być zaszyfrowane i zabezpieczone hasłem.
7. Szyfrowane mogą być same pliki lub pliki mogą się znajdować na zaszyfrowanej partycji dysku.
8. Obowiązuje zakaz przechowywania na komputerze przenośnym, które są wynoszone z Urzędu, całych zbiorów danych nawet w postaci zaszyfrowanej.
9. Użytkownicy przetwarzający dane osobowe na komputerach przenośnych zobowiązani są do systematycznego wprowadzania tych danych do określonego miejsca na serwerze administratora danych, a następnie do trwałego usunięcia ich z pamięci powierzonego im komputera przenośnego.

### III.13. Procedura przeglądu i konserwacji systemów informatycznych oraz nośników informacji

1. Osobą odpowiedzialną za prawidłowe działanie systemu informatycznego jest Administrator Systemu Informatycznego.
2. Administrator Systemu Informatycznego dokonuje napraw i konserwacji systemu informatycznego.
3. Gdy naprawa systemu musi się odbyć w serwisie zewnętrznym lub przez osobę niebędącą upoważnioną do przetwarzania danych osobowych, Administrator Systemu Informatycznego zobowiązany jest do odpowiedniego zabezpieczenia danych znajdujących się na dyskach urządzenia.

4. Jeżeli nie jest możliwe odpowiednie zabezpieczenie danych zawartych na dyskach, wszelkie naprawy wykonuje się w obecności osoby upoważnionej.
5. Przekazania i odbioru sprzętu komputerowego do i z serwisu może dokonywać wyłącznie Administrator Systemu Informatycznego oraz osoby przez niego upoważnione.
6. W przypadku przekazywania wraz z komputerem dokumentacji licencyjnej należy sporządzić protokół oddania do serwisu komputera wraz z dokumentacją. W protokole musi zostać wyszczególniona cała dokumentacja licencyjna przekazywana razem z komputerem. Protokół podpisuje osoba przekazująca i osoba przyjmująca komputer wraz dokumentacją do serwisu. Na podstawie protokołu serwis bierze całkowitą odpowiedzialność za tę dokumentację.
7. Serwis odpowiada w całości za ewentualną instalację oprogramowania dokonaną w ramach prac serwisowych.
8. Po odebraniu komputera z serwisu należy sprawdzić stan dokumentacji licencyjnej i zainstalowanego na nim oprogramowania ze stanem z momentu przed oddaniem do serwisu. Osobą odpowiedzialną za to jest informatyk lub osoby przez niego upoważnione. W przypadku stwierdzenia rozbieżności należy przywrócić stan z momentu przed oddaniem do serwisu.
9. Każde przeprowadzenie napraw serwisowych musi być dokumentowane.
10. Wszystkie dokumenty związane z naprawami serwisowymi lub gwarancyjnymi są dołączane do teczki komputera.
11. Konserwacje sprzętu komputerowego wykonywane są na bieżąco. Każda zgłoszona usterka usuwana jest niezwłocznie przez informatyka lub zlecona zostaje naprawa do serwisu zewnętrznego.
12. Informatyk sprawdza nośniki informacji pod względem ich przydatności do pracy.

### III.14. Kontrola przestrzegania zasad

1. Sekretarz Gminy lub osoba przez niego wyznaczona sprawuje nadzór nad przestrzeganiem Polityki Bezpieczeństwa przetwarzania danych osobowych w Urzędzie.
2. Sekretarz Gminy lub osoby przez niego wyznaczone mogą dokonywać okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad i procedur bezpieczeństwa zawartych w niniejszym dokumencie.
3. Okresowe kontrole przestrzegania zasad powinny odbywać się przynajmniej raz na rok.
4. W przypadku wykrycia niesprawności jednostki komputerowej lub jednej z jej części należy przekazać urządzenie do naprawy przez informatyka. Gdy naprawa wymaga działania osoby trzeciej dane przechowywane na dyskach twardych należy w odpowiedni sposób zabezpieczyć poprzez usunięcie danych lub zaszyfrowanie.
5. Kontroli wykorzystania systemu informatycznego dokonuje Administrator Systemu Informatycznego.
6. Przynajmniej raz w roku informatyk wykonuje weryfikację zainstalowanego oprogramowania.

