STAROSTA NIDZICKI
13-100 Nidzica
ul. Traugutta 23

Zarządzenie Nr Z/ 21/2019
Starosty Nidzickiego
z dnia 30 sierpnia 2019 r.

w sprawie wprowadzenia Dokumentacji systemu zarządzania bezpieczeństwem informacji (Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych) w Starostwie Powiatowym w Nidzicy.

Na podstawie art. 34 ust. 1 i art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz. U. z 2019 r. poz. 511) oraz art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – Dz. Urz. UE z 2016 r., Nr 119, str. 1) zarządzam co następuje:

§ 1

Ustala się dokumentację systemu zarządzania bezpieczeństwem informacji w Starostwie Powiatowym w Nidzicy, stanowiącą załącznik do zarządzenia.

§ 2

Dokumentacja ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe.

§ 3

Zobowiązuje się pracowników Starostwa Powiatowego w Nidzicy do zapoznania się i stosowania zasad określonych w dokumentacji systemu zarządzania bezpieczeństwem informacji w Starostwie Powiatowym w Nidzicy.

§ 4

Traci moc Zarządzenie Nr Z/ 29/2018 Starosty Nidzickiego z dnia 13 sierpnia 2018 r. w sprawie wprowadzenia Dokumentacji systemu zarządzania bezpieczeństwem informacji w Starostwie Powiatowym w Nidzicy.

§ 5

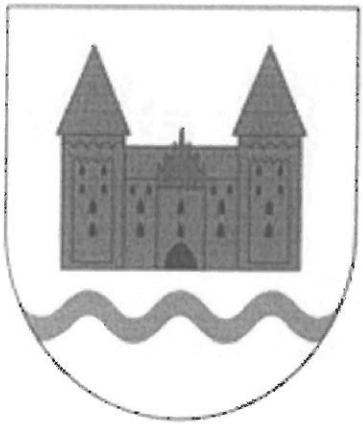
Wykonanie zarządzenia powierza się Kierownikom Wydziałów i samodzielnym stanowiskom.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Marcin Paliński

Polityka bezpieczeństwa informacji



Starostwa Powiatowego
w Nidzicy

Wprowadzenie Polityki Bezpieczeństwa Informacji, zwanej dalej Polityką, ma na celu ustanowienie kierunku zarządzania bezpieczeństwem informacji. Polityka stanowi nadrzędny dokument Systemu Zarządzania Bezpieczeństwem Informacji. Wynikające z niej zasady pozwalają na rozwój działalności poprzez zapewnienie klientów oraz kontrahentów o wysokim standardzie zadań realizowanych przez Starostwo Powiatowe w Nidzicy, zwane dalej Starostwem.

1. Zakres dokumentu

Polityka wraz z dokumentacją powiązaną oraz wypełnianie ich postanowień obowiązuje wszystkie osoby uczestniczące w procesie przetwarzania informacji w Starostwie. Poszczególne regulacje podległe polityce mogą obejmować również podmioty współpracujące, przetwarzające informacje.

2. Deklaracja najwyższego kierownictwa

Zarząd Powiatu niniejszym dokumentem deklaruje świadomość potrzeby ochrony informacji oraz wskazuje zabezpieczenia, mechanizmy i procesy to umożliwiające. Zarządzanie bezpieczeństwem informacji jest procesem podlegającym ciągłym zmianom, dlatego Zarząd Powiatu rozpoznaje ciągłe doskonalenie jako istotny element systemu.

3. Podstawa prawna

3.1. System Zarządzania Bezpieczeństwem Informacji (SZBI) uwzględnia regulacje prawne, którym podlega Starostwo, w szczególności:

a) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

b) 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.

c) 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.

4. Definicje

4.1. Przez użyte w treści Polityki i dokumentacji powiązanej sformułowania należy rozumieć:

a) **Administrator Danych Osobowych (ADO)** – Starosta Nidzicki, decyduje o celach i środkach przetwarzania danych osobowych. Organem realizującym obowiązki ADO jest najwyższe kierownictwo, tj. Zarząd Powiatu.

b) **Administrator Systemu Informatycznego (ASI)** – osoba lub osoby funkcyjne wyznaczane przez Administratora Danych Osobowych odpowiedzialne za przestrzeganie i nadzór nad przestrzeganiem zasad bezpieczeństwa informacji w systemie informatycznym w zakresie przypisanych im obowiązków i uprawnień. Różne systemy mogą posiadać różnych ASI.

c) **Bezpieczeństwo informacji** – oznacza zapewnienie poufności, integralności oraz dostępności informacji.

