Zarządzenie Nr 021 29.2018

Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie
z dnia 25 maja 2018r.

w sprawie wprowadzenie Polityki Bezpieczeństwa Danych Osobowych w Gminnym Ośrodku Pomocy Społecznej w Gminie Malechowo

Na podstawie art. 33 ust 3 i 5 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U z 2017r. poz. 2232, Dz. U z 2018r. poz. 130) w związku z art. 24 ust. 2, Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenie dyrektywy 95/46/WE oraz § 20 ust 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U z 2017r., poz. 2247 t.j) zarządzam co następuje:

§ 1 Wprowadzam do użytku wewnętrznego w Gminnym Ośrodku Pomocy Społecznej w Malechowie Politykę bezpieczeństwa danych osobowych, stanowiącą załącznik do niniejszego zarządzenia.

§ 2 Traci moc:

- Zarządzenie na 1/2005 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 16 lutego 2005 w sprawie ustalenia „ Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych w Gminnym Ośrodku Pomocy Społecznej w Malechowie”
- Zarządzenie nr 2/2005 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 16 lutego 2005 w sprawie ustalania „ Polityki bezpieczeństwa informatycznych służących do przetwarzania danych osobowych w Gminnym Ośrodku Pomocy Społecznej w Malechowie

§ 3 Zobowiązuję wszystkich pracowników Gminnego Ośrodka Pomocy Społecznej w Malechowie do stosowania zasad określonych w niniejszym zarządzeniu .

§ 4 Zarządzenie wchodzi w życie z dniem podpisania.

Kierownik Gminnego
Ośrodka Pomocy Społecznej
w Malechowie

/-/ Zdzisława Kubiak

Załącznik do Zarządzenia Nr 021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej Gminy Malechowo z dnia 25 maja 2018 roku w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych w Gminnym Ośrodku Pomocy Społecznej Gminy Malechowo

Polityka Bezpieczeństwa Danych Osobowych w Gminnym Ośrodku Pomocy Społecznej w Gminie Malechowo

PREAMBUŁA

Gminny Ośrodek Pomocy Społecznej w Gminie Malechowo (zwany dalej Ośrodkiem) świadomy wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających swoje dane osobowe do właściwej i skutecznej ochrony tych danych deklaruje zamiar:

podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych,

stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Ośrodku w zakresie problematyki bezpieczeństwa tych danych, w tym propagowania
świadomości wartości powierzonych Ośrodkowi danych osobowych jako czynnika wpływającego na jakość i ciągłość działalności oraz wiarygodności Ośrodka,

traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby,

doskonalenia i rozwijania nowoczesnych metod zabezpieczania danych

przed zagrożeniami związanymi z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych.

Użyte w dokumencie określenia oznaczają:

1. **Administrator Danych Osobowych (ADO)** - należy przez to rozumieć Gminny Ośrodek Pomocy Społecznej Malechowo, który ustala cele i sposoby przetwarzania informacji w tym danych osobowych, i jest reprezentowany przez Wójta Gminy Malechowo;
2. **Administrator Systemu Informatycznego (ASI)** - należy przez to rozumieć osobę wyznaczoną przez ADO, będącą odpowiedzialną za poprawne funkcjonowanie, zabezpieczenie oraz nadzór nad infrastrukturą i systemami informatycznymi służącymi do przetwarzania informacji w tym danych osobowych w Ośrodku ;
3. **aktywa -** zasoby niezbędne do realizacji czynności związanych z operacjami przetwarzania informacji w tym danych osobowych tj. procesy, informacje, personel, sprzęt, oprogramowanie, sieć, siedziba;
4. **analiza ryzyka** – systematyczne podejście mające na celu zidentyfikowanie w systemie źródeł ryzyka i przypisanie zidentyfikowanym ryzykom wartości;
5. **dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);
6. **grupa aktywów** - zbiór aktywów rozpatrywanych wspólnie ze względu na podobny charakter i funkcjonalność**;**
7. **incydent** – zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony informacji. Następuje w szczególności, gdy stan urządzenia, zawartości informacji, ujawnione metody pracy, sposób działania programu lub jakości komunikacji w sieci teleinformatycznej mogą wskazywać na naruszenie bezpieczeństwa informacji w tym danych osobowych;
8. **Inspektor Ochrony Danych (IOD)** – należy przez to rozumieć wyznaczoną osobę przez ADO, odpowiedzialną za nadzorowanie stosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszenia bezpieczeństwa informacji w tym danych osobowych przetwarzanych przez Ośrodek;
9. **KRI** – Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247);
10. **ocena ryzyka** – proces porównywania wartości ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
11. **osoba upoważniona** – osoba przeszkolona z zakresu bezpieczeństwa informacji w tym danych osobowych przetwarzanych przez Ośrodek oraz posiadająca imienne upoważnienie wydane przez ADO;
12. **podatność** – słabość aktywów, która może być wykorzystana przez zagrożenie. Podatność charakteryzuje łatwość, z jaką dane zagrożenie może wyrządzić szkodę;
13. **podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
14. **polityka** – Polityka bezpieczeństwa informacji w tym danych osobowych – zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania zatwierdzony przez ADO, będący zbiorem reguł dotyczących ochrony informacji w tym danych osobowych Ośrodka ;

15 **postępowanie z ryzykiem** – proces wyboru i wdrażania środków sterowania ryzykiem mających na celu zmianę wartości poziomu ryzyka;
16 **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
17 **ryzyko** – prawdopodobieństwo, że określone zagrożenie wykorzysta podatność aktywu lub grupy aktywów, aby spowodować straty lub szkody, co spowoduje niepożądane konsekwencje;
18 **ryzyko szczątkowe** – ryzyko, którego poziom nie przekracza akceptowanej wartości;
19 **skutek (ze strony zagrożenia**) - rezultat niepożądanego incydentu. Stopień strat powstałych w przypadku zaistnienia zagrożenia;
20 **Ośrodek** – Gminny Ośrodek Pomocy Społecznej w Malechowie - ADO
21 **UODO –** Urząd Ochrony Danych Osobowych;
22 **Ustawa -** Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
23 **PUODO –** Prezes Urzędu Ochrony Danych Osobowych;
24 **właściciel aktywa** osoba lub podmiot, który ma zatwierdzoną kierowniczą odpowiedzialność w organizacji za nadzorowanie wytworzenia, rozwój, utrzymanie, korzystanie i bezpieczeństwo aktywów. Pojęcie to nie oznacza, że osoba ta rzeczywiście posiada jakiekolwiek prawa własności do aktywów;
25 **zagrożenie** – potencjalna przyczyna niepożądanego incydentu, która może wywołać naruszenie praw i wolności osób fizycznych lub bezpieczeństwa informacji;
26 **zarządzanie ryzykiem** – jest to ciągły nadzór nad stanem bezpieczeństwa systemu. Zarządzanie ryzykiem jest to proces identyfikacji, kontrolowania, eliminacji lub ograniczania prawdopodobieństwa zaistnienia ewentualnych zdarzeń (zagrożeń), które mogą mieć wpływ na bezpieczeństwo informacji;
27 **zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

CZĘŚĆ I
INSTRUKACJA OCHRONY DANYCH OSOBOWYCH

ROZDZIAŁ 1

Przepisy ogólne i objaśnienia

§ 1

1 Polityka Bezpieczeństwa Danych Osobowych Gminnego Ośrodka Pomocy Społecznej Gminy Malechowo jest zbiorem zasad i procedur obowiązujących przy zbieraniu, utrwalaniu, organizowaniu, porządkowaniu, przechowywaniu, adaptowaniu lub modyfikowaniu, pobieraniu, przeglądaniu, wykorzystywaniu, ujawnianiu poprzez przesłanie, rozpowszechnianiu lub innego rodzaju udostępnianiu, ograniczeniu, usuwaniu lub niszczeniu danych osobowych we wszystkich zbiorach.

2 Przetwarzanie danych osobowych w Gminnym Ośrodku Pomocy Społecznej Gminy Malechowo jest dopuszczalne tylko pod warunkiem przestrzegania 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 (zwanej dalej RODO).

§ 2

Administrator Danych Osobowych zobowiązany jest do zapewnienia, aby dane osobowe były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów oraz przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne dla osiągniecia celu przetwarzania.

§ 3

1 Do realizacji postanowień niniejszej Polityki, Administrator Danych Osobowych wyznacza Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych.

2 Do zadań Inspektora ochrony danych należy:

2.a Określenie i przedstawienie do zatwierdzenia dla ADO zasad ochrony informacji w tym danych osobowych;

2.b Stałe informowanie ADO oraz pracowników o obowiązkach i odpowiedzialności spoczywającej na nich na mocy przepisów prawa z szczególnym uwzględnieniem RODO, KRI i innych aktów prawa dotyczących ochrony informacji w tym danych osobowych;

2.c monitorowanie przestrzegania przepisów prawa w zakresie bezpieczeństwa informacji w tym danych osobowych oraz polityki bezpieczeństwa ADO

2.d nadzorowanie i aktualizowanie dokumentacji w zakresie ochrony informacji w tym danych osobowych

2.e zapewnienie zapoznania osób upoważnionych do przetwarzania informacji w tym danych osobowych z przepisami w tym zakresie

2.f udzielanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie ich wykonania

2.g wydawanie i anulowanie upoważnień do przetwarzania informacji w tym danych osobowych

2.h wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony informacji w tym danych osobowych

2.i Nadzorowanie i kontrolowanie pracy Kierowników referatów, wszystkich pracowników w zakresie ochrony danych osobowych, oraz podmiotów zewnętrznych realizujących zadania mające wpływ na ochronę i bezpieczeństwo informacji w tym danych osobowych

2.j Dokonywanie systematycznych audytów i przeglądów stosowania przepisów w zakresie ochrony informacji w tym danych osobowych

2.k W ramach audytów i przeglądów, których mowa w pkt 4.6 ust. 10 IOD ma prawo:

- wstępu do pomieszczeń (również po godzinach pracy) w których przetwarzane są informacje w tym dane osobowe i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z RODO i KRI
- żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego
- żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli
- żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych

l) powołać za zgodą ADO do komisji kontrolującej przestrzeganie procedur ochrony informacji w tym danych osobowych pracowników Ośrodka w szczególności osoby pełniące funkcję ASI

m) niezwłocznie informować ADO o przypadkach naruszania przepisów RODO lub KRI a także zapisy dokumentacji wewnętrznej regulującej ten zakres.

n) prowadzenie ewidencji osób upoważnionych do przetwarzania informacji w tym danych osobowych w Ośrodka

o) prowadzenie i stała aktualizacja Rejestru czynności przetwarzania danych osobowych w Ośrodka

p) podejmowanie działań mających na celu doskonalenie procedur ochrony informacji w tym danych osobowych w Ośrodka

r) przeprowadzenie szkoleń z zakresu ochrony informacji w tym danych osobowych

s) reprezentowanie ADO w kontaktach z biurem UODO

t) pełnienie funkcji punktu kontaktowego dla osoby , której dane dotyczą

3 Do zadań Administratora Systemów Informatycznych należy w szczególności:

3.a zapewnienie optymalnej ciągłości działania systemu informatycznego,

3.b nadzór nad naprawami, konserwacją oraz likwidacja urządzeń komputerowych, na których zapisane są dane osobowe,

3.c nadawanie, zmiana i blokowanie uprawnień do systemów informatycznych,

3.d właściwa konfiguracja systemu informatycznego zapewniająca jego bezpieczeństwo

i ograniczenie dostępu do danych osobowych przez osoby nieupoważnione,

3.e monitorowanie funkcjonowania zabezpieczeń wdrożonych w celu ochrony danych osobowych,

3.f zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany,

3.g monitorowanie funkcjonowania zabezpieczeń nadzór nad czynnościami związanymi z prowadzeniem systemu sprawdzania oraz nadzorowanie wykonywanych procedur uaktualniania systemów antywirusowych i ich konfiguracji,

3.h podejmowanie działań w przypadku wykrycia naruszeń bezpieczeństwa w systemie zabezpieczeń lub podejrzenia naruszeń,

3.i nadzór nad wykorzystywanym oprogramowaniem oraz jego legalnością,

3.j wykonywanie i zarządzanie kopiami bezpieczeństwa ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu.

3.k nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do

przetwarzania danych osobowych.

3.l Konfigurowanie komputerów użytkowników i instalacje oprogramowania

ROZDZIAŁ 2
Gromadzenie i przetwarzanie danych osobowych

§ 4

1 Dane osobowe przetwarzane w Ośrodku mogą być uzyskiwane bezpośrednio od osób których dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa.

2 Jeżeli przetwarzane odbywa się na podstawie zgody, osoba, której dane dotyczą musi dobrowolnie wyrazić zgodę na przetwarzanie swoich danych osobowych. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę.

§ 5

1 W przypadku zbierania danych osobowych od osoby, której dane dotyczą oraz w przypadku pozyskiwania ich w sposób inny niż od osoby, której dane dotyczą Administrator Danych Osobowych wypełnia obowiązek informacyjny.

2 Obowiązek informacyjny, o którym mowa w pkt.1 jest spełniony w sposób zwięzły, przejrzysty i zrozumiały, w łatwo dostępnej formie, jasnym i prostym językiem.

§ 6

1 Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą.