### III.15. Odpowiedzialność użytkownika

1. Zasady i procedury zawarte w niniejszej Instrukcji obowiązują tak samo każdego pracownika w Urzędzie.
2. Instalacje oprogramowania na stanowiskach pracowniczych mogą dokonywane być z nośników znajdujących się w zasobach Urzędu. Ich instalacja może być dokonywana przez Administratora Systemu Informatycznego lub osobę przez niego upoważnioną tylko i wyłącznie po wydaniu zgody na autoryzowaną instalację.
3. Każdy jest indywidualnie odpowiedzialny za powierzony mu sprzęt.
4. Użytkownicy nie mogą sami dokonywać jakiejkolwiek zmiany komponentów sprzętu komputerowego, ani przyłączać własnych komponentów.
5. Wszelkie zapotrzebowanie na dodatkowe komponenty takie jak: RAM, dysk twardy, karta sieciowa, napęd optyczny i inne muszą być zgłaszane do informatyka, który osobiście lub przez wyznaczoną osobę dokonuje zmian.
6. Sprzęt komputerowy nie może być wynoszony z Urzędu lub przenoszony w inne miejsce w Urzędzie bez wcześniejszej zgody informatyka.
7. Utrata lub kradzież sprzętu powinna być niezwłocznie zgłaszana bezpośredniemu przełożonemu, który zawiadamia Administratora Danych.
8. Na terenie Urzędu zabrania się kopiowania informacji z nośników magnetycznych i optycznych, a także w formie papierowej zawierającej dane osobowe bez zgody bezpośredniego przełożonego.
9. Każdy pracownik jest indywidualnie odpowiedzialny za przechowywanie przez siebie informacje w formie tradycyjnej (papierowej) jak i w formie elektronicznej.
10. Za umożliwienie korzystania z komputera przez osobę nieupoważnioną odpowiada pracownik, któremu sprzęt ten został przydzielony.
11. Na każdym użytkowniku systemu informatycznego spoczywa odpowiedzialność za rodzaj i zakres danych przetwarzanych przez niego w ramach przydzielonych mu uprawnień systemowych i programowych, oraz odpowiedzialność za ochronę tych danych przed niepowołanym dostępem, niepowołaną modyfikacją, zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.
12. Pracownik odpowiada za zachowanie w czystości stacji roboczych oraz urządzeń peryferyjnych (drukarki, głośniki itp.) znajdujące się na wyposażeniu stanowiska pracy.
13. Pracownikom nie wolno spożywać posiłków oraz napojów w pobliżu sprzętu komputerowego.
14. W bezpośrednim sąsiedztwie sprzętu komputerowego nie wolno zawieszać ani stawiać roślin ozdobnych a podlewanie roślin ozdobnych powinno odbywać się z zachowaniem maksymalnej ostrożności i dbałości o sprzęt komputerowy.
15. Do wydzielonej sieci energetycznej zasilającej system komputerowy nie wolno podłączać żadnych innych urządzeń (czajników elektrycznych, grzejników elektrycznych, itp.).

16. Dopuszczalne jest przywracanie gotowości do pracy drukarek (np. po „zacięciu" papieru) przez użytkownika po uprzednim przeszkoleniu przez informatyka i za jego zgodą.
17. W sprawach dotyczących systemu informatycznego należy niezwłocznie egzekwować polecenia ASI.
18. W razie jakichkolwiek niejasności należy kierować się zasadą „wszystko, co nie jest dozwolone, jest zabronione" lub kontaktować się z ASI.

Załącznik nr 1
do Instrukcji Zarządzania Systemem Informatycznym

| *Lp.* | *Nazwa zasobu* | *Rodzaj i typ kopii* | *Osoba odpowiedzialna za wykonanie kopii* | *Nośnik przechowywania kopii* | *Miejsce przechowywania kopii* | *Oznaczenie kopii* | *Czas przechowywania kopii* | *Niszczenie* |
|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | |
| 2 | | | | | | | | |
| | | | | | | | | |

Załącznik nr 2
do Instrukcji Zarządzania Systemem Informatycznym

## POROZUMIENIE

Niniejsze porozumienie (zwane dalej „Porozumieniem") zostało zawarte w dniu ..... r. w Poznaniu pomiędzy: OT PORT ŚWINOUJŚCIE S.A., reprezentowanym przez Prezesa, (zwanego dalej „Pracodawca") a, Panią/Panem.....zwaną/ym dalej „Pracownikiem".