d) **Dane „wrażliwe"** – dane osobowe objęte szczególną ochroną, wskazane w art. 9 i 10 RODO. Takimi danymi są m.in. dane o stanie zdrowia, dane daktyloskopijne, dane o wyrokach, itp.

e) **Dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, przy czym możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

f) **Dostępność** – oznacza zapewnienie, że informacja jest dostępna zawsze wtedy, kiedy zachodzi taka potrzeba przez podmiot uprawniony.

g) **Incydent** – (Incydent związany z bezpieczeństwem informacji) oznacza pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń,

które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

h) **Inspektor Ochrony Danych (IOD)** - osoba fizyczna wyznaczana przez Administratora Danych Osobowych monitorująca przestrzeganie przepisów o ochronie danych osobowych, zgodnie z przydzielonym zakresem obowiązków.

i) **Integralność** – oznacza właściwość zapewniającą, że informacja nie została zmieniona lub zniszczona w sposób nieautoryzowany.

j) **KKO** – kierownik komórki organizacyjnej

k) **Naruszenie ochrony danych osobowych** – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

l) **Osoby upoważnione** - wszystkie osoby mające upoważnienie do przetwarzania danych osobowych, z racji wykonywanych obowiązków służbowych oraz nadanego upoważnienia lub upoważnione do przetwarzania na podstawie przepisów prawa i umów powierzenia. Osoby upoważnione są osobami uprawnionymi.

m) **Osoby uprawnione** - wszystkie osoby uprawnione do przetwarzania informacji, z racji wykonywanych obowiązków służbowych lub uprawnione do przetwarzania na podstawie przepisów prawa lub zawartych umów.

n) **Poufność** – oznacza właściwość zapewniającą, że informacje nie są udostępniane osobom trzecim.

o) **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na informacjach w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

p) **Przetwarzanie danych** - operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym.

q) **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.

r) **Struktura informatyczna** - zespół środków technicznych i ich zabezpieczeń, tj. urządzeń (komputerów, urządzeń drukujących, łączności, wraz z okablowaniem i oprogramowaniem) oraz oprogramowania (systemów operacyjnych, oprogramowania urządzeń), a także sieć informatyczna i udostępniane przez nią zasoby.

s) **System informatyczny** – oznacza oprogramowanie lub grupę programów służących do przetwarzania danych w obrębie wspólnej bazy danych, w szczególności posiadające wspólne uwierzytelnianie użytkowników.

t) **System Zarządzania Bezpieczeństwem Informacji (SZBI)** – oznacza zbiór wszystkich zasad, procedur i procesów realizowanych w celu zapewniania bezpieczeństwa informacji.

u) **Ustawa** - Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

v) **Usuwanie danych** - zniszczenie danych osobowych lub taka ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

w) **Użytkownik** – osoba, której zostały przydzielone uprawnienia w systemie informatycznym.

x) **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie.

y) **Zdarzenie** – (Zdarzenie związane z bezpieczeństwem informacji) oznacza stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji.

5. Ogólne zasady bezpieczeństwa informacji

5.1. Podstawą Systemu Zarządzania Bezpieczeństwem Informacji oraz stosowanych zabezpieczeń są wymagania prawne, wyniki przeprowadzanego szacowania ryzyka utraty bezpieczeństwa informacji oraz wyniki monitorowania realizowanego przez IOD i audytów zewnętrznych lub wewnętrznych oraz przeglądy zarządcze.

5.2. Bezpieczeństwo informacji jest realizowane poprzez stosowanie zabezpieczeń organizacyjnych, technicznych, fizycznych oraz środowiskowych.

5.3. Przez informacje objęte ochroną opisaną w dokumentacji SZBI należy rozumieć dane osobowe, w rozumieniu artykułu 4 RODO.

5.4. Przez zapewnienie bezpieczeństwa informacji rozumie się zapewnienie każdego z tych atrybutów informacji:

a) poufności – rozumianej jako właściwość zapewniająca, że informacje nie są udostępniane nieupoważnionym osobom,

b) integralności – rozumianej jako właściwość zapewniająca, że informacja nie została zmieniona lub zniszczona w sposób nieautoryzowany,

c) dostępności – rozumianej jako zapewnienie, że informacja jest dostępna zawsze wtedy, kiedy zachodzi taka potrzeba.

5.5. W Starostwie obowiązują następujące zasady bezpieczeństwa:

a) „Zasada wiedzy koniecznej" – osoby uprawnione posiadają informacje niezbędne do wykonywania przez nich obowiązków.

b) „Zasada potrzeby koniecznej" – osoby uprawnione mają dostęp jedynie do zasobów, które są niezbędne do wykonywania przez nich obowiązków.

c) „Zasada zachowania poufności" – osoby uprawnione są zobowiązane do zachowania poufności o informacjach, które zdobyły przez realizowanie swoich czynności zawodowych oraz o stosowanych w Starostwie zabezpieczeniach obejmujących te informacje.