2 W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe nie mające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

§ 7

1 W przypadku konieczności przetwarzania danych przez odrębne podmioty świadczące usługi dla Administratora Danych Osobowych może on powierzyć ich przetwarzanie. Powierzenie przetwarzania odbywa się na podstawie umowy.

2 Administrator Danych Osobowych prowadzi Ewidencję podmiotów, którym powierza

przetwarzanie danych. Wzór Ewidencji stanowi załącznik nr 1 do niniejszej Polityki.

§ 8

1 Inspektor Ochrony Danych prowadzi Rejestr czynności przetwarzania danych osobowych stanowiący załącznik nr 2 do niniejszej Polityki oraz sporządza Arkusz identyfikacji, oceny oraz określenia metod przeciwdziałania ryzyku stanowiący załącznik nr 3 do niniejszej Polityki.

2 Pracownicy poszczególnych komórek zgłaszają Inspektorowi Ochrony Danych zmiany dotyczące czynności przetwarzania danych osobowych w celu ich aktualizacji oraz wszystkie nowe czynności przetwarzania danych osobowych.

3 Pracownicy poszczególnych komórek zgłaszają Inspektorowi Ochrony Danych zagrożenia realizacji celów. Arkusz zgłoszenia ryzyka stanowi załącznik nr 4 do niniejszej polityki.

4 IOD prowadzi Rejestru kategorii czynności przetwarzania danych osobowych przetwarzanych

w imieniu innego administratora stanowiący załącznik nr 5 do niniejszej Polityki.

§ 9

Gminny Ośrodek Pomocy Społecznej Gminy Malechowo nie przetwarza danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, chyba że osoba, której powyższe dane dotyczą wyraziła pisemną zgodę lub przetwarzanie to jest niezbędne do wypełnienia obowiązków wynikających z obowiązujące przepisy prawa.

§ 10

1 Osoby zaangażowane w procesie przetwarzania danych osobowych są zobowiązane do przechowywania danych osobowych we właściwych zbiorach nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.

2 Osoby zaangażowane w procesie przetwarzania danych osobowych w systemach informatycznych są zobowiązane do postępowania zgodnie z „Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych”.

§ 11

1 Do przetwarzania danych osobowych są dopuszczeni jedynie osoby posiadające upoważnienie wydane przez ADO zgodnie z załącznikiem nr 6.

2 Osoby przetwarzające dane osobowe są zobowiązani do zachowania w tajemnicy danych osobowych do których mają dostęp w związku z wykonywanymi zadaniami służbowymi.

3 Nadanie upoważnienia do przetwarzania danych osobowych wymaga zaznajomienia się z przepisami dotyczącymi ochrony danych osobowych, w zakresie niezbędnym do czynności wykonywanych w ramach udzielonego upoważnienia.

4 Administrator Danych Osobowych jest odpowiedzialny za organizacje i przeprowadzenie szkoleń lub zaznajomienia osób upoważnionych z przepisami dotyczącymi ochrony danych osobowych.

5 Odbycie szkolenia z zakresu ochrony danych osobowych zostaje potwierdzone przez osobę w nim uczestniczącą w formie pisemnej. Wzór potwierdzenia uczestnictwa w szkoleniu stanowi załącznik nr 7 do niniejszej Polityki.

§ 12

Osoby przetwarzające dane są zobowiązane powiadomić IOD lub ASI o ewentualnych incydentach/ naruszeniach bezpieczeństwa systemu ochrony danych osobowych we wszystkich zbiorach. Tryb postępowania określa „Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych".

§ 13

Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe stanowi załącznik nr 8.

ROZDZIAŁ 3

Zbiory danych osobowych

§ 14

1 Pracownicy Ośrodka przetwarzający dane osobowe są zobowiązani do zgłoszenia Inspektorowi Ochrony Danych wszystkich informacji dotyczących powstania nowych zbiorów danych osobowych oraz wnoszenia zmian do zbiorów już istniejących. Wzór informacji o zbiorze danych osobowych stanowi załącznik nr 9 do niniejszej Polityki

2 ABI prowadzi wykaz zbiorów danych osobowych oraz systemów informatycznych zastosowanych do ich przetwarzania stanowiący załącznik nr 10 do niniejszej Polityki.

ROZDZIAŁ 4
Ochrona przetwarzania danych osobowych

§ 15

Administrator Danych Osobowych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostepnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 16

Administrator danych osobowych ma obowiązek uwzględniania zagadnień ochrony danych osobowych, prywatności osób, których dane dotyczą oraz wdrożenia domyślnych ustawień prywatności już na etapie projektowania i opracowywania sposobów przetwarzania danych oraz w każdym kolejnym etapie przetwarzania.

§ 17

Środki techniczne ochrony danych osobowych:

2.1 pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi),

2.2 pomieszczenia, w których przetwarzane są dane osobowe wyposażone są w system alarmowy

2.3 pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i wolnostojącej gaśnicy,

2.4 dokumenty oraz nośniki elektroniczne zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

§ 18

Zestawienie środków organizacyjnych i technicznych zapewniających ochronę danych osobowych u ADO:

1 został wyznaczony IOD;

2 został wyznaczony ASI;

3 została opracowana i wdrożona „Polityka bezpieczeństwa informacji w tym danych osobowych”;

4 została opracowana i wdrożona „Metodyka zarządza ryzykiem informacji w tym danych osobowych”;

5 został opracowany i wdrożony „Rejestr czynności przetwarzania danych osobowych”;

6 został opracowany i wdrożony „Plan ciągłości działania systemów informatycznych”;

7 zastosowane techniczne i organizacyjne środki bezpieczeństwa informacji oparte zostały na analizie ryzyka, posiadanej wiedzy oraz posiadanych środkach finansowych;

8 do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych;

9 prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;

10 osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;

11 osoby zatrudnione przy przetwarzaniu informacji w tym danych osobowych obowiązane zostały do zachowania ich w tajemnicy oraz metod zastosowanych do ich zabezpieczeń;

12 przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są informacje w tym dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu w/w informacji oraz w warunkach zapewniających ich bezpieczeństwo;

13 budynek Urzędu, w którym zlokalizowane są obszary przetwarzania danych osobowych jest nadzorowany przez zewnętrzną firmę ochroniarską przez całą dobę (zamykany po zakończeniu pracy);

14 wszystkie pomieszczenia, w których przetwarza się informacje w tym dane osobowe, są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania informacji w tym danych osobowych – także w godzinach pracy;

15 została opracowana i wdrożona „Polityka kluczy oraz zabezpieczeń budynku i pomieszczeń";

16 informacje w tym dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pendirve, płyta CD/DVD, dyskietka) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe – w szafach metalowych lub pancernych;

17 nieaktualne lub błędne wydruki zawierające informacje w tym dane osobowe niszczone są w niszczarkach;

18 dostęp do systemu operacyjnego komputerów na których przetwarzane są dane osobowe został zabezpieczony hasłem;

19 dostęp do zbioru danych osobowych w systemie teleinformatycznym wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika i hasła;

20 zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;

21 w pomieszczeniach gdzie obsługiwani są klienci Urzędu monitory komputerów, na których przetwarzane są informacje w tym dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane, w pozostałych pomieszczeniach dopuszcza się ustawienie monitora w inny sposób, jednak w przypadku przebywania w pomieszczeniu osoby nieupoważnionej do przetwarzania konkretnych informacji w tym danych osobowych – pracownik jest zobowiązany do uruchomienia wygaszacza, aby na monitorze nie było żadnych informacji zawierających dane osobowe;

22 cyklicznie wykonywane są kopie bezpieczeństwa, z których w przypadku awarii odtwarzane są dane;

23 Wszystkie urządzenia służące do przetwarzania danych osobowych połączone są kablem UTP kat.5 lub wyższej;

24 komunikacja z serwerem w sieci odbywa się przez sieć komputerową opartą na technologii FastEthernet 100 MB/s;

25 okablowanie strukturalne poprowadzone jest w korytach i nie ma do niego bezpośredniego dostępu;

26 programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje;

27 drzwi serwerowni wyposażone są, w co najmniej jeden zamek o skomplikowanym mechanizmie;

28 w serwerowni zainstalowano dwa klimatyzatory pracujące naprzemiennie;

29 do przebywania w serwerowni uprawnieni są: IOD, ASI oraz ADO;

30 przebywanie w pomieszczeniu serwera osób nieuprawnionych (konserwator, elektryk, sprzątaczka) dopuszczalne jest tylko w obecności jednej z osób upoważnionych, o których mowa wyżej, a w przypadku ich nieobecności – w obecności osoby pisemnie upoważnionej przez ADO;

31 pomieszczenia zabezpieczone są pod względem pożarowym zgodnie z obowiązującymi przepisami w tej materii;

32 wejście do stref przetwarzania zabezpieczone monitoringiem;

33 do zabezpieczenia stanowisk komputerowych przed oprogramowaniem złośliwym i wirusami stosowane jest oprogramowanie antywirusowe - poprawki bezpieczeństwa instalowane są na bieżąco i automatycznie;

34 Firewall zabezpiecza sieć wewnętrzną przed niepowołanym dostępem z zewnątrz;

35 serwery oraz komputery w Ośrodku są zabezpieczone przed utratą danych spowodowaną awarią zasilania lub zakłóceń w sieci zasilającej poprzez zastosowanie odrębnych UPS-ów;

36 w przypadku braku zasilania energetycznego z linii miejskiej budynek zasilany jest z zewnętrznego agregatu prądotwórczego załączanego automatycznie;

37 dostęp do informacji w tym danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora i hasła.

38 zastosowano czasowy mechanizm blokady dostępu po pięciokrotnym błędnym wprowadzeniu hasła do systemu;

39 hasła użytkowników na serwerze przechowywane są w formie niejawnej;

40 wykorzystano dostępne w aplikacjach środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;

41 zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych;

42 zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;

43 zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;

44 użytkownicy są zobowiązani do realizowania obowiązku zmiany hasła nie rzadziej, niż co 30 dni, a tam gdzie jest to możliwe ustawiony jest mechanizm wymuszenia zmiany hasła;

§ 19

1 W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je do Prezesa Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzkiem naruszenia prawa lub wolności osób fizycznych.

2 Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Ewidencja naruszeń bezpieczeństwa stanowi załącznik nr 11 do niniejszej Polityki.

3 Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

4 Pracownicy Gminnego Ośrodka Pomocy Społecznej Gminy Malechowo mają obowiązek niezwłocznie dokonać zgłoszenia naruszenia bezpieczeństwa ochrony danych osobowych, zgodnie z załącznikiem nr 12 do niniejszej Polityki.

§ 20

Zabezpieczenia danych osobowych w systemach informatycznych zostały opisane w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych".

§ 21

Nadzór i kontrolę nad przestrzeganiem zasad ochrony danych osobowych realizuje IOD.

1 IOD jest zobowiązany do prowadzenia:

1.a ewidencji osób upoważnionych do przetwarzania danych osobowych w Gminnym Ośrodku Pomocy Społecznej Gminy Malechowo, zgodnie z załącznikiem nr 13,

1.b prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych.

2 W celu realizacji powierzonych zadań IOD ma prawo:

2.a kontrolować komórki organizacyjne w Ośrodku w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe,

2.b wydawać polecenia koordynatorom komórek organizacyjnych w zakresie bezpieczeństwa danych osobowych,

2.c żądania od wszystkich pracowników wyjaśnień w sytuacjach naruszeń bezpieczeństwa danych osobowych.

ROZDZIAŁ 5

Zasady udostępniania danych osobowych

§ 22

Administrator Danych Osobowych oraz inne upoważnione osoby tj. pracownicy Ośrodka udostępniają dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 23

1 Zbiory danych udostępnia się na pisemny, umotywowany wniosek, chyba, że odrębne przepisy prawa stanowią inaczej.

2 Wniosek powinien zawierać informacje, umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.

3 Wniosek jest rozpatrywany przez Administratora Danych Osobowych lub inną upoważnioną osobę.

4 Decyzje w sprawie udostępnienia podejmuje Administrator Danych Osobowych osobiście lub inna upoważniona osoba.

5 Rejestr udostępnionych danych osobowych stanowi załącznik nr 14.

6 W komórkach organizacyjnych Ośrodka prowadzone są na bieżąco w formie papierowej lub elektronicznej rejestry udostępnianych danych osobowych.

§ 24

Administrator Danych Osobowych może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

CZĘŚĆ II
INFRASTRUKTURA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH

ROZDZIAŁ 1

Przepisy ogólne i objaśnienia

§ 25

1 Instrukcja Zarządzania Systemami Informatycznymi, zwana dalej „Instrukcją” jest dokumentem eksploatacyjnym, regulującym zasady oraz procedury używania, zarządzania

i administrowania systemami informatycznymi służącymi do przetwarzania danych osobowych, wykorzystywanymi w Gminnym Ośrodku Pomocy Społecznej Gminy Malechowo.

2 Instrukcja obejmuje swoim zakresem wszystkie osoby zatrudnione w Ośrodku, które biorą udział w procesie przetwarzania danych osobowych w systemach informatycznych.