1. Pracownik zatrudniony jest przez Pracodawcę na podstawie umowy o pracę.
2. Pracodawca wyposażył stanowisko pracy Pracownika w oprogramowanie komputerowe wykazane w metryce komputera stanowiące załącznik do niniejszego porozumienia.
3. Pracownik korzysta z oprogramowania w związku z wykonywaniem obowiązków pracowniczych.
4. Pracodawca i Pracownik uzgadniają, że do podstawowych obowiązków Pracownika należy korzystanie z oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodne z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków pracowniczych jak również niekorzystanie z jakiegokolwiek oprogramowania komputerowego, do używania którego Pracodawca nie jest uprawniony, w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Pracodawcy.
5. Podpisując oświadczenie pracownik jest zobowiązany do przestrzegania zakazu używania pamięci przenośnych (CD, DVD, SD, Pamięci USB...itp.) bez wcześniejszego porozumienia z administratorem sieci.
6. Pracownik oświadcza, iż jest świadomy odpowiedzialności karnej o której mowa w artykułach: 278 § 2, 293 w związku z 291 oraz art. 292 ustawy z dnia 6 czerwca 1997 r. kodeks karny oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach: 116 i następnych ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie oprogramowania.
7. Pracodawca i Pracownik uzgadniają, że naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, może stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą wypowiedzenie przez Pracodawcę umowy o pracę łączącej Pracodawcę z Pracownikiem lub rozwiązanie przez Pracodawcę tejże umowy o pracę bez wypowiedzenia z winy pracownika, zgodnie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy.
8. Niniejsze porozumienie zostało sporządzone w dwóch egzemplarzach, po jednym dla każdej ze stron.
9. Zmiana, uzupełnienie oraz rozwiązanie niniejszego Porozumienia za zgodą obu stron wymaga formy pisemnej pod rygorem nieważności.
10. Niniejsze porozumienie traci moc z dniem rozwiązania stosunku pracy.

.....
podpis Pracownika

.....
podpis Pracodawcy

Załącznik nr 3
do Instrukcji Zarządzania Systemem Informatycznym

# WNIOSEK O ZAREJESTROWANIE UŻYTKOWNIKA

| ☐ Nowy użytkownik | ☐ Modyfikacja uprawnień | ☐ | Odebranie uprawnień w systemie |
|---|---|---|---|
| **Imię i nazwisko użytkownika:** | | | |
| | | | |
| Posiada upoważnienie do przetwarzania danych osobowych: | ☐ TAK | ☐ NIE | |

Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie:

1. ***Nadanie loginu i hasła do systemu teleinformatycznego***

   ☐ Do systemu Windows
   Proszę o zaznaczenie

2. ***Nadanie loginu i uprawnień do następujących aplikacji:***
   Proszę o zaznaczenie
   ☐ Aplikacja 1
   Rodzaj uprawnień .....
   ☐ Aplikacja 2
   Rodzaj uprawnień .....
   ☐ Aplikacja 3
   Rodzaj uprawnień .....
   ☐ Aplikacja 4
   Rodzaj uprawnień .....
   ☐ Aplikacja 5
   Rodzaj uprawnień .....

3. ***Innych aplikacji*** :

| Podpis bezpośredniego przełożonego | |
|---|---|
| Podpis ASI | Podpis AD |

Załącznik nr 11

## Procedura postępowania z prawami osób

### 1. Cel procedury

Procedura przygotowana została w celu ujednolicenia i usystematyzowania realizacji prawa osób

### 2. Realizacja praw osób

2.1. Żadna z osób, których dane dotyczą nie może być w jakikolwiek sposób ograniczana w możliwości skorzystania ze swoich praw i w celu ich realizacji może zgłosić stosowny wniosek do administratora.