5.6. We wszystkich sytuacjach spornych lub specyficznych wymaganiach nieujętych w dokumentacji SZBI, zezwolenia na odstępstwa może wydać Starosta lub w uzasadnionych sytuacjach bezpośredni przełożony. Sytuacje wymagające odstępstw mogą być podstawą do dalszego rozwijania dokumentacji.

6. Odpowiedzialności w bezpieczeństwie informacji

6.1. Administrator Danych Osobowych

a) Starosta Powiatu (jako realizujący zadania ADO) – odpowiada za zapewnianie środków na realizowanie postanowień wynikających z wymagań prawnych, zatwierdzanie dokumentacji SZBI, przydzielanie obowiązków w zakresie bezpieczeństwa informacji oraz prowadzenie nadzoru nad zgodnością przetwarzania danych osobowych.

b) Starosta Nidzicki, zgodnie z art. 37 RODO wyznacza Inspektora Ochrony Danych.

c) Starosta Nidzicki może wyznaczyć Administratora Systemów Informatycznych (ASI), który odpowiada za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych określonych w Instrukcji Zarządzania Systemem Informatycznym.

d) Obowiązki ADO wynikające z przepisów prawa, m.in. przeprowadzanie oceny skutków, spełnianie obowiązku informacyjnego, wypełnianie praw osób, których dane dotyczą są realizowane przez wyznaczone osoby oraz zgodnie z postanowieniami dokumentacji SZBI.

6.2. Inspektor Ochrony Danych

a) Do obowiązków IOD w szczególności należy:
- monitorowanie zgodności funkcjonowania urzędu z przepisami w zakresie ochrony danych osobowych,
- przeprowadzenie szacowań ryzyka oraz oceny skutków naruszeń,
- monitorowanie dokumentacji SZBI,
- szkolenie osób upoważnionych do przetwarzania danych osobowych z przepisami i zasadami dotyczącymi ochrony danych osobowych,
- dokonuje aktualizacji prowadzonego Rejestru Czynności Przetwarzania lub opiniuje planowane zmiany pod kątem wdrożenia dodatkowych zabezpieczeń
- doradztwo osobom upoważnionym oraz Administratorowi w kwestiach przetwarzania danych osobowych i zgodności z RODO.

b) W celu realizacji w/w powierzonych zadań IOD ma prawo:
- kontrolować osoby przetwarzające dane osobowe w zakresie właściwego stosowania ochrony danych osobowych w odniesieniu do SZBI oraz przepisów prawa,
- wydawać polecenia osobom upoważnionym w zakresie bezpieczeństwa danych osobowych – jeśli zagrożone jest bezpieczeństwo informacji lub zgodność z przepisami prawa,
- informować ADO o przypadkach naruszenia bezpieczeństwa danych osobowych,
- żądać od wszystkich osób przetwarzających wyjaśnień, w sytuacjach naruszenia bezpieczeństwa danych osobowych oraz w celu ustalenia stanu faktycznego ochrony danych osobowych,
- współpracować z organem nadzorczym.

6.3. Administrator Systemu Informatycznego

a) ASI, w zależności od przypisanego zakresu czynności wynikającego z zatrudnienia, odpowiada za:
- Przeprowadzanie lub nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
- zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur, określających częstotliwość ich zmiany w systemach informatycznych,
- nadzór nad czynnościami związanymi z prowadzeniem systemu, w zakresie obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywanych procedur uaktualnienia systemów antywirusowych i ich konfiguracji,
- nadzór nad wykonywaniem i przechowywaniem kopii zapasowych baz danych, systemów informatycznych i innych plików,
- nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów, służących do przetwarzania danych osobowych,
- czuwanie nad prawidłowym działaniem podległego mu systemu informatycznego.

- nadawania uprawnień, gromadząc wnioski od Kierowników poszczególnych działów organizacyjnych, dotyczące uprawniania nowych pracowników.

b) ASI bierze udział w ocenie zdarzeń naruszających bezpieczeństwo informacji, dotyczących struktury informatycznej.

c) W zależności od sytuacji ASI uczestniczy w ocenie skutków naruszeń oraz uczestniczy w procesie analizowania wpływu na bezpieczeństwo informacji przy wprowadzanych zmianach.