3 Nieprzestrzeganie postanowień niniejszej instrukcji oraz brak nadzoru nad bezpieczeństwem informacji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej przepisami Kodeksu Pracy. Jeżeli skutkiem działania użytkownika jest ujawnienie informacji osobie nieupoważnionej, sprawca może być pociągnięty do odpowiedzialności karnej określonej przepisami Kodeksu Karnego. Jeżeli skutkiem działania użytkownika jest szkoda materialna, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Kodeksu Cywilnego.

4 Polityka ustanawia procedury obowiązujące dla:

4.a Zbierania i przetwarzania danych osobowych przy użyciu systemu informatycznego,

4.b Powierzenia danych osobowych przetwarzanych przy użyciu systemu informatycznego upoważnionym podmiotom wewnętrznym i zewnętrznym,

4.c Uwierzytelniania dostępu podmiotów wewnętrznych i zewnętrznych do systemu informatycznego Podmiotu służącego do przetwarzania danych osobowych,

4.d Zapewnienia bezpieczeństwa systemu informatycznego i telekomunikacyjnego,

wykorzystywanego przy przetwarzaniu danych osobowych przez podmiot,

4.e Zapewnienia bezpieczeństw zbiorów danych osobowych przetwarzanych przy użyciu systemu informatycznego,

4.f Korzystania z jednostki roboczej, sieci Internet i poczty e-mail przy użyciu systemu informatycznego Podmiotu,

4.g Zapewnienia bezpieczeństwa i korzystania z aplikacji stosowanych przy przetwarzaniu danych przy użyciu systemu informatycznego,

4.h Postepowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego.

5 Podmiot dochowuje należytej staranności przy zapewnianiu ochrony danych osobowych przetwarzanych w toku jego działalności w ramach systemu informatycznego którym się posługuje.

6 Przestrzeganie procedur ustanowionych w Instrukcji jest konieczne dla realizacji zasad zgodnego z prawem przetwarzania danych osobowych.

ROZDZIAŁ 2

Słowniczek

§ 26

Ilekroć w niniejszej Instrukcji jest mowa o:

1 Identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

2 Integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

3 Haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

4 Osobie upoważnionej – rozumie się przez to użytkownika systemu informatycznego uprawnionego do przetwarzania danych osobowych;

5 Poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

6 Raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

7 Rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

8 Uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

ROZDZIAŁ 3

Poziom bezpieczeństwa

§ 27

Poziom bezpieczeństwa systemów informatycznych przetwarzających dane osobowe określono jako wysoki. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną. Na bezpieczeństwo procesu przetwarzania danych osobowych składają się rozliczalność, poufność i integralność przetwarzanych danych.

1 Obszar, w którym przetwarza się dane osobowe zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

2 Przebywanie osób nieuprawnionych w obszarze w którym przetwarza się dane osobowe jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

3 W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.

4 Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

4.a W systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;

4.b Dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora

i dokonaniu uwierzytelnienia.

5 System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

5.a Działaniem oprogramowania, którego celem jest uzyskania nieuprawnionego dostępu do

systemu informatycznego;

5.b Utrata danych spowodowana awarią zasilania lub zakłóceniami w sieci zasilającej.

6 Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być

przydzielony innej osobie.

7 W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielki litery oraz cyfry lub znaki specjalne. Hasła nie mogą zawierać loginu konta, do którego tworzone jest hasło, oraz innych informacji słownikowych.

8 Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych osobowych.

9 Kopie zapasowe:

9.a Przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;

9.b Usuwa się niezwłocznie po ustaniu ich użyteczności.

10 Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarza się dane osobowe, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

11 Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

11.a Likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to

możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

11.b Przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

11.c Naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

12 System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

13 Zabezpieczenia logiczne, o których mowa w pkt. 12, obejmują:

13.a Kontrolę przepływu informacji pomiędzy systemem informatycznym administratora
danych a siecią publiczną;

13.b Kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego

administratora danych.

14 Administrator Danych Osobowych stosuje środki kryptograficznej ochrony wobec danych

wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej.

15 Administrator Danych Osobowych monitoruje wdrożenie zabezpieczenia systemu informatycznego, stosując na poziomie wysokim środki bezpieczeństwa.

16 Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych szczegółowo określone zostały w Polityce Bezpieczeństwa.

ROZDZIAŁ 4
Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemach informatycznych

§ 28

1 Każdy użytkownik przed przystąpieniem do przetwarzania danych zapoznaje się z Polityką Bezpieczeństwa Informacji w Gminnym Ośrodku Pomocy Społecznej Gminy Malechowo oraz otrzymuje upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych Osobowych.

2 Stosowany w Ośrodku schemat uprawnień zakłada, iż użytkownicy uzyskują dostęp do sieci komputerowej i do systemów informatycznych na z góry zdefiniowanym poziomie uprawnień użytkownika w zależności od zakresu obowiązków i powierzonych zadań do wykonania na danym stanowisku.

3 Rejestracji użytkowników w danym systemie dokonuje Administrator Systemów Informatycznych. Użytkownik po otrzymaniu od ASI informacji o założonym koncie z wymaganymi uprawnieniami, loguje się na nie w celu sprawdzenia poprawności otrzymanych informacji i uprawnień.

4 Wyłączenie użytkownika z ewidencji osób upoważnionych do przetwarzania danych osobowych lub rozwiązanie stosunku pracy lub umowy o innym charakterze obliguje ASI do odebrania temu użytkownikowi możliwości dostępu do danych osobowych przetwarzanych w systemach informatycznych.

5 Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych nie jest usuwany z systemu informatycznego i nie jest przydzielany innej osobie.

ROZDZIAŁ 5

Metody i środki uwierzytelniania w systemach informatycznych oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 29

1 Do uwierzytelniania użytkownika podczas dostępu do sieci komputerowej i systemów informatycznych używa się identyfikatorów i haseł. Stosowanie unikalnych identyfikatorów użytkownika zapewnia bezpieczeństwo i realizuje zasady rozliczalności – wszelkie działania w systemie przypisywane są konkretnemu użytkownikowi (nie dopuszcza się aby użytkownik korzystał z konta innego użytkownika),

2 Hasło użytkownika musi składać się z minimum 8 znaków, w tym minimum jedna wielka litera i jedna cyfra lub znaki specjalne.

3 Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: identyfikatorów, dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów bądź innych słów bezpośrednio kojarzących się z użytkownikiem.

4 Hasło nie może być ujawnione innej osobie nawet po utracie jego ważności.

5 Użytkownik musi zmieniać hasło nie rzadziej, niż raz na 30 dni.

6 Hasło przy wpisywaniu nie może być w sposób jawny wyświetlane na ekranie.

7 Obowiązuje bezwzględny zakaz notowania w jakiejkolwiek formie obecnych oraz wygasłych haseł dostępu.

8 Użytkownik ponosi pełną odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

9 Hasła administracyjne zapisane są za pomocą dedykowanego oprogramowania i zaszyfrowane. Klucz oraz hasło do rozszyfrowania haseł administracyjnych przechowywany jest w sejfie.

ROZDZIAŁ 6
Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemów

§ 30

1 Dostęp użytkowników do zasobów sieci komputerowej Ośrodka jest ograniczony, ze względu na czas i sytuacje opisane w Regulaminie Pracy Ośrodka.

2 Podczas rozpoczęcia pracy w sieci komputerowej użytkownik jest autoryzowany poprzez podanie swojego identyfikatora i hasła. Dopiero po pomyślnej autoryzacji w sieci komputerowej użytkownik może uzyskać możliwość uruchomienia programu służącego do przetwarzania danych osobowych, dokonując osobnej autoryzacji w tym programie.

3 Przy każdorazowym opuszczeniu stanowiska komputerowego, użytkownik jest zobowiązany dopilnować, aby na ekranie nie były wyświetlane informacje lub dane osobom nieuprawnionym, poprzez:

3.a zablokowanie komputera odpowiednią kombinacją klawiszy, lub

3.b stosowanie wygaszacza ekranu zabezpieczonego hasłem, lub

3.c wylogowanie się z sieci komputerowej.

4 Użytkownik jest zobowiązany do zadbania, aby niemożliwe było odczytanie informacji

z monitora przez osoby nieuprawnione.

5 Podczas kończenia pracy na danej stacji roboczej należy:

5.a wylogować się z systemu informatycznego,

5.b wylogować się z sieci komputerowej, zamknąć system operacyjny komputera i zaczekać na jego wyłączenie,

5.c sprawdzić czy elektroniczne nośniki informacji zawierające dane osobowe nie zostały pozostawione bez nadzoru.

6 Użytkownik w pełnym zakresie odpowiada za powierzony mu sprzęt komputerowy i wykonane czynności aż do momentu rozliczenia ze sprzętu komputerowego.

7 W sytuacji naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego, użytkownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie ABI lub ASI.

ROZDZIAŁ 7
Procedury tworzenia kopii zapasowych zbiorów danych

§ 31

1 Zasady tworzenia kopii zapasowych umożliwiające otworzenie funkcjonalności systemu informatycznego określa załącznik nr 16 i jest przeznaczony jedynie dla ADO, ASI i osób wskazanych przez ADO.

2 W przypadku braku możliwości wykonywania kopii bezpieczeństwa wykonywanych na komputerach użytkowników dotyczących plików pomocniczych, za kopie odpowiada użytkownik komputera.

3 Przechowywanie elektronicznych nośników odbywa się zgodnie z technicznymi warunkami składowania nośników magnetycznych, określonych przez producenta nośników.

4 Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub sejfie, za wyjątkiem dysków komputerowych, które są zamontowane na stałe w komputerach.

5 Urządzenia, dyski lub inne informatyczne nośniki, zawierające informacje w tym dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

6 Podlegające likwidacji uszkodzone lub przestarzałe nośniki, a w szczególności twarde dyski z informacjami w tym danymi osobowymi są komisyjnie niszczone w sposób fizyczny.

7 Urządzenia, dyski lub inne informatyczne nośniki, zawierające informacje w tym dane osobowe, nie mogą podlegać przekazaniu innemu podmiotowi, nieuprawnionemu do otrzymywania w/w informacji.

8 W sytuacji przekazania nośników z danymi poza obszar organizacji należy stosować następujące zasady bezpieczeństwa:

1 nadawca musi znać podstawę prawną przekazania danych poza organizację;

2 adresat winien być poinformowany o przesyłce;

3 nadawca wykonuje kopie wysyłanych danych;

4 dane przed wysłaniem winne być zaszyfrowane i zabezpieczone hasłem;

5 hasło podaje się adresatowi innym kanałem komunikacyjnym niż przesłany plik z danymi;

6 adresat jest zobowiązany do potwierdzenia otrzymania danych.

9 Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

10 Czas przechowywania nośników elektronicznych, na których są przechowywane dane osobowe nie może być dłuższy niż wynikający z celu przetwarzania danych.

11 W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.

12 Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, użytkownik zniszczy w sposób uniemożliwiający ich odczytanie.

13 Wydruki przechowywane w pomieszczeniach przeznaczonych do przetwarzania danych osobowych po godzinach pracy muszą być zamykane w szafach zabezpieczonych zamkami.

14 Zewnętrzne nośniki elektroniczne zawierające dane osobowe są ewidencjonowane przez ASI w „Rejestrze nośników komputerowych zawierających dane osobowe" – wzór stanowi załącznik nr 19.

ROZDZIAŁ 8

Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

§ 33

1 Elektroniczne nośniki informacji:

1.a dane w postaci elektronicznej przetwarzane w systemie zapisane na nośnikach materialnych (płytach CD\DVD, pamięciach przenośnych czy dyskach twardych) są własnością Ośrodka,

1.b w/w elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych,

1.c po zakończeniu pracy przez użytkownika systemu informatycznego, w/w elektroniczne nośniki informacji są przechowywane w meblach biurowych,

1.d elektroniczne nośniki informacji, o których mowa powyżej powinny być oznaczone w sposób umożliwiający ich identyfikację.

2 Przekazywanie i niszczenie elektronicznych nośników informacji:

2.a elektroniczne nośniki informacji zawierające dane osobowe można przekazywać tylko podmiotom lub osobom uprawnionym na podstawie przepisów prawa, za zgodą osoby do tego upoważnionej przez Administratora Danych Osobowych,

2.b dane osobowe na każdym nośniku zewnętrznym powinny być zabezpieczone przed odczytem (minimum hasłem),

2.c dane osobowe przenoszone za pomocą zewnętrznych nośników informacji powinny być z nich trwale usunięte po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy i do docelowej bazy danych,

2.d przekazanie i niszczenie elektronicznych nośników informacji zawierających dane osobowe, odbywa się na podstawie protokołu podpisanego przez ADO, ABI oraz właściwych użytkowników.

3 Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.

ROZDZIAŁ 9
Środki ochrony systemów informatycznych przed tzw. „szkodliwym oprogramowaniem” oraz próbami dostępu przez osoby nieuprawnione

§ 34

1 Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.

2 W przypadku przesyłania informacji w szczególności zawierających dane osobowe pocztą e-mail wewnątrz lub na zewnątrz Urzędu należy wykorzystywać mechanizmy kryptograficzne (szyfrowanie danych lub pakowanie i zabezpieczenie hasłem wysyłanych informacji).

3 Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej od nieznanego nadawcy lub podejrzanych załączników nadanych od znanego nadawcy.