2.2. Osoba musi złożyć pisemny wniosek (lub przesłać informację mailem) o dostęp do informacji. Każdy wniosek (żądanie, zapytanie, skarga, itp.), o którym mowa w pkt. 1 może być złożony w każdej formie, a sprawa z nim związana jest dokumentowana i załatwiana zgodnie z obowiązującym w Urzędzie systemem kancelaryjno-archiwizacyjnym, chyba że administrator wykaże, że nie jest w stanie zidentyfikować osoby, której dane dotyczą.

2.3. Po wpłynięciu wniosku należy go zweryfikować pod kątem właściwości merytorycznej - uprawnienia danej osoby do jego złożenia. W przypadku złożenia wniosku przez przedstawiciela osoby, której dane dotyczą należy najpierw zweryfikować prawidłowość reprezentacji.

2.4. Wnioski rozpatruje się wyłącznie, gdy zostały złożone przez uprawnioną osobę, tj. osobę, której dane dotyczą lub osobę właściwie umocowaną.

2.5. Nie udziela się odpowiedzi na zapytania ustne, w tym kierowane telefonicznie, o ile administrator nie ma możliwości potwierdzenia tożsamości rozmówcy.

2.6. Wnioski rozpatruje się biorąc pod uwagę ich treść, a nie tytuł.

2.7. Każdy wpływający wniosek należy niezwłocznie skonsultować z Inspektorem Ochrony Danych.

2.8. Każdy projekt odpowiedzi na wniosek wymaga przed jego wysłaniem konsultacji z Inspektorem Ochrony Danych.

2.9. Odpowiedzi na wnioski udziela się bez zbędnej zwłoki, najpóźniej w terminie miesiąca od daty otrzymania wniosku. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.

2.10. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

2.11. Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

2.12. Działania podejmowane w zakresie obsługi wniosków są wolne od opłat.

2.13. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może odmówić podjęcia działań w związku z żądaniem.

2.14. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

2.15. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

**3. Prawo dostępu:**

3.1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące. Jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich.

3.2. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

3.3. Administrator nie przekazuje informacji, o której mowa w pkt. 6.1. w przypadku wykonywania przez niego zadania publicznego, a szczegóły z tym związane reguluje art. 5 UODO.

3.4. Jeżeli przetwarzanie danych nie ma miejsca, administrator informuje osobę występującą z wnioskiem o nie występowaniu przetwarzania danych jej dotyczących. W tym celu administrator weryfikuje wszystkie miejsca, w którym może następować przetwarzanie danych (dokumenty papierowe, systemy IT, poczta elektroniczna, itp.).

**4. Prawo do sprostowania**

4.1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania (poprawienia) dotyczących jej danych osobowych, które są nieprawidłowe.

4.2. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia (np. dla celów uprzedniej weryfikacji prawidłowości i aktualności podawanych danych).

**5. Prawo do usunięcia danych**

5.1. Osoba, której dane dotyczą, ma prawo żądania od administratora danych niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z okoliczności, o których mowa w ust. 1 art. 17 RODO:

5.1.1. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

5.1.2. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO, i nie ma innej podstawy prawnej przetwarzania;

5.1.3. osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;

5.1.4. dane osobowe były przetwarzane niezgodnie z prawem;

5.1.5. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

5.1.6. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego – dane osobowe dziecka (art. 8 ust. 1 RODO).

5.2. Jeżeli upubliczniono dane osobowe, co do których istnieje obowiązek usunięcia, to biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje się rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe w wyniku udostępnienia, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

5.3. Prawo usunięcia danych nie ma zastosowania w przypadkach, gdy przetwarzanie jest niezbędne:

5.3.1. do korzystania z prawa do wolności wypowiedzi i informacji;

5.3.2. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

5.3.3. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3;

5.3.4. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo do usunięcia danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;

5.3.5. do ustalenia, dochodzenia lub obrony roszczeń.

## 6. Prawo do ograniczenia przetwarzania danych

6.1. Osoba, której dane dotyczą, ma prawo zażądać ograniczenia przetwarzania jej danych osobowych w następujących przypadkach:

6.1.1. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

6.1.2. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;

6.1.3. osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania na mocy art. 21 ust. 2 ;

6.1.4. dane osobowe były przetwarzane niezgodnie z prawem;

6.1.5. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

6.1.6. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego – zgoda dziecka.