6.4. Kierownicy komórek organizacyjnych

a) Przez Kierowników komórek organizacyjnych (KKO), uważa się Kierowników Wydziałów Starostwa, jak również osoby kierujące wyznaczonymi Zespołami, wyznaczone w ramach struktury Starostwa.

b) Samodzielne Stanowiska, na potrzeby realizacji procesów opisanych w dokumentacji SZBI, samodzielnie realizują działania KKO.

c) KKO odpowiadają za:

- uczestnictwo w procesie upoważniania oraz nadawania uprawnień – w tym określanie zakresu upoważnień podległych pracowników,
- zgłaszanie zmian w zakresie obowiązków wpływających na zakres upoważnienia lub uprawnień w systemie informatycznym,
- nadzór nad przestrzeganiem obowiązujących zasad przez podległych pracowników,
- uczestniczenie w procesie zarządzania incydentami – w tym zgłaszania, określania wymaganych działań oraz dalszego postępowania z incydentami,
- uczestniczenie w określaniu wpływu zmian w Starostwie na bezpieczeństwo przetwarzanych informacji,
- analizowanie zawieranych umów oraz zlecania usług podmiotom zewnętrznym pod kątem sytuacji powierzenia danych osobowych.

6.5. Pracownik ds. kadrowych

a) Do obowiązków pracownika ds. kadrowych należy:

- Informowanie IOD o zatrudnieniu nowych osób lub o zwolnieniach.

6.6. Osoby uprawnione

a) Osoby uprawnione, w tym osoby posiadające upoważnienie, są zobowiązane do:

- przestrzegania przepisów prawa oraz zasad bezpieczeństwa informacji,
- zwracanie uwagi na obce osoby, znajdujące się bez nadzoru w obszarach z ograniczonym dostępem dla osób trzecich lub w miejscach przeznaczonych dla osób uprawnionych,
- zgłaszania zdarzeń potencjalnie naruszających bezpieczeństwo informacji,
- zgłaszania słabości lub niepoprawnego działania stosowanych zabezpieczeń,
- zgłaszania wszelkich zmian w zakresie procesów przetwarzania informacji lub zbiorów danych osobowych, w tym rozszerzania lub zmniejszania zakresu przetwarzanych danych, usuwania lub konieczności utworzenia nowych procesów lub zbiorów.

6.7. Pozostali pracownicy

a) Pozostali pracownicy, nie związani z przetwarzaniem informacji, są zobowiązani do:

- zgłaszania zdarzeń potencjalnie naruszających bezpieczeństwo informacji – pozostawionych dokumentów poza zamykanymi obszarami, szafami lub otwartych pomieszczeń po godzinach pracy, itp.

- zgłaszania źle funkcjonujących zabezpieczeń, zwłaszcza fizycznych.

7. Przegląd i rozwój systemu zarządzania bezpieczeństwem informacji

7.1. ADO zobowiązany jest do przeprowadzania okresowych audytów, w tym mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, zgodnie z art. 32 ust. 1 lit. d) RODO, w celu weryfikowania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz efektywności zasad bezpieczeństwa wdrożonych na podstawie niniejszej Polityki.

7.2. Audyty obejmują przegląd systemu ochrony danych osobowych, w tym audyt systemu ochrony danych osobowych, analizę ryzyka związanego z bezpieczeństwem zasobów uczestniczących w operacjach przetwarzania danych oraz ocenę skutków przetwarzania dla ochrony danych, jeśli ADO jest zobowiązany do wykonania takiej oceny, bądź podejmie decyzję o jej wykonaniu pomimo braku takiego obowiązku. Dokonując przeglądu wykonywanych operacji przetwarzania danych osobowych, należy dokonać oceny podmiotów przetwarzających, o ile takie istnieją, w zakresie spełnienia obowiązków dotyczących powierzenia danych osobowych wynikających z art. 28 RODO.

7.3. Rozwój SZBI jest realizowany zgodnie z Procedurą zarządzania zmianą oraz podejmowanymi na tej podstawie działaniami udoskonalającymi.

7.4. Okresowo lecz nie rzadziej niż raz w roku przeprowadzane jest szacowanie ryzyka utraty bezpieczeństwa informacji zgodnie z procedurą przeprowadzania szacowania ryzyka i oceny skutków.

7.5. Przegląd SZBI jest realizowany wewnętrznie, poprzez bezpośredni nadzór nad przestrzeganiem przyjętych zasad, zgodnie z podziałem obowiązków oraz w związku z realizacją procedur zarządzania incydentami oraz zarządzania zmianą.

7.6. Przegląd jest również realizowany poprzez audyty wewnętrzne w zakresie bezpieczeństwa informacji. Audyty mogą być realizowane siłami wewnętrznymi lub zewnętrznie.