4 Na każdym stanowisku komputerowym jest zainstalowane oprogramowanie antywirusowe.

5 Wszelkie oprogramowanie instalowane na komputerach może być tylko instalowane przez ASI, lub inną wskazaną osobę.

6 Niedopuszczalne jest zmienianie ustawień oprogramowania antywirusowego oraz instalowanie oprogramowania niebędącego własnością Urzędu na komputerach przez użytkowników.

7 Każdy e-mail wpływający do Urzędu jest sprawdzany pod kątem występowania wirusów.

8 Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła.

9 Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym, lub innym zakazanym przez prawo.

10 Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

11 Definicje wzorców wirusów aktualizowane są na bieżąco – on-line.

12 Zabrania się używania nośników niewiadomego pochodzenia oraz podłączania do komputerów jakichkolwiek urządzeń prywatnych (np. telefonów, pendrive itp.).

13 Zabrania się wynoszenia nośników będących własnością Urzędu poza obszar Urzędu.

14 Nośnik zewnętrzny każdorazowo jest sprawdzany programem antywirusowym.

15 Zabrania się pobierania z Internetu plików niewiadomego pochodzenia.

16 W razie wykrycia wirusa przez program, użytkownik winien niezwłocznie zgłosić to zdarzenie do ASI.

17 W przypadku podjęcia podejrzeń, iż oprogramowanie mogło powodować ryzyko naruszenia bezpieczeństwa danych osobowych należy postępować zgodnie z działem XVIII Polityki - Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych.

18 Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

19 W przypadku wykrycia wirusów komputerowych komputer, na którym wykryto wirusy odłączany jest od sieci.

20 Kontrole, antywirusowe wykonuje się bez zbędnej zwłoki na wszystkich komputerach i nośnikach w przypadku wykrycia oprogramowania złośliwego na jednym komputerze lub nośniku będącym własnością Urzędu.

21 Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ASI.

§ 35

1 ASI jest odpowiedzialny za aktywowanie i poprawną konfigurację specjalistycznego oprogramowania monitorującego wymianę danych na styku:
1.a sieci lokalnej i sieci zewnętrznej,

1.b stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

2 ASI obowiązany jest do utrzymywania stałej aktywności zainstalowanego specjalistycznego oprogramowania monitorującego wymianę danych oraz do jego aktualizacji.

ROZDZIAŁ 10

Procedury wykonywania przeglądów i konserwacji sprzętu oraz systemów informatycznych

§ 36

1 Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.

2 Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. Zaistniały fakt ASI odnotowuje w dzienniku dla systemu informatycznego (stanowiącego załącznik nr 12).

3 Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.

4 Bezwzględnie należy przestrzegać zasady, że gdy naprawa/serwis/przegląd /konserwacja sprzętu, na którym są przetwarzane informacje w tym dane osobowe ma odbywać się w siedzibie Urzędu – to tylko w obecności upoważnionego pracownika.

5 Ze sprzętu uszkodzonego przeznaczonego do naprawy poza jednostką, lub zniszczenia muszą zostać usunięte wszystkie nośniki informacji, a fakt wymontowania musi być odnotowany w dzienniku dla systemu informatycznego.

6 Każde działanie serwisu musi zostać poprzedzone wcześniejszą informacją dla ASI lub osoby przez niego wyznaczonej o zakresie planowanych prac, terminie oraz czasie prac.

7 Po zakończeniu działań serwisu zewnętrznego na sprzęcie i aplikacjach służących do przetwarzania danych osobowych należy sprawdzić stan systemu, poprawność praw dostępu i uprawnień użytkowników systemu.

8 Awarie, naprawy, przeglądy oraz konserwacje należy odnotować w dzienniku dla systemu informatycznego urządzenia- stanowiący załącznik nr 12.

9 W przypadku podjęcia podejrzeń, iż awaria sprzętu mogła powodować ryzyko naruszenia bezpieczeństwa danych osobowych należy postępować zgodnie z działem XVIII Polityki – Postępowanie w sytuacji naruszenia bezpieczeństwa informacji w tym danych osobowych.

10 Nośniki informatyczne zawierające informacje w tym dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione oraz powinny zostać zarejestrowane w „Rejestrze nośników komputerowych zawierających dane osobowe", który prowadzi ASI.

11 Dyski lub inne informatyczne nośniki, zawierające informacje w tym dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie. Fakt ten musi być odnotowany w dzienniku dla systemu informatycznego.

12 Likwidację nośników informacji przeprowadza komisja powołana przez Administratora Danych Osobowych. W protokole potwierdzającym likwidację danych wskazuje się: skład osobowy komisji, datę likwidacji i sposób usunięcia nośnika danych, nazwa zbioru, do którego był on wykorzystywany.

ROZDZIAŁ 11
Dostęp zdalny do systemów informatycznych Ośrodka

§ 37

a.1 Pod pojęciem zdalnego dostępu do systemów informatycznych rozumie się połączenie z systemem informatycznym Ośrodka z lokacji znajdującej się poza siedzibą.

a.2 Zdalnego połączenia z systemem informatycznym Ośrodka mogą dokonać wyłącznie osoby do tego upoważnione.

a.3 System, z którego osoba upoważniona dokonuje dostępu zdalnego powinien posiadać odpowiednie zabezpieczenia i odpowiadać wymogom systemów używanych przy przetwarzaniu danych osobowych.

ROZDZIAŁ 12

Postanowienia końcowe

§ 38

1 Instrukcja zarządzania systemem informatycznym stanowi integralną część Polityki Bezpieczeństwa i jest dokumentem obowiązującym Podmiot w zakresie wdrażania, przestrzegania i weryfikacji zasad ochrony danych osobowych.

2 Instrukcja zarządzania systemem informatycznym jest dokumentem obowiązującym wszystkie osoby dopuszczone do przetwarzania danych osobowych w ramach działalności podmiotu.

3 Każda osoba dopuszczona do przetwarzania danych osobowych w ramach działalności Podmiotu ma obowiązek zapoznania się z niniejszą Instrukcją zarządzania systemem informatycznym.

4 Naruszenie zasad wynikających z Polityki Bezpieczeństwa Danych Osobowych oraz z Instrukcji zarządzania systemem informatycznym może stanowić podstawę wszczęcia postępowania dyscyplinarnego przeciwko sprawcy naruszenia.

5 Wszczęcie lub przeprowadzenie postępowania dyscyplinarnego przeciwko osobie naruszającej zasady wynikające z Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym nie wyklucza możliwości wszczęcia postępowania karnego oraz dochodzenia roszczeń z powództwa cywilnego

CZĘŚĆ III
Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

ROZDZIAŁ 1

Opis zdarzeń naruszających ochronę danych osobowych

§ 38

Podział zagrożeń:

1 zagrożenia losowe zewnętrzne (np. klęski żywiołowe, zalania, ogień, przerwy w zasilaniu w energię elektryczną, zwarcia i przepięcia w sieci elektroenergetycznej). Ich występowanie może prowadzić do utraty integralności danych, ich uszkodzenia, zniszczenia, uszkodzenia systemów komputerowych oraz elementów technicznych komputera lub sieci. Ciągłość systemu zostaje zakłócona, jednak nie dochodzi do naruszenia poufności danych,

2 zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, działanie wirusów). Może dojść do zniszczenia danych, zakłócenia ciągłości pracy systemu lub naruszenia poufności danych,

3 zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na:

- nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do systemu z jego wnętrza,
- nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie składników technicznych systemu.

§ 39

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe to:

1 sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,

2 niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

3 awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,

4 pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,

5 jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,

6 naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,

7 stwierdzenie próby modyfikacji danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),

8 niedopuszczalna manipulacja danymi osobowymi w systemie,

9 ujawnienie osobom nieupoważnionym danych osobowych, objętych tajemnicą procedur ochrony przetwarzania lub innych strzeżonych elementów zabezpieczeń systemu,

10 praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy, co świadczy o przełamaniu lub zaniechaniu ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu do sieci lub komputera, itp.,

11 ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. "luk

w systemie", itp.,

12 podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia

oraz skasowanie lub skopiowanie w sposób niedozwolony danych osobowych,

13 rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie z programu, systemu przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, prace na danych osobowych w celach prywatnych, itp.).

§ 40

1. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. papier (wydruki), dyskietki, płyty CD/DVD w formie niezabezpieczonej itp.

ROZDZIAŁ 2

Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 41

1 Każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie IOD i/lub ASI w przypadku stwierdzenia naruszenia:

1.1 zabezpieczenia systemu informatycznego,

1.2 technicznego stanu urządzeń,

1.3 zawartości zbioru danych osobowych,

1.4 ujawnienia metody pracy lub sposobu działania programu,

1.5 jakości transmisji danych w sieciach komputerowych mogącej wskazywać na naruszenie zabezpieczeń tych danych,

1.6 innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie pomieszczeń, pożar, itp.).

2 W razie niemożliwości zawiadomienia IOD i/lub ASI należy powiadomić Administratora Danych Osobowych.

3 Wzór zgłoszenia naruszenia bezpieczeństwa ochrony danych osobowych stanowi załącznik nr 12 do niniejszej Polityki.

§ 42

Czynności podejmowane przez IOD i/lub ASI w przypadku stwierdzenia naruszenia ochrony danych osobowych:

1 poinformowanie osoby zgłaszającej o dalszym trybie postępowania oraz zlecenie jej właściwego wykonywania czynności,

2 podjęcie czynności niezbędnych dla powstrzymania niepożądanych skutków zaistniałego naruszenia oraz w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych,

3 ustalenie czasu trwania i charakteru naruszenia, w miarę możliwości określić kategorie i przybliżoną liczbę osób, których dotyczy naruszenie,

4 ustalić możliwe konsekwencje naruszenia ochrony danych osobowych,

5 zarekomendować działania zapobiegawcze w kierunku wyeliminowania podobnych zagrożeń w przyszłości,

6 w przypadku naruszenia ochrony danych osobowych, bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – dokonać zgłoszenia do Prezesowi Urzędu Ochrony Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia),

7 w razie konieczności zainicjowanie działań dyscyplinarnych,

8 udokumentowanie prowadzonego postępowania w rejestrze naruszeń bezpieczeństwa danych osobowych stanowiącym załącznik nr 10 do niniejszej Polityki.

Załącznik nr 1 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

EWIDENCJA PODMIOTÓW KTÓRYM POWIERZONO DANE OSOBOWE

Lp.	Nazwa i adres podmiotu	Data powierzenia	Data końca/ cofnięcia powierzenia	Cel powierzenia

Załącznik nr 2 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr 021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

Załącznik nr 3 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr 021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

Załącznik nr 4 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr 021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

ARKUSZ ZGŁOSZENIA RYZYKA				
Nazwa komórki organizacyjnej:				
Imię i nazwisko osoby zgłaszającej:				
I. Działanie/proces w jakim występuje ryzyko:				
Zagrożony cel:				
Potencjalne ryzyko	**Przyczyny (czynnik ryzyka)**	**Prawdopodobieństwo wystąpienia:**	**Skutki:**	**Uwagi:**
Wprowadzić do arkusza identyfikacji, oceny oraz określania metody przeciwdziałania ryzyku*				
☐ **Tak** ☐ **Nie** *właściwe zaznaczyć				
Data i podpis osoby zgłaszającej:				
Data i podpis osoby przyjmującej:				
Podjęte działania:				
Spodziewane efekty:				
II. Działanie/proces w jakim występuje możliwość usprawnienia:				
Data i podpis osoby zgłaszającej:				
Data i podpis osoby przyjmującej:				
Podjęte działania:				

Spodziewane efekty:	

Załącznik nr 5 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr 021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

Załącznik nr 6 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr 021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

……

(miejscowość, data)

U P O W A Ż N I E N I E

DO PRZETWARZANIA INFORMACJI W TYM DANYCH OSOBOWYCH

Nr……/……..

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz art. 20 pkt 2 ust. 4 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz ……
……
……

upoważniam z dniem……..

Panią/Pana ……

do przetwarzania informacji w tym danych osobowych zawartych w zbiorze o nazwie:

……..

w systemie tradycyjnym i/lub informatycznym - w programie ……..

w zakresie……..

(zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie, udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie, pełnym, innym – podać jakim) **

Identyfikator……

(wypełnia się w przypadku gdy dane przetwarzane są w systemie informatycznym)

Okres trwania upoważnienia……..

(okres obowiązywania upoważnienia)

……..

(podpis ADO lub osoby upoważnionej)

Przyjmuje do wiadomości i przestrzegania,

Zobowiązuje się do zachowania w poufności tych danych

oraz sposobów ich zabezpieczeń

……

Data i podpis osoby upoważnionej

* niepotrzebne skreślić

** wskazać odpowiednie

Załącznik nr 7 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr 021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

…….. ……

(imię i nazwisko) *(miejscowość, data)*

OŚWIADCZENIE

Oświadczam, iż zostałam/zostałem przeszkolona/przeszkolony z zakresu przepisów dotyczących ochrony informacji w tym danych osobowych, w szczególności 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 w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE i §15 - 21 rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, a także wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki Bezpieczeństwa Danych Osobowych w Gminnym Ośrodku Pomocy Społecznej w Gminie Malechowo ”.