6.2. Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

6.3. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.

## 7. Prawo do przenoszenia danych

7.1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące oraz ma prawo przesłać te dane osobowe innemu administratorowi bez żądnych przeszkód ze strony administratora, jeżeli:

7.1.1. przetwarzanie odbywa się na podstawie zgody i jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (art. 6 ust. 1 lit. a) RODO) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz

7.1.2. przetwarzanie odbywa się w sposób zautomatyzowany.

7.2. Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

7.3. Wykonanie prawa do przenoszenia danych pozostaje bez uszczerbku dla prawa do usunięcia danych. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

7.4. Prawo, o którym mowa w pkt. 7.1. nie może niekorzystnie wpływać na prawa i wolności innych.

## 8. Prawo do sprzeciwu

8.1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych w przypadkach, o których mowa w art. 21 RODO.

## 9. Obowiązek powiadomienia o sprostowaniu lub usunięciu danych

9.1. Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

**10. Obowiązek powiadomienia o sprostowaniu lub usunięciu danych**

10.1. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

10.2. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie. (ust.3 art. 7 RODO).

10.3. W takim przypadku administrator nie ma dłużej prawa przetwarzać danych osobowych w celu objętym oświadczeniem zgody.

10.4. W wyniku odwołania zgody dane przetwarzane w celach objętych zgodą powinny zostać bezpowrotnie usunięte.

Załącznik nr 11 A

**Wzór**
**ewidencji realizacji praw przez osoby, których danych dotyczą**

| *Lp.* | *Dane osoby* | *Rodzaj prawa* | *Dane żądania* | *Podjęte działania* | *Uwagi* |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| 6 | | | | | |

## 1. Cel

1.1. Niniejszy dokument opisuje sposób realizacji procesu zarządzania ryzykiem w bezpieczeństwie informacyjnym, w skład którego wchodzą: analiza ryzyka, określenie i wdrożenie sposobu postępowania z ryzykiem, monitorowanie i przegląd ryzyka.

1.2. Organizacja wprowadza politykę zarządzania ryzykiem, której zadaniem jest monitorowanie zagrożeń dla działalności systemu ochrony danych osobowych w organizacji.

1.3. Obowiązującym standardem w działalności jest przygotowanie się do następstw wystąpienia zagrożenia lub zagrożeń, określenie prawdopodobieństwa jego wystąpienia oraz zaplanowania działań na rzecz minimalizacji możliwości jego wystąpienia.

1.4. Procedurą analizy ryzyka objęte są wszystkie elementy działalności organizacji.

## 2. Przebieg procesu

2.1. W trakcie analizy ryzyka należy wyodrębnić następujące elementy:

2.1.1. aktywa – są to wszystkie środki i narzędzia mające istotne znaczenie dla organizacji,

2.1.2. zagrożenia – są to przykłady potencjalnych naruszeń systemu,

2.1.3. skutki – są to niepożądane następstwa zrealizowania się zagrożeń w praktyce,

2.1.4. ryzyko – jest to prawdopodobieństwo, że zagrożenia się zrealizują i przyniosą konkretny, negatywny skutek dla aktywów.

2.2. Proces zarządzania ryzykiem w bezpieczeństwie informacji składa się z:

2.2.1. ustanowienia kontekstu,

2.2.2. szacowania ryzyka,

2.2.2.1. analiza ryzyka

2.2.2.2. ocena ryzyka

2.2.3. postępowania z ryzykiem,

2.2.4. akceptowania ryzyka,

2.2.5. informowania o ryzyku oraz monitorowania i przeglądu ryzyka.

## 3. Szacowanie ryzyka

3.1. Analiza ryzyka ma na celu oszacowanie poziomu ryzyka związanego z przetwarzaniem informacji. Ryzyko rozumiane jest jako wartość zależna od wysokości potencjalnych strat wynikających z niewłaściwego przetwarzania informacji i od prawdopodobieństwa wystąpienia takich strat.

3.2. Analiza ryzyka obejmuje kolejne etapy:

3.2.1. kreślenie aktywów wraz z ich ważnością;

Skala ważności aktywów opisana jest według poniższej tabeli:

| Ważność aktywu | Skala |
|---|---|
| Mało istotne | 1 |
| Średnio istotne | 2 |
| Znaczące | 3 |
| Bardzo ważne | 4 |

3.2.2. identyfikacja zagrożeń;

Listę potencjalnych zagrożeń określa poniższa tabela.

| Lp. | Zagrożenie |
|---|---|
| 1 | Atak fizyczny – kradzież, utrata sprzętu poza Organizacją |
| 2 | Atak fizyczny – nieuprawniony dostęp do pomieszczeń Organizacji |
| 3 | Atak fizyczny – nieuprawniony dostęp do SI |
| 4 | Atak fizyczny – włamania poprzez interfejsy lokalne |
| 5 | Atak fizyczny – włamanie do pomieszczeń Organizacji |
| 6 | Ataki na dane – podsłuch/przechwytywanie danych |
| 7 | Ataki na oprogramowanie – namierzanie wersji testowych |
| 8 | Ataki na oprogramowanie – skanowanie sieci i usług |
| 9 | Ataki na oprogramowanie – włamania z wykorzystaniem API (interfejsów programistycznych) |
| 10 | Ataki na oprogramowanie – włamania z wykorzystaniem luk typu zero day |
| 11 | Ataki na oprogramowanie – włamania z wykorzystaniem najczęstszych błędów programistycznych |
| 12 | Ataki na oprogramowanie – włamanie z wykorzystaniem znanych dziur w nieaktualizowanym Oprogramowaniu |
| 13 | Ataki na sprzęt – man in the middle attack (podsłuch) |
| 14 | Ataki na sprzęt – włamania do urządzeń nieaktualizowanych |
| 15 | Ataki na system – atak DOS/DDOS |
| 16 | Ataki na system – eskalacja uprawnień |
| 17 | Ataki na zabezpieczenia – dostęp do sieci z użyciem hackerskiego urządzenia |
| 18 | Ataki na zabezpieczenia – łamanie haseł |
| 19 | Ataki na zabezpieczenia – włamanie do sieci poprzez WIFI |
| 20 | Ataki na zabezpieczenia – włamanie z sieci zewnętrznej do sieci wewnętrznej |
| 21 | Błąd człowieka – awaria oprogramowania |
| 22 | Błąd człowieka – błędy projektowe/konfiguracyjne |
| 23 | Błąd człowieka – łatwo dostępne, łatwe lub standardowe hasła |

| | |
|---|---|
| 24 | Błąd człowieka – nieprzestrzeganie procedur |
| 25 | Błąd człowieka – nieuprawniona modyfikacja / usunięcie |
| 26 | Błąd człowieka – nieuprawnione kopiowanie danych |
| 27 | Błąd człowieka – pomyłki i błędy administratorów, użytkowników |
| 28 | Błąd człowieka – udostępnianie danych osobom nieupoważniony |
| 29 | Błąd człowieka – włamania do urządzeń nieodpowiednio skonfigurowanych |
| 30 | Błąd człowieka – włamania za pośrednictwem zbędnych usług |
| 31 | Natura – pożar |
| 32 | Natura – wichury i tornada |
| 33 | Natura – zalanie |
| 34 | Natura – zaleganie śniegu na dachach |
| 35 | Organizacyjne – brak aktualnej dokumentacji (instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania) |
| 36 | Organizacyjne – brak dokumentacji odo |
| 37 | Organizacyjne – brak kopii bezpieczeństwa |
| 38 | Organizacyjne – brak oświadczeń o zachowaniu poufności |
| 39 | Organizacyjne – brak procedur napraw w serwisach zewnętrznych |
| 40 | Organizacyjne – brak procedur niszczenia nośników z danymi |
| 41 | Organizacyjne – brak procedury na wypadek upadku firmy outsourcingowej lub dostawczej |
| 42 | Organizacyjne – brak sprzętu, przestarzały |
| 43 | Organizacyjne – brak struktury organizacyjnej |
| 44 | Organizacyjne – brak umowy gwarancyjnej lub wsparcia serwisowego |
| 45 | Organizacyjne – brak umowy o współpracy |
| 46 | Organizacyjne – brak umów powierzenia |
| 47 | Organizacyjne – braki kadrowe |
| 48 | Organizacyjne – nakładanie się kompetencji |
| 49 | Organizacyjne – nielegalne oprogramowanie |
| 50 | Organizacyjne – niewłaściwa organizacja stanowisk |
| 51 | Organizacyjne – utrata kluczowego pracownika |
| 52 | Techniczne – przegrzanie serwerowni |
| 53 | Techniczne – awaria elementów IT |
| 54 | Techniczne – awaria łączy telekomunikacyjnych |
| 55 | Techniczne – awaria zasilania |
| 56 | Techniczne – niewłaściwa wilgotność pomieszczeń składnicy akt |
| 57 | Techniczne – zły stan instalacji elektrycznej |