Zobowiązuję się do:

- respektowanie w/w wymienionych aktów prawnych i dokumentów;
- zachowania w tajemnicy informacji w tym danych osobowych uzyskanych w związku z zatrudnieniem oraz sposobów ich zabezpieczania, również po ustaniu stosunku pracy;
- korzystania ze sprzętu teleinformatycznego będącego własnością pracodawcy wyłącznie w związku z wykonywaniem obowiązków pracowniczych;
- wykorzystywania jedynie legalnego oprogramowania będącego własnością pracodawcy;
- należytej dbałości o sprzęt i oprogramowanie.

……..

podpis pracownika

Załącznik nr 8 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr 021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

WYKAZ BUDYNKÓW I POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

Lp.	Miejsce

Załącznik nr 9 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr 021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

Załącznik nr 10 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr 021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

Załącznik nr 11 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr 021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

Załącznik nr 12 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr 021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

ZGŁOSZENIE NARUSZENIA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

1. Data: ..... Godzina: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu: .....
..... (Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia: .....
..... (np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące: .....
.....
.....

5. Podjęte
działania: .....
.....
.....

6. Przyczyny wystąpienia
zdarzenia: .....
.....
.....

7. Postępowanie
wyjaśniające .....
.....
.....

.....

(Data i podpis Administratora Bezpieczeństwa Informacji)

Załącznik nr 13 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr 021.29.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

Załącznik nr 14 do Polityki Bezpieczeństwa stanowiącej załącznik do Zarządzenia nr 14 Kierownika Gminnego Ośrodka Pomocy Społecznej w Malechowie z dnia 25 maja 2018

CZĘŚĆ IV
Metodyka zarządzaniem ryzykiem w ochronie informacji w tym danych osobowych

ROZDZIAŁ 1

Postanowienia ogólne

1 Metodyka zarządzania ryzykiem w ochronie informacji w tym danych osobowych (zwana dalej „Metodyką) wspiera zapewnienie adekwatnych oraz skutecznych środków organizacyjnych i technicznych minimalizujących ryzyko naruszenia praw i wolności osób fizycznych, zapewnienie ochrony przed nieuprawnionym dostępem do informacji w tym danych osobowych i aktywów służących ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i aktywów.

2 Metodyka jest zgodna z wymogami prawa tj.:

- Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE -zwanym dalej RODO;

- Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jednolity Dz.U. 2017 poz. 2247) - zwanym dalej KRI;

3 Metodyka bazuje na:

- Wytycznych grupy roboczej art. 29 dotyczących oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679;

- Polskiej Normie PN-ISO/IEC 27005 – Technika informatyczna, technika bezpieczeństwa, zarządzanie ryzykiem w bezpieczeństwie informacji;
- Polskiej Normie PN-ISO/IEC 31000 – Zarządzanie ryzykiem – zasady i wytyczne;
- Podręczniku wdrożenia systemu zarządzania ryzykiem w administracji publicznej w Polsce – Ministerstwo Finansów;
- Metodyce zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych – Ministerstwo Cyfryzacji.

4 Metodyka w Gminnym Ośrodku Pomocy Społecznej została ustanowiona między innymi w związku z art. 24 ust. 1, art. 25 ust 1, art. 32, art. 35 RODO oraz w związku z art. 20 ust. 2 pkt 3 KRI.

5 Metodyka odnosi się do zarządzania ryzykiem w kontekście zarządzania bezpieczeństwem informacji oraz respektowania praw i wolności osób fizycznych, których dane osobowe przetwarza GOPS.

6 Metodyka opisuje reguły dotyczące bezpieczeństwa informacji w tym danych osobowych przetwarzanych zarówno w formie tradycyjnej, np. w postaci teczek, akt czy wydruków oraz w systemie informatycznym służącym do przetwarzania informacji lub danych osobowych w Gminnym Ośrodku Pomocy Społecznej.

7 Zasady określone w niniejszej Metodyce oraz w dokumentach powiązanych powinny być znane i stosowane przez wszystkie osoby, które biorą udział w procesie analizy ryzyka bez względu na zajmowane stanowisko, jak również charakter stosunku pracy.

8 Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszego dokumentu, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony informacji oraz danych osobowych, a także realizacji praw osób, których te dane dotyczą w procesie przetwarzania przez Gminny Ośrodek Pomocy Społecznej.

9 Metodyka nie ma zastosowania do analizy ryzyka informacji niejawnych przetwarzanych w myśl Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

ROZDZIAŁ 2

Definicje

1 Użyte w niniejszym dokumencie pojęcia są tożsame z definicjami zawartymi w dziale Polityka Bezpieczeństwa Danych Osobowych w Gminnym Ośrodku Pomocy Społeczne w Malechowie.

ROZDZIAŁ 3
Zarządzanie ryzykiem - założenia

1 Zarządzanie ryzykiem w ochronie informacji w tym danych osobowych jest procesem ciągłym, monitorującym adekwatność oraz skuteczność stosowanych zabezpieczeń organizacyjnych i technicznych, w celu utrzymania ryzyka na akceptowalnym poziomie.

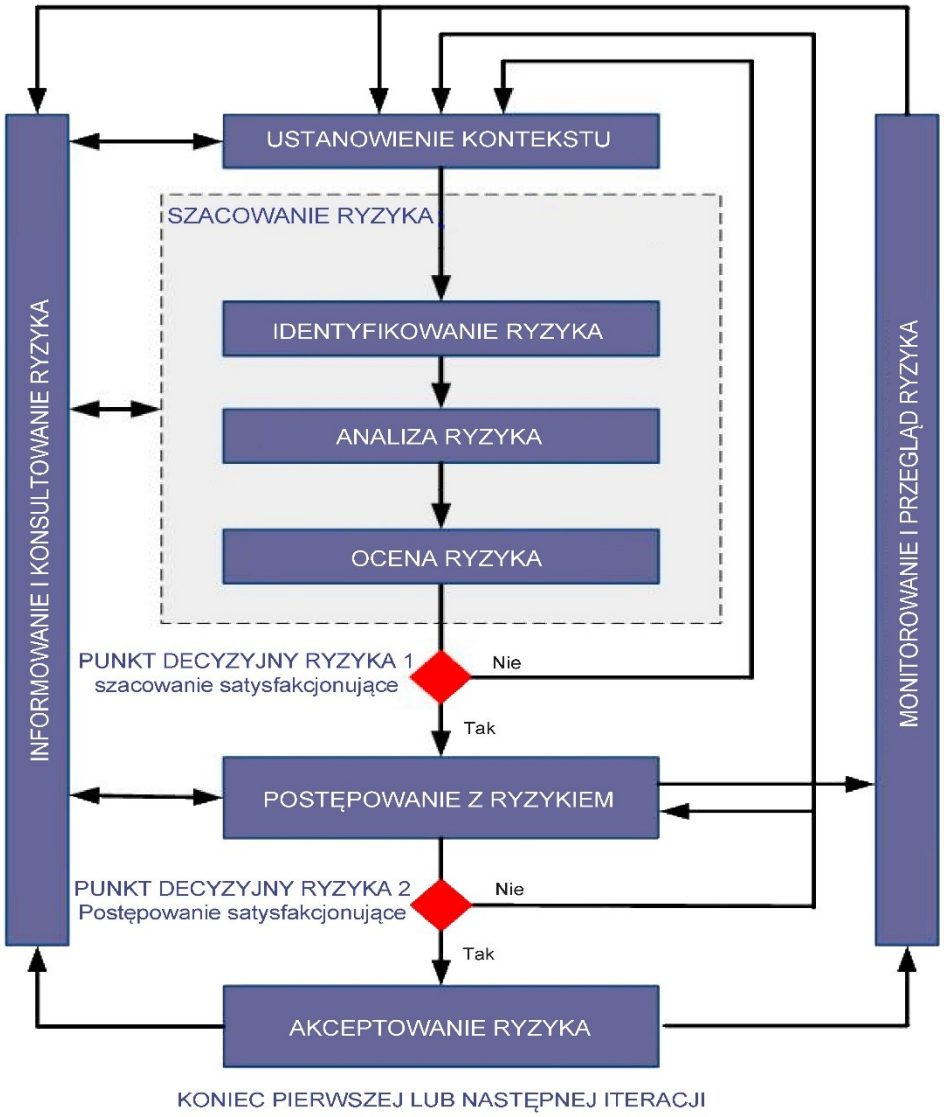
2 Do analizy ryzyka wykorzystywana jest matryca skutek/prawdopodobieństwo.

3 Odpowiedzialności osób funkcyjnych biorących udział w przetwarzaniu informacji w tym danych osobowych zostały opisane w Polityce Bezpieczeństwa.

4 Metodyka zarządzania ryzykiem ma zapewnić porównywalne i powtarzalne rezultaty, poprzez zastosowanie standaryzacji skali oceny oraz sposobu przeprowadzania analizy, niezależnie kto będzie przeprowadzał analizę i ocenę ryzyka informacji w tym danych osobowych w organizacji.

5 Analizę ryzyka należy uruchamiać na etapie projektowania operacji przetwarzania, nawet jeśli niektóre operacje przetwarzania są wciąż nieznane. Takie działanie ma na celu dać odpowiedzi jak zaprojektować system i procesy przetwarzania, aby zminimalizować ryzyko naruszenia praw i wolności osób fizycznych, których dane są przetwarzane. Wymóg prawny takiego działania stanowi art. 25 RODO.

6 Zarządzanie ryzykiem w bezpieczeństwie informacji odbywa się zgodnie z modelem przedstawionym na Rysunku 1.



Rysunek 1: Model procesu zarządzania ryzykiem (za Polską Normą PN ISO/IEC 27005)

ROZDZIAŁ 4
Kontekst przetwarzania informacji w tym danych osobowych

I.1 ADO działa w ramach przepisu prawa w tym również RODO oraz KRI i dlatego maksymalne akceptowalne ryzyko szczątkowe nie może powodować wysokiego ryzyka naruszenia praw i wolności osób fizycznych, których dane osobowe są przetwarzane przez ADO a także narażenia informacji na utratę poufności, integralności i dostępności.

I.2 Analizę ryzyka realizuje zespół, w którym musi uczestniczyć co najmniej IOD i ASI.

I.3 Przed przystąpieniem do analizy ryzyka należy wykazać udokumentowaną inwentaryzację posiadanych aktywów wykorzystywanych do przetwarzania informacji.

I.4 W zakresie spełnienia wymogów RODO dane osobowe przed rozpoczęciem analizy ryzyka muszą mieć określone cechy:

a.a podstawę prawną przetwarzania danych;
a.b cel przetwarzania, tzn. potwierdzenia, że dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
a.c zakres przetwarzania danych oraz porównanie zakresu w stosunku do celów oraz podstawy prawnej;
a.d odbiorców i przetwarzających dane osobowe, czyli określenie osoby fizycznej lub prawnej, organu publicznego, jednostki lub innego podmiotu, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią a także ustalenie kategorii i zakresu przetwarzania danych przez poszczególnych lub grup odbiorców i przetwarzających;
a.e okres przechowywania danych osobowych, w tym planowanego terminu usunięcia;
a.f opis technicznych i organizacyjnych środków bezpieczeństwa.

I.5 Udokumentowaniem zapisów wymaganych pkt 4.4 może być rejestr czynności przetwarzania danych osobowych, o którym się mówi w art. 30 ust. 1 RODO.

I.6 Wszystkie aktywa informacyjne i materialne zawierające informacje, w tym dane osobowe podlegają:

a) **identyfikacji** – określeniu, gdzie znajduje się informacja, jaki jest jej zakres, jaką ma postać, kto z niej korzysta, w jakim trybie i na jakich zasadach,
b) **klasyfikacji** – określeniu wartości informacji z punktu widzenia prawa oraz jej znaczenia dla funkcjonowania.

I.7 Analizę ryzyka w organizacji przeprowadza się niezależnie od audytów i sprawdzeń bezpieczeństwa opisanych w Polityce bezpieczeństwa informacji w tym danych osobowych w dziale XIX.

I.8 Analizę ryzyka przeprowadza się dla istniejących informacji i zbiorów danych osobowych nie rzadziej niż co pięć lat na podstawie planu analizy ryzyka przygotowanego przez IOD, z uwzględnieniem pkt 10.3 Metodyki.

I.9 Analizę ryzyka przeprowadza się, niezależnie od pkt 4.8, każdorazowo przy kluczowych zmianach w sposobie przetwarzania informacji (np. wdrożenie nowych rozwiązań technicznych, zmiany lokalizacji przetwarzania informacji, istotnych zmianach przepisów prawnych, itp).

I.10 Zasoby informacji przetwarzane przez GOPS zawarte są w „Wykazie systemów informatycznych służących do przetwarzania informacji w tym danych osobowych" prowadzonym według wzoru znajdującego się w „Polityce bezpieczeństwa informacji w tym danych osobowych"

ROZDZIAŁ 5
Identyfikowanie aktywów i istniejących zabezpieczeń.

1 Wszystkie aktywa w Gminnym Ośrodku Pomocy Społecznej posiadają swoich właścicieli.

2 Przykład aktywów wykorzystywanych do operacji przetwarzania informacji stanowi załącznik nr 1.

3 Aktywa nie są stopniowane na etapie analizy ryzyka z powodu ich ważności, dopiero na etapie raportu z analizy ryzyka opracowujący dokument wskazuje priorytety ważności usuwania usterek, biorąc pod uwagę przede wszystkim wielkość zagrożenia oraz ważność aktywa.