| | |
|---|---|
| 58 | Techniczne – zły stan instalacji odgromowej |
| 59 | Techniczne – zły stan przewodów wentylacyjnych |
| 60 | Wymuszenia – atak ransomeware |
| 61 | Wymuszenia – instalacja szkodliwego oprogramowania |
| 62 | Wymuszenia – nakłanianie do określonego zachowania przez telefon |
| 63 | Wymuszenia – nakłanianie do określonego zachowania w mailu |
| 64 | Wymuszenia – phishing (podrabianie stron) |
| 65 | Wymuszenia – przekazywanie, jako upominków nośniki danych |

3.2.3. określenie prawdopodobieństwa wystąpienia zagrożenia;

Skala prawdopodobieństwa opisana została w tabeli poniżej.

| Wartość | Prawdopodobieństwo |
|---|---|
| 0 | Brak podatności, zdarzenie nie zaistnieje |
| 1 | Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem nie zdarzy się w ciągu roku lub wystąpi nie częściej niż raz na pięć lat |
| 2 | Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się raz w ciągu roku |
| 3 | Istnieje uzasadnione prawdopodobieństwo, by sadzić, że zdarzenie objęte ryzykiem może kilkakrotnie zdarzyć się w ciągu roku lub wystąpi przynajmniej raz na kwartał |
| 4 | Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się wielokrotnie w ciągu roku lub wystąpi przynajmniej raz w miesiącu |

3.2.4. określenie skutków wystąpienia zagrożenia;

Skala skutków opisana została w tabeli poniżej.

| Wartość | Skutki |
|---|---|
| 0 | Brak podatności, nie będzie skutków, gdyż zdarzenie nie wystąpi. |
| 1 | Szum medialny, np. z powodu ujawnienia danych niepodlegających ochronie prawnej.<br>Zdarzenie objęte ryzykiem powoduje minimalną stratę finansową lub krótkotrwałe zakłócenia lub opóźnienie w wykonywaniu zadań. Nie wpływa na reputację. Skutki zdarzenia można łatwo usunąć. |
| 2 | Nałożenie kar ustawowych w dolnej granicy kary. Koszt nielicznych procesów sądowych (obsługa prawna, informacyjna, odszkodowania); |

| | |
|---|---|
| | Zdarzenie objęte ryzykiem powoduje niewielką stratę finansową, niewielkie zakłócenie lub opóźnienie w wykonywaniu zadań. Wpływa na reputacje jednostki. Skutki zdarzenia można łatwo usunąć. |
| 3 | Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych, jednak nie są one wysokie. Wysokie ustawowe kary pieniężne. Koszt kilkudziesięciu procesów sądowych (obsługa prawna, informacyjna, odszkodowania). Kontrole i kary UODO. Zdarzenie objęte ryzykiem powoduje znaczącą stratę posiadanych zasobów, ma negatywny wpływ na efektywność działania, jakość wykonywanych zadań, reputację jednostki Z wystąpieniem zdarzenia objętego ryzykiem może się wiązać trudny proces przywracania stanu poprzedniego. |
| 4 | Skutki mogą prowadzi do wysokiego uszczerbku fizycznego, szkód majątkowych dla osób fizycznych. Zagrożenie ustawową karą pozbawienia wolności. Koszty kilkuset procesów sądowych (obsługa prawna, informacyjna, odszkodowania). Kontrole organów ścigania. Zdarzenie objęte ryzykiem powoduje brak realizacji kluczowych zadań albo osiąganie założonych celów – poważny uszczerbek w zakresie jakości wykonywanych zadań, poważna strata finansowa albo reputacji. Z wystąpieniem zdarzenia objętego ryzykiem wiąże się długotrwały i trudny proces przywracania stanu poprzedniego. |