4 Identyfikowanie aktywów musi się odbyć na odpowiednim poziomie szczegółowości, który zapewni wystarczające informacje na potrzeby szacowania ryzyka.

5 Za inwentaryzację zasobów informatycznych (tj. w kategoriach – sprzęt, oprogramowanie, sieć) odpowiada ASI.

6 Wdrożone przez ADO środki techniczne i organizacyjne mające zapewnić odpowiedni stopień bezpieczeństwa, zawarte są w Polityce bezpieczeństwa informacji w tym danych osobowych lub w rejestrze czynności przetwarzania danych osobowych.

ROZDZIAŁ 6
Identyfikowanie ryzyka

1 Dla zidentyfikowanych aktywów lub/i grup aktywów wykorzystywanych do operacji przetwarzania danych należy przypisać zagrożenia, które mogą oddziaływać na naruszenie praw i wolności osób fizycznych.

2 Przykładowy katalog zagrożeń zawiera załącznik nr 2 do Metodyki.

3 Podczas analizy ryzyka z załącznika nr 2 rozpatruje się te zagrożenia, które są możliwe do zaistnienia w kontekście konkretnego aktywu.

4 Podczas wykonywania szacowania ryzyka z wykorzystaniem załącznika nr 2 lub wyników wcześniejszych szacowań ryzyka należy uwzględniać ciągłe zmiany otoczenia wewnętrznego i zewnętrznego organizacji i aktualizować potencjalne zagrożenia.

5 W tworzeniu wykazu zagrożeń należy uwzględnić historię incydentów w organizacji oraz w organizacjach podobnych, informacje uzyskane z przeprowadzonych konsultacji z osobami z wewnątrz lub zewnątrz organizacji, które posiadają odpowiednią wiedzę, doświadczenie lub stykają się z ryzykiem w organizacji, np. prawnikami, informatykami, ekspertami ds. bezpieczeństwa, audytorami, właścicielami procesów i aktywów.

ROZDZIAŁ 7
Analiza i ocena skutków / następstw

I.1 Szacowanie następstw polega na rozważeniu jakie skutki dla zasobów informacyjnych lub systemów teleinformatycznych niesie ze sobą zmaterializowanie się zagrożeń z uwzględnieniem podatności zasobów lub systemów.

I.2 Następstwa mogą mieć charakter prawny (np. naruszenie art. 24, 32, 35, RODO lub art. 20 KRI) materialny (np. koszt odtworzenia danego zasobu lub przywrócenia jego sprawności) lub niematerialny (np. utrata wizerunku podmiotu w społeczeństwie).

I.3 W przypadku wystąpienia różnych skutków rozpatrywanych pod względem charakteru wskazanego w pkt 7.2 do analizy ryzyka przyjmuje się wartość najwyższą.

I.4 Należy wziąć pod uwagę, iż w określonych sytuacjach następstwo (skutek) może przekształcać się w samoistne zagrożenie, wywołując kolejne ryzyko.

I.5 Przy szacowaniu skutków należy uwzględnić zastosowane środki techniczne i organizacyjne mające na celu minimalizację negatywnych skutków dla bezpieczeństwa informacji.

I.6 Do celów metodyki przyjmuje się skalę od 1 do 5. Gdzie:

Wartość skutku	Opis skutku

5	Bardzo wysoki	Bardzo poważne szkody dla organizacji.
4	Wysoki	Poważne szkody dla organizacji.
3	Średni	Ważne zaburzenia funkcjonowania organizacji.
2	Niski	Małe zaburzenia funkcjonowania organizacji.
1	Nieistotny	Nieistotne dla celów praktycznych.

Tabela nr 1. Ocena punktowa skutków następstw.

I.7 Opis poszczególnych wartości zawarto w załączniku nr 3.

I.8 Biorąc pod uwagę, iż wszystkie informacje i aktywa są istotne z punktu zarządzania organizacją minimalna wartość skutków przyjmuje się na poziomie 1.

I.9 Wsparciem przy szacowaniu skutków są:

a historia dotychczasowych incydentów przetwarzania informacji w tym danych osobowych w organizacji lub w organizacjach podobnych;

b informacje uzyskane z przeprowadzonych konsultacji z osobami z wewnątrz lub zewnątrz organizacji, które posiadają odpowiednią wiedzę, doświadczenie lub stykają się z ryzykiem w organizacji, np. prawnikami, informatykami, ekspertami ds. bezpieczeństwa, audytorami, właścicielami procesów i aktywów;

c Załącznik nr 3 do Metodyki – „Opis oceny skutków".

ROZDZIAŁ 8
Analiza i ocena prawdopodobieństwa

I.1 Każde zagrożenie zidentyfikowane w ramach aktywa wykorzystywanych do operacji przetwarzania, przy uwzględnieniu zidentyfikowanych podatności i istniejących zabezpieczeń, należy ocenić w kontekście prawdopodobieństwa urzeczywistnienia się zagrożenia.

I.2 Szacowanie prawdopodobieństwa incydentu ma na celu ustalenie częstotliwości z jaką mogą pojawiać się określone incydenty.

I.3 Przy szacowaniu prawdopodobieństwa musimy brać pod uwagę:

a podatność aktywu;

b źródło potencjalnego zagrożenia;
c słabość lub luki aktywu;
d zabezpieczenia aktywu;
e w przypadku zagrożeń spowodowanych przez ludzi - atrakcyjność zasobu lub efektu skutku dla wywołującego incydent;
f dla zagrożeń o charakterze przypadkowym położenie geograficzne, warunki pogodowe itp., które mogą oddziaływać na powstawanie błędnych działań użytkowników zasobów informacyjnych lub systemów teleinformatycznych.

I.4 Wsparciem przy szacowaniu prawdopodobieństwa jest:

a doświadczenie szacującego;

b historia dotychczasowych incydentów przetwarzania informacji w tym danych osobowych w organizacji lub w organizacjach podobnych;

c informacje uzyskane z przeprowadzonych konsultacji z osobami z wewnątrz lub zewnątrz organizacji które posiadają odpowiednią wiedzę, doświadczenie lub stykają się z ryzykiem w organizacji, np. prawnikami, informatykami, ekspertami ds. bezpieczeństwa, audytorami, właścicielami procesów i aktywów;

d Załącznik nr 4 do Metodyki – „Przykłady podatności".

I.5 Do celów metodyki przyjmuje się skalę od 1 do 5. Gdzie:

Wartość prawdopodobieństwa		**Opis prawdopodobieństwa**
5	Bardzo wysokie	zdarzenie niemal pewne
4	Wysokie	zdarzenie wysoce prawdopodobne
3	Średnie	zdarzenie mało prawdopodobne
2	Niskie	zdarzenie prawie nieprawdopodobne
1	Zerowe	zdarzenie nieprawdopodobne (zagrożenie nie występuje)

Tabela nr 2. Ocena punktowa prawdopodobieństwa wystąpienia zagrożenia.

I.6 Biorąc pod uwagę, iż wszystkie informacje i aktywa są istotne z punktu zarządzania organizacją minimalną wartość prawdopodobieństwa wystąpienia zagrożenia przyjmuje się na poziomie 1.

ROZDZIAŁ 9
Określanie poziomu ryzyka

f.1 Określanie poziomu ryzyka polega na przypisaniu danemu zagrożeniu prawdopodobieństwa oddziaływania na zasoby informacyjne lub system teleinformatyczny oraz ustaleniu wpływu materializacji zagrożenia na:

a dostępność systemu lub informacji,

b integralność systemu lub informacji,

c poufność informacji przetwarzanej w systemie,

a następnie wyznaczeniu poziomu ryzyka.

f.2 Poziom ryzyka wyznacza się według następującego wzoru:

R=S*P

Gdzie :

R – poziom ryzyka

S - Ocena skutków naruszenia bezpieczeństwa

P - Ocena prawdopodobieństwa urzeczywistnienia się zagrożenia

f.3 W celu ułatwienia przeprowadzenia analizy ryzyka dane wprowadza się do szablonu będącego załącznikiem nr 5 do Metodyki.

f.4 Proponowane są cztery poziomy wielkości ryzyka dla obliczonych wartości liczbowych ryzyka:

a niski (1-6);

b średni (7-14);

c wysoki (15-19);

d maksymalny (20-25).

f.5 Na potrzeby metody oceny ryzyka naruszenia bezpieczeństwa informacji w tym danych osobowych przyjęto następujący rozkład ryzyka opisany w tabeli nr. 3.

Tabela nr 3. Macierz rozkładu oceny ryzyka naruszeniem bezpieczeństwa informacji w tym danych osobowych.

Ocena prawdopodobieństwa		Ocena skutków				
		1	2	3	4	5
	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

f.6 Otrzymane wyniki poziomu ryzyka naruszenia bezpieczeństwa informacji w tym danych osobowych należy przedstawić w postaci rankingu ryzyk, czyli od największego do najmniejszego i porównać z wyznaczonym poziomem akceptacji ryzyka (ryzyka szczątkowego), oddzielającym ryzyka akceptowane od nieakceptowanych.

f.7 Ryzyko szczątkowe – akceptowalne przyjęto na poziomach niskim i podwyższonym. Tabela nr 4.

Poziom	Wartość	Opis
niski	1-6	Ryzyko akceptowane, niewymagające dalszego postępowania.
podwyższony	7-14	Ryzyko podwyższone, akceptowane, wymagające monitoringu i ewentualnych działań zaradczych.
wysoki	15-19	Ryzyko wysokie, nieakceptowane, wymagające zastosowania postępowania z ryzykiem a także wymagające monitoringu ryzyka.
maksymalny	20-25	Ryzyka nieakceptowane, wymagające zastosowania postępowania z ryzykiem, stałego monitoringu i działania w pierwszej kolejności.

Tabela nr 4. Macierz rozkładu akceptacji ryzyka naruszeniem bezpieczeństwa informacji w tym danych osobowych.

ROZDZIAŁ 10
Postępowanie z ryzykiem

1 Celem postępowania z ryzykiem jest dokonanie wyboru wariantu postępowania z ryzykiem oraz zaplanowanie zabezpieczeń organizacyjnych i technicznych mających zapewnić ochronę informacji w tym danych osobowych i wykazać zgodność z RODO i KRI.

2 W ramach postępowania z ryzykiem należy dokonać wyboru wariantu postępowania z ryzykiem nieakceptowanym. Wyróżniamy następujące warianty:

a.a modyfikacja ryzyka - wdrożenie odpowiednich zabezpieczeń organizacyjnych i technicznych mających na celu minimalizację ryzyka do poziomu akceptowalnego oraz zapewnianie zgodności z RODO i KRI;

a.b unikanie ryzyka – rezygnacja z realizacji działań lub warunków, które powodują powstanie określonych ryzyk (W przypadku realizacji zadań publicznych unikanie ryzyka, co do zasady, nie ma zastosowania);

a.c przeniesienia ryzyka - przeniesienie ryzyka na inny podmiot, który może skutecznie zarządzać ryzykiem;

a.d akceptacja ryzyka - podjęcie przez Administratora danych decyzji o zachowaniu ryzyka szczątkowego bez podejmowania dalszych działań. W przypadku ryzyka wysokiego lub krytycznego decyzję Administrator danych może podjąć tylko w przypadku wydania pozytywnej opinii przez organ nadzorujący przetwarzanie danych osobowych.

3 Na podstawie analizy ryzyka tworzy się dokument „Sprawozdanie z analizy ryzyka”, który jest przedstawiany ADO.

4 Na podstawie „Sprawozdania z analizy ryzyka” przygotowywany jest „Harmonogram działań obniżających poziom ryzyka”.

ROZDZIAŁ 11
Monitorowanie i przegląd czynników ryzyka oraz ryzyka.

1 Ryzyko nie jest statyczne i elementy wpływające na poziom ryzyka (podatności, prawdopodobieństwo, następstwa) mogą się zmieniać w sposób nagły, bez żadnej oznaki.

2 Monitorowanie i przegląd mechanizmów ochrony informacji powinien być realizowany na każdym etapie procesu zarządzania informacją, tj.:

a wdrożenia nowych aktywów;

b konieczności modyfikacji wartości aktywów;

c weryfikacji, czy kontekst przetwarzania danych nie uległ zmianie lub planowane są jego modyfikacje, co może powodować realizację nowych operacji przetwarzania danych;

d weryfikacji, czy operacje przetwarzania, wyłączone z przeprowadzenia oceny skutków, aktualnie nie powodują wysokiego ryzyka naruszenia praw i wolności osób fizycznych;

e weryfikacji, czy organ nadzorczy ustanowił nowy lub zaktualizował wykaz rodzajów operacji przetwarzania podlegających i niepodlegających wymogowi dokonania oceny skutków dla ochrony danych;

f weryfikacji, czy zidentyfikowane ryzyka naruszenia praw i wolności osób fizycznych są wciąż adekwatne;

g pojawienia się nowych zagrożeń;

h incydentów związanych z bezpieczeństwem informacji, itp.

3 Proces monitorowania jest realizowany na bieżąco, natomiast przegląd punktów wskazanych w pkt 11.2 powinien być przeprowadzony co najmniej raz w roku lub częściej w przypadku modyfikacji lub planowania modyfikacji kontekstu czynników ryzyka przetwarzania informacji.

ROZDZIAŁ 12
Postanowienia końcowe

1 Niniejsza Metodyka jest zgodna z przepisami o ochronie danych osobowych.

2 Niniejsza Metodyka powinna być aktualizowana wraz ze zmieniającymi się przepisami w obszarach bezpieczeństwa informacji w tym danych osobowych oraz zmianami faktycznymi w ramach Administratora Danych Osobowych, które mogą powodować, że zasady ochrony informacji określone w obowiązującym dokumencie będą nieaktualne lub nieadekwatne.

3 Zmiany niniejszej metodyki wymagają przeglądu innych dokumentów dotyczących ochrony informacji w tym danych osobowych obowiązujących u Administratora Danych Osobowych.

4 Niniejszą metodykę wprowadza się w życie w formie zarządzenia ADO.

5 Wszelkie zmiany w niniejszej metodyce nie wymagają zarządzenia ADO.

6 W przypadku edycji metodyki, wszystkie zmiany są odpowiednio oznaczone i opisane w „historii zmian". Nowe edycje dokumentu mają nadany kolejny numer i datę opracowania oraz są udostępniane Kierownikom referatów, którzy są odpowiedzialni do zapoznania swoich pracowników

ROZDZIAŁ 13
Historia zmian

Nr wersji	Data	Autor	Opis zmian

Załącznik nr 1 – Przykłady aktywów

Grupy aktywów	Aktywa szczegółowe	Przykłady
Informacje	Dane osobowe	
	Informacje o dużej wartości	Hasła administratorów, kluczowe umowy, specyfikacje przetargowe przed ogłoszeniem
	Informacje publiczne	Informacje w BIP oraz na stronie internetowej
	Informacje niejawne	Informacje zbierane
Sprzęt	Urządzenia przetwarzania danych	Serwery, systemy backupu, macierze
	Urządzenia stacjonarne	Stacje robocze, terminale
	Urządzenia przenośne	Laptopy, PDA
	Urządzenia peryferyjne	Drukarki, skanery, kserokopiarki, wymienny napęd dyskowy
	Nośnik danych	Pendrive, CD-ROM, w tym nośniki do kopii bezpieczeństwa, dyski zewnętrzne
	Inne nośniki informacji	Wydruki, faxy, dokumentacja
Sieć	Media i usługi wspierające	Ethernet, PSTN (Publiczna Komutowana Sieć Telefoniczna)
	Przekaźniki aktywne i pasywne	Przełączniki, most, router, hub, automatyczna centrala
	Interfejs komunikacyjny	Modemy , adaptery Ethernet
Oprogramowanie	Systemy operacyjne	Windows, Unix, Linux,
	Pakiety oprogramowania lub oprogramowanie standardowe	Oprogramowane do zarządzania bazą danych, poczta elektroniczna, pakiety biurowe
	Oprogramowane do obsługi, pielęgnacji lub zarządzania	Programy służące do monitorowania systemów, zarządzania siecią
	Standardowa aplikacja biznesowa	Program księgowy, płacowy, oprogramowanie służące do zarządzania kompetencjami personelu, CRM
	Dedykowane aplikacje biznesowe	Oprogramowanie dedykowane specjalnie dla ADO
Personel	Użytkownicy	Personel z ograniczonym dostępem i uprawnieniami w zakresie przetwarzania informacji
	Decydenci	Właściciele aktywów np. ścisłe kierownictwo, kierow-

Grupy aktywów	Aktywa szczegółowe	Przykłady
		nik projektu itp.
	Decydenci	Właściciele aktywów np. ścisłe kierownictwo, kierownik projektu itp.
	Administratorzy	Personel z pełnymi dostępami do informacji
Organizacja	Struktura organizacji	Zarządzanie personelem, zarządzanie informatyką
	Organizacja projektu	Wdrażanie nowych rozwiązań, projekty migracji
	Podmiot przetwarzający	Podmiot zewnętrzny, któremu powierza się przetwarzanie informacji
	Dostawca	Podmiot zewnętrzny, który zapewnia usługi i zasoby
Siedziba	Lokalizacja	
	Strefa	Część pomieszczeń w siedzibie. Np. strefa bezpieczeństwa, strefy przetwarzania danych osobowych
	Usługi	Wszystkie usługi niezbędne do działania urządzeń organizacji np. łączność, usługi komunalne i techniczne
Sprzęt pomocniczy	Zasilanie	Agregat, ups
	Klimatyzator	
	Sprzęt do niszczenia	Demagnetyzer, niszczarka
	Meble	Szafy drewniane, szafy pancerne, regały

Załącznik nr 2 – Przykłady typowych zagrożeń

Poniżej przedstawiono przykłady zagrożeń jednak podkreśla się, iż podane zagrożenia są tylko przykładami mogącymi być wsparciem przy realizacji analizy ryzyka lecz nie jest to lista zamknięta.

Nazwa zagrożenia	Opis
Zjawiska naturalne	Wydarzenia, które mogą wystąpić bez bezpośredniego lub pośredniego uczestnictwa ludzi.
Ogień	Pożary: możliwość pożaru niszczy aktywa.
Powódź	Powodzie: możliwość, że woda niszczy aktywa.
Zjawiska pogodowe	Ekstremalnie niskie lub wysokie temperatury, wysokie opady atmosferyczne, silne wiatry…
Pozostałe klęski żywiołowe	Inne zdarzenia, które występują bez udziału człowieka: błyskawice, burze elektryczne, trzęsienia ziemi, cyklony, lawina, osunięcie ziemi itp.
Zniszczenia, uszkodzenie mechaniczne lub awaria	Zdarzenia, które mogą się przypadkowo pojawić w wyniku działalności człowieka typu przemysłowego. Te zagrożenia może być przypadkowe lub celowe.
Pożar	Ogień: możliwość, że ogień zniszczy aktywy.
Szkody spowodowane przez wodę	zalania, wycieki, powodzie: możliwość, że woda niszczy aktywa.
Zanieczyszczenie mechaniczne	Wibracje, kurz, brud itd.
Zanieczyszczenia elektromagnetyczne	Zakłócenia radiowe, pola magnetyczne, światło ultrafioletowe itp.
Awaria sprzętu lub oprogramowania	Błędy w sprzęcie i / lub programach. Może to być spowodowane wadą produkcyjną lub może powstać podczas działania systemu.
Przerwanie zasilania	Awaria zasilania elektrycznego.
Nieodpowiednie warunki temperatury i / lub wilgotności	Niedociągnięcia w klimatyzacji pomieszczeń, które przekraczają ograniczenia robocze dla sprzętu: nadmiar ciepła, nadmiar wilgotności itp.
Awaria usług telekomunikacyjnych	Ograniczenie możliwości przesyłania danych z jednego miejsca do drugiego.
Przerwanie innych usług i niezbędnych dostaw	Inne usługi lub zasoby, od których zależy działanie urządzenia, na przykład papier do drukarki, toner itp.
Degradacja zasobów	W wyniku upływu czasu.

Nazwa zagrożenia	Opis
Promieniowanie elektromagnetyczne	Fakt udostępniania danych wewnętrznych stronom trzecim drogą radiową. Niemal wszystkie urządzenia elektryczne emitują promieniowanie na zewnątrz, które może zostać przechwycone przez inny sprzęt (odbiorniki radiowe) powodujące wyciek informacji.
Przeciążenie systemu informacyjnego	
Niewłaściwe funkcjonowanie systemu informatycznego	
Błędy i niezamierzone awarie	Niezamierzone awarie spowodowane przez osoby.
Błędy użytkowników	Błędy popełniane przez osoby korzystające z usług, danych itp.
Błędy administratora	Błędy popełniane przez osoby odpowiedzialne za instalację i obsługę.
Błędy monitorowania (rejestrowania)	Niewłaściwe zapisy dotyczące działalności: niepoprawne zapisy, niekompletne zapisy, niepoprawnie datowane zapisy, niepoprawnie przypisane rekordy itp.
Błędy konfiguracji	Wprowadzenie błędnych danych konfiguracyjnych. Prawie wszystkie zasoby zależą od konfiguracji i zależy to od staranności administratora: uprawnienia dostępu, przepływy aktywności, rekordy działań, routing itp.
Braki organizacyjne	Brak lub niedokładny rozdział obowiązków i odpowiedzialności. Nieskoordynowane działania, błędy przez zaniechanie itp.
Rozpowszechnianie złośliwego oprogramowania	Rozprzestrzenianie się wirusów, spyware, robaków, trojanów, bomb logicznych, itp.
Błędy routingu	Przesyłanie informacji w sposób przypadkowy przez system lub sieć. Mogą to być wiadomości między osobami, pomiędzy procesami lub między nimi.
Błędy sekwencji	Przypadkowa zmiana kolejności wysyłanych wiadomości.
Wycieki informacyjne	Informacje przypadkowo docierają do osób, które nie powinny o tym wiedzieć.
Zmiana informacji	Przypadkowa zmiana informacji.
Wprowadzanie nieprawidłowych informacji	Przypadkowe wprowadzenie nieprawidłowych informacji.
Degradacja informacji	Przypadkowa degradacja informacji.
Zniszczenie informacji	Przypadkowa utrata informacji.
Ujawnianie informacji	Ujawnienie ze względu na niedyskrecję. Niedyskrecja słowna, media elek-

Nazwa zagrożenia	Opis
	troniczne, kopie itp.
Luki w oprogramowaniu	Wady kodu, które powodują wadliwe działanie bez zamiaru ze strony użytkownika ale z konsekwencjami dla integralności danych lub ich zdolności do działania.
Usterki w utrzymaniu / aktualizacji oprogramowania	Wady procedur lub kontroli w celu aktualizacji kodu, który pozwala aby programy ze znanymi wadami które zostały naprawione przez producenta w dalszym ciągu były stosowane.
Usterki w konserwacji / aktualizacji sprzętu	Usterki w procedurach lub kontroli dotyczące aktualizacji sprzętu, które pozwalają na jego dalszą eksploatację po normalny czasie użytkowania.
Awaria systemu z powodu wyczerpania zasobów	Brak wystarczających zasobów powoduje awarię systemu, gdyż obciążenie jest zbyt duże.
Niedobór personelu	Przypadkowa nieobecność na stanowisku pracy: choroba, sytuacje losowe itp.
Rozmyślne ataki	Umyślne awarie spowodowane przez osoby.
Manipulacja konfiguracją	Prawie wszystkie aktywa zależą od konfiguracji, a to z kolei zależy od staranności administratora: uprawnienia dostępu, przepływu aktywności, rejestr aktywności, routing itp.
Maskowanie tożsamości użytkownika	Gdy atakującym udaje się pojawiać jako upoważnieni użytkownicy, korzystają z przywilejów użytkowników dla swoich własnych celów. Zagrożenie to może być popełniane przez personel wewnętrzny, osoby spoza organizacji lub przez osoby tymczasowo zatrudnione.
Nadużycie uprawnień dostępu	Każdy użytkownik ma pewien poziom uprawnień do określonego celu. Gdy użytkownicy nadużywają swojego przywileju do wykonywania zadań, za które nie są odpowiedzialni, może pojawić się zagrożenie aktywów.
Niewłaściwe użycie aktywów	Wykorzystanie zasobów systemowych do nieplanowanych celów, zazwyczaj z osobistych pobudek: gry, prywatne wyszukiwania w Internecie, osobiste bazy danych, programy osobiste, itp.
Rozpowszechnianie złośliwego oprogramowania	Celowe rozprzestrzenianie wirusów, spyware, robaków, trojanów, bomb logicznych itp.
Zmiana trasy wiadomości	Przesyłanie informacji do niewłaściwego miejsca docelowego za pośrednictwem systemu lub sieci. Mogą to być wiadomości między osobami, między procesami lub między nimi. Osoba atakująca może zmusić wiadomość do przejścia przez określony węzeł w sieci, gdzie może zostać przechwycona.
Zmiana sekwencji	Zmiana kolejności wysyłanych wiadomości. Chodzi o to, że nowe zamówienie zmienia znaczenie grupy wiadomości, naruszając integralność dotkniętych danych.