3.2.5. określenie zabezpieczeń;

3.2.5.1. Należy określić zabezpieczenia stosowane w celu zminimalizowaniu zagrożenia.

3.2.6. oszacowanie ryzyka;

3.2.6.1. Administrator, po dokonaniu wyliczenia Ryzyka (R) ma obowiązek odniesienia jego poziomu do skali i podejmuje dalsze działania związane z ryzykiem.

Skalę Ryzyka w podmiocie leczniczym określa tabela poniżej.

| Lp. | Wartość | Działania |
|---|---|---|
| 1. | 0 | brak ryzyka |
| 2. | 1 - 3 | istotność ryzyka na poziomie akceptowalnym, należy je monitorować |
| 3. | 4 - 8 | ryzyko umiarkowane, nieakceptowalne, wymagające uwagi i wprowadzenia dodatkowych mechanizmów kontrolnych oraz dalszego monitorowania |

| | | |
|---|---|---|
| 4. | 9 - 16 | ryzyko nieakceptowalne, obszary szczególnie narażone na wystąpienie ryzyka, wymagają pilnej reakcji ze strony Organizacji, należy podjąć natychmiastowe działania zmniejszające ryzyko. |

## *4. Postępowanie z ryzykiem*

4.1. Jeśli ryzyko jest na poziomie akceptowalnym, Administrator potwierdza jedynie, że zastosowane zabezpieczenia są właściwe.

4.2. W przypadku ryzyka na poziomie umiarkowany Administrator musi ocenić czy jest możliwość obniżenia jego poziomu poprzez zastosowanie stosownych zabezpieczeń lub czy może je zaakceptować. W przypadku akceptacji ryzyka Administrator ma obowiązek jego monitorowania.

4.3. Po zaakceptowaniu akceptowalnego poziomu ryzyka, na podstawie przeprowadzonej analizy i oceny ryzyka należy określić i wdrożyć zasady postępowania z ryzykiem. Istnieją cztery warianty postępowania z ryzykiem:

4.3.1. Zachowanie ryzyka - polega na podjęciu decyzji o zachowaniu ryzyka bez podejmowania dalszych działań, na podstawie oceny ryzyka.

4.3.2. Redukowanie ryzyka - Polega na zredukowaniu poziomu ryzyka przez taki wybór zabezpieczeń, aby ryzyko szczątkowe można było ponownie oszacować jak ryzyko akceptowalne, np. poprzez zastosowanie dodatkowych zabezpieczeń

4.3.3. Unikanie ryzyka - polega na unikaniu działań lub warunków, które powodują powstanie określonych ryzyk, poprzez modyfikację procedur, które mają na celu wyeliminowanie potencjalnie niebezpiecznych sytuacji,

4.3.4. Transfer ryzyka - na podstawie oceny ryzyka zaleca się transfer ryzyka do innej strony, która może skutecznie zarządzać ryzykiem, np. zakup ubezpieczenia, powierzenie procesów przetwarzania podmiotom zewnętrznym.

4.4. Wszystkie ryzyka o wartości poniżej akceptowanego zostaną zachowane.

4.5. Po wybraniu wariantu postępowania z ryzykiem należy utworzyć Plan postępowania z ryzykiem.

4.6. Plan postępowania z ryzykiem powinien zawierać:

4.6.1. wybrane warianty postępowania z ryzykiem,

4.6.2. dobór zabezpieczeń,

4.6.3. podział odpowiedzialności,

4.6.4. planowane koszty,

4.6.5. harmonogramy.

4.7. Po akceptacji przez kierownictwo, Plan postępowania z ryzykiem zostaje wdrożony.