Nazwa zagrożenia	Opis
Nieautoryzowany dostęp	Osoba atakująca może uzyskać dostęp do zasobów systemu bez upoważnienia, zazwyczaj korzystające z awarii w systemie identyfikacji i autoryzacji.
Analiza ruchu	Bez potrzeby analizowania zawartości komunikacji atakujący może wyciągać wnioski w oparciu o analizę pochodzenia, przeznaczenia, ilości i częstotliwości wymian. Jest to czasami nazywane "monitorowaniem ruchu".
Odrzucenie	Późniejsze odrzucenie działań lub przedsięwzięć nabytych w przeszłości. Odrzucenie nadawcy: odmowa bycia nadawcą lub źródłem wiadomości lub komunikacji. Odrzucenie odbioru: odmowa odebrania wiadomości lub komunikacji. Odrzucenie dostawy: odmowa odebrania wiadomości do innych osób.
Podsłuch	Napastnicy mają dostęp do informacji, które nie należą do nich, bez zmiany samych informacji.
Zmiana informacji	Zamierzona zmiana informacji w celu uzyskania korzyści lub spowodowania szkody.
Wprowadzanie fałszywych informacji	Celowe wprowadzanie fałszywych informacji w celu uzyskania korzyści lub uszkodzenia.
Uszkodzenie informacji	Celowa degradacja informacji, aby uzyskać korzyść lub spowodować uszkodzenie.
Niszczenie informacji	Celowe usunięcie informacji, aby uzyskać korzyści lub spowodować szkody.
Ujawnianie informacji	Ujawnienie informacji.
Manipulowanie programami	Zamierzona zmiana działania programu w celu uzyskania korzyści pośredniej, przez upoważnioną osobę do używania tego programu.
Odmowa usługi	Brak wystarczających zasobów powoduje awarię systemu, gdy obciążenie jest zbyt wysokie.
Kradzież	Kradzieży sprzętu bezpośrednio powoduje brak zasobów do świadczenia usług, czyli niedostępność. (dotyczy też kradzieży informacji) Kradzież może zostać przeprowadzona przez personel wewnętrzny, osoby spoza organizacji lub osoby tymczasowo zakontraktowane, co zapewnia różny stopień łatwości dostępu do skradzionego obiektu i różne konsekwencje. W przypadku urządzeń udostępniających dane może również wystąpić wyciek informacji.
Atak niszczycielski	Wandalizm, terroryzm, działania wojskowe itp. Zagrożenie to może być wykonywane przez personel wewnętrzny, osoby spoza organizacji lub przez osoby tymczasowo zatrudnione.
Niedobór personelu	Umyślna nieobecność w pracy: takie jak strajki, absencja w pracy, nieuzasadnione nieobecności, blokowanie dostępu itp.
Wymuszenia	Nacisk i groźby w celu zobowiązania do działania w określony sposób.

Nazwa zagrożenia	Opis
Socjotechniki	Korzystanie z dobrej woli niektórych osób, aby umożliwić prowadzenie działań będących przedmiotem zainteresowania na rzecz strony trzeciej.
Nieautoryzowane działanie	
Nieautoryzowane użycie urządzeń	
Nieuprawnione kopiowanie oprogramowania	
Użycie fałszywego lub skopiowanego oprogramowania	
Zniekształcenie danych	

Opracowanie własne na podstawie MAGERIT – version 2 oraz PN-ISO/IEC 27005

Załącznik nr 3 – Opis oceny skutków

Wartość	Ocena skutków - opis
5	– Obowiązki prawne i regulacyjne: może doprowadzić do wyjątkowo poważnego naruszenia przepisu prawnego lub regulacyjnego; – Dane osobowe: może doprowadzić do wyjątkowo poważnego uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych; – Administracja i zarządzanie: może poważnie utrudnić efektywne działanie całej organizacji; – Prawdopodobnie doprowadzi do powszechnego, niepożądanego rozgłosu, który szczególnie niekorzystnie wpłynie na relacje z opinią publiczną oraz z innymi organizacjami; – Może powodować poważne szkody w skuteczności operacyjnej lub bezpieczeństwie sieci teleinformatycznej. – Skutki finasowe – bardzo wysokie.
4	– Obowiązki prawne i regulacyjne: może doprowadzić do poważnego naruszenia przepisu prawnego lub regulacyjnego (np. narusza prawa lub wolosc osoby fizycznej); – Dane osobowe: może doprowadzić do poważnego naruszenia uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych; – Administracja i zarządzanie: może utrudnić sprawne działanie całości organizacja; – Prawdopodobnie spowoduje poważne zakłócenia w działaniach w organizacji; – Prawdopodobnie doprowadzi do powszechnego niepożądanego rozgłosu, który poważnie niekorzystnie wpłynie na relacje z opinią publiczną oraz z innymi organizacjami; – stanowią poważne naruszenie zobowiązań umownych w zakresie utrzymania bezpieczeństwa informacji dostarczanych przez strony trzecie; – Skutki finasowe – wysokie.
3	– Obowiązki prawne i regulacyjne: może doprowadzić do naruszenia przepisu prawnego lub regulacyjnego (np. narusza prawa lub wolosc osoby fizycznej); – Dane osobowe: doprowadzić do naruszenia uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych; – Administracja i zarządzanie: prawdopodobnie doprowadzi do nieefektywnego działania więcej niż jedną część organizacji; – Prawdopodobnie spowoduje ograniczony niepożądany rozgłos, który negatywnie wpłynie na relacje z opinią publiczną oraz z innymi organizacjami; – Skutki finasowe – średnie.
2	– Obowiązki prawne i regulacyjne: może doprowadzić do do drobnego / technicznego naruszeń

	nia przepisu prawnego lub regulacyjnego; – Dane osobowe: mogą doprowadzić do do drobnego / technicznego naruszenia bezpieczeństwa danych osobowych bez powodowania uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych; – Administracja i zarządzanie: może doprowadzić do nieefektywnego działania jedną część organizacji (o znaczeniu ograniczonym); – Może spowodować minimalny niepożądany rozgłos, który może negatywnie wpłynąć na relacje z opinią publiczną oraz z innymi organizacjami; – Skutki finasowe – niskie.
1	– Obowiązki prawne i regulacyjne: nie może doprowadzić do nawet do najmnijeszego naruszenia przepisu prawnego lub regulacyjnego; – Dane osobowe: nie ma wpływu na możliwość wystąpienia naruszenia praw lub wolności osoby fizycznej; – Administracja i zarządzanie: nie ma wpływu na działanie organizacji; – Nie ma wpływu na rozgłos, który może wpłynąć na relacje z opinią publiczną oraz z innymi organizacjami; – Skutki finasowe – brak.

Załacznik nr 4 – Przykłady podatności

Poniżej przedstawiono przykłady podatności w różnych obszarach bezpieczeństwa, które mogą być wykorzystane do urzeczywistniania się zagrożenia w kontekście danego aktywa lub grupy aktywów. Podkreśla się, iż podane podatności są tylko przykładami mogącymi być wsparciem przy realizacji analizy ryzyka lecz nie jest to lista zamknięta.

Grupy aktywów	Przykłady
Informacje	Brak kopii bezpieczeństwa
	Brak umów powierzenia informacji
	Brak ograniczenia dostępu do informacji
	Brak przypisanych właścicieli informacji
	Brak określonej polityki obiegu dokumentów
	Brak klasyfikacji informacji
	Transfer danych osobowych poza siedzibę ADO w formie jawnej (nie zabezpieczonej)
Sprzęt	Brak skutecznej kontroli konfiguracji
	Brak rezerwy kluczowych elementów
	Niezabezpieczone urządzenia do przechowywania danych
	Brak przeglądów i konserwacji
	Brak staranności przy niszczeniu sprzętu
	Brak planów okresowej wymiany
	Niekontrolowane kopiowanie
	Wrażliwość na zmiany wilgoci, temperatury, pył, zanieczyszczenie itp.
Sieć	Brak alternatywnych dróg połączenia
	Nieodpowiednie zarządzanie siecią
	Niezabezpieczone okablowanie strukturalne
	Brak zabezpieczenia na styku z siecią publiczną
	Brak stałego nadzoru nad ruchem sieciowym
	Złe łączenie kabli
	Brak dokumentacji dotyczącej sieci

Grupy aktywów	Przykłady
	Pozostawianie dostępów zdalnych do sieci (niebezpieczna konfiguracja sieci)
	Nieodpowiednie zarządzanie siecią (elastyczny routing)
Oprogramowanie	Brak aktualizacji oprogramowania (usługi sieciowe i systemy operacyjne)
	Brak kontroli pobieranego oprogramowania
	Akceptacja znanych wad oprogramowania
	Brak lub niewystarczające procedury testowania oprogramowania
	Brak mechanizmów identyfikacji i uwierzytelniania
	Brak mechanizmów monitorowania aktywności użytkowników (logowania zdarzeń)
	Brak sformułowanych wymagań bezpieczeństwa dla tworzonych aplikacji
	Niedostateczne zarządzanie hasłami (hasła łatwe do odgadnięcia)
	Niezabezpieczone tablice haseł
	Nieprawidłowe ustawienie parametrów
	Brak kopii oprogramowania
	Uruchomione zbędne usługi
	Niedojrzałe lub nowe oprogramowanie
	Brak skutecznej kontroli zmian
	Brak ewidencji historii zmian
Personel	Nieobecność personelu
	Brak wymagań bezpieczeństwa na stanowiskach pracy
	Brak szkoleń
	Nieodpowiednie procedury rekrutacyjne
	Brak procedur rozwiązywania stosunku pracy
	Nieodpowiednie użycie oprogramowania lub sprzętu
	Podatność na socjotechniki
	Praca personelu zewnętrznego lub sprzątającego bez nadzoru (w tym działań popołudniowych)
	Brak stosowania „polityki czystego biurka i ekranu”
Organizacja	Brak wyznaczonych osób odpowiedzialnych za systemy, procesy i zasoby
	Wdrażanie nowych rozwiązań, projekty migracji
	Podmiot zewnętrzny któremu powierza się przetwarzanie informacji
	Podmiot zewnętrzny który zapewnia usługi i zasoby

Grupy aktywów	Przykłady
Siedziba	Brak fizycznej ochrony budynków, okien, drzwi
	Lokalizacja na terenie zagrożonym powodzią
	Stan techniczny budynku
	Stan techniczny instalacji grzewczych, wod-kan, elektrycznej, gazowej
	Usytuowanie budynku
	Brak zabezpieczenia pomieszczeń odpowiednimi drzwiami o odpowiedniej klasie
	Brak odpowiedniego zapewnienia warunków bezpieczeństwa i środowiskowych dla pomieszczeń specjalnych (archiwum, serwerownia)
Sprzęt pomocniczy	Brak testowania urządzeń zasilających
	Brak gwarantowanego zasilania
	Brak systemów sygnalizacji napadu i włamania
	Brak niszczarek
	Brak odpowiedniej ilości szaf do zabezpieczenia informacji

Załącznik nr 5 - Arkusz oceny ryzyka

Zagrożenia	zasoby		
	wskaźniki oceny		
	skutki	prawdopodo-bieństwo	ryzyko
Zjawiska naturalne			**0**
Ogień			**0**
Powódź			**0**
Zjawiska pogodowe			**0**
Pozostałe klęski żywiołowe			**0**
Zniszczenia, uszkodzenie mechaniczne lub awaria			**0**
Pożar			**0**
Szkody spowodowane przez wodę			**0**
Zanieczyszczenie mechaniczne			**0**
Zanieczyszczenia elektromagnetyczne			**0**
Awaria sprzętu lub oprogramowania			**0**
Przerwanie zasilania			**0**
Nieodpowiednie warunki temperatury i / lub wilgotności			**0**
Awaria usług telekomunikacyjnych			**0**
Przerwanie innych usług i niezbędnych dostaw			**0**
Degradacja zasobów			**0**
Promieniowanie elektromagnetyczne			**0**
			0
Przeciążenie systemu informacyjnego			**0**
Niewłaściwe funkcjonowanie systemu informatycznego			**0**
Błędy i niezamierzone awarie			**0**
Błędy użytkowników			**0**

Zagrożenia	zasoby		
	wskaźniki oceny		
	skutki	prawdopodo-bieństwo	ryzyko
Błędy administratora			**0**
Błędy monitorowania (rejestrowania)			**0**
Błędy konfiguracji			**0**
Braki organizacyjne			**0**
Rozpowszechnianie złośliwego oprogramowania			**0**
Błędy routingu			**0**
Błędy sekwencji			**0**
Wycieki informacyjne			**0**
Zmiana informacji			**0**
Wprowadzanie nieprawidłowych informacji			**0**
Degradacja informacji			**0**
Zniszczenie informacji			**0**
Ujawnianie informacji			**0**
Luki w oprogramowaniu			**0**
Usterki w utrzymaniu / aktualizacji oprogramowania			**0**
Usterki w konserwacji / aktualizacji sprzętu			**0**
Awaria systemu z powodu wyczerpania zasobów			**0**
Niedobór personelu			**0**
Rozmyślne ataki			**0**
Manipulacja konfiguracją			**0**
Maskowanie tożsamości użytkownika			**0**
Nadużycie uprawnień dostępu			**0**
Niewłaściwe użycie aktywów			**0**
Rozpowszechnianie złośliwego oprogramowania			**0**

	zasoby		
Zagrożenia	wskaźniki oceny		
	skutki	prawdopodo-bieństwo	ryzyko
Zmiana trasy wiadomości			**0**
Zmiana sekwencji			**0**
Nieautoryzowany dostęp			**0**
Analiza ruchu			**0**
Odrzucenie			**0**
Podsłuch			**0**
Zmiana informacji			**0**
Wprowadzanie fałszywych informacji			**0**
Uszkodzenie informacji			**0**
Niszczenie informacji			**0**
Ujawnianie informacji			**0**
Manipulowanie programami			**0**
Odmowa usługi			**0**
Kradzież			**0**
Atak niszczycielski			**0**
Niedobór personelu			**0**
Wymuszenia			**0**
Socjotechniki			**0**

Nieautoryzowane działanie			**0**
Nieautoryzowane użycie urządzeń			**0**
Nieuprawnione kopiowanie oprogramowania			**0**
Użycie fałszywego lub skopiowanego oprogramowania			**0**
Zniekształcenie danych			**0**

maksymal. 20-25
wysokie 15 - 29
podwyższone 7-14
niskie 1-6