7.7. Na potrzeby rozwoju dokumentacji SZBI oraz zapewniania jej przestrzegania, wprowadza się numery wydania. Przed wypełnieniem postanowień danej regulacji, należy zweryfikować jej aktualne wydanie, zgodnie z wykazem dokumentów powiązanych, zgodnie z punktem 9.

8. Dokumenty powiązane

Polityka bezpieczeństwa informacji posiada poniższą dokumentację powiązaną:

8.1. Polityka bezpieczeństwa danych osobowych – Wydanie 2

8.2. Instrukcja zarządzania systemem informatycznym – Wydanie 1

8.3. Procedura realizacji praw osób, których dane dotyczą – Wydanie 2

8.4. Procedura przeprowadzania szacowania ryzyka i oceny skutków – Wydanie 1

8.5. Procedura zarządzania incydentami – Wydanie 2

8.6. Procedura zarządzania zmianą – Wydanie 1

Polityka bezpieczeństwa danych osobowych

1. Cel dokumentu

Celem Polityki jest ustanowienie zasad i reguł postępowania zabezpieczających przetwarzanie danych osobowych w Starostwie Powiatowym w Nidzicy, dalej rozumianym Starostwem. Niniejsza polityka reguluje takie procesy jak: upoważnianie osób do prawidłowego przetwarzania, sposoby postępowania z danymi oraz ich nadzór, jak również przedstawia prowadzoną w związku z powyższymi działaniami dokumentację bezpieczeństwa.

2. Zasady przetwarzania danych osobowych

2.1. Organem realizującym obowiązki ADO w Starostwie jest Starosta Nidzicki.

2.2. Dostęp do danych osobowych oraz możliwość ich przetwarzania posiadają wyłącznie osoby, które otrzymały pisemne upoważnienie do przetwarzania danych osobowych, zgodne z **Załącznikiem nr 1** do Polityki.

2.3. Podczas zatrudnienia nowego pracownika KKO wypełnia wniosek o nadanie upoważnienia do przetwarzania danych osobowych, zgodnie **z załącznikiem nr 7** do niniejszej Polityki, który następnie przekazuje do sekretariatu celem dalszej dekretacji.

2.4. Wniosek o nadanie upoważnienia należy uzupełnić o odpowiednie procesy, zgodnie aktualnym Rejestrem Czynności Przetwarzania.

2.5. Na podstawie wniosku IOD sporządza upoważnienie do przetwarzania danych osobowych, które zatwierdza Starosta Nidzicki lub osoby działające w jego imieniu.

2.6. Upoważnienie nadaje się na czas trwania umowy zawartej z pracownikiem.

2.7. Podczas zmiany stanowiska pracy, komórki organizacyjnej lub obowiązków służbowych pracownika, należy przygotować nowe upoważnienie, zgodnie z opisem pkt 2.3 – 2.5, wskazując na aktualny zakres uprawnień.

2.8. W przypadku rozwiązania stosunku pracy upoważnienie wygasa automatycznie.

2.9. Wykaz osób posiadających upoważnienie do przetwarzania danych osobowych przedstawia ewidencja osób upoważnionych do przetwarzania danych osobowych, tj. **Załącznik nr 5**.

2.10. Każdy pracownik zostaje zobowiązany do zapoznania się oraz przestrzegania zasad ochrony danych osobowych, w tym dokumentacji bezpieczeństwa oraz podpisuje stosowne oświadczenie, tzn. **Załącznik nr 2** lub **Załącznik nr 2a**.

2.11. Nadawanie uprawnień do systemów informatycznych opisuje Instrukcja zarządzania systemem informatycznym.

2.12. Starostwo udostępnia przetwarzane dane osobowe innym podmiotom, w tym wynikającym z przepisów prawa z uwzględnieniem odpowiednich środków ostrożności.

2.13. Każda sytuacja przekazania danych osobowych w celu ich dalszego przetwarzania przed podmioty zewnętrzne w zakresie realizowanym przez Starostwo odbywa się w sposób sformalizowany oraz zgodnie z zasadami punktu 7.

2.14. Przetwarzanie danych osobowych podlega bieżącemu nadzorowi oraz monitorowaniu realizowanemu odpowiednio przez KKO oraz IOD.

2.15. Obowiązki w zakresie bezpieczeństwa informacji opisuje Polityka Bezpieczeństwa Informacji.

2.16. W przypadku naruszenia bezpieczeństwa danych osobowych każdy pracownik ma obowiązek niezwłocznego zgłoszenia sytuacji, której jest świadkiem lub uczestnikiem do osoby pełniącej rolę bezpośredniego przełożonego oraz postępowania zgodnie z procedurą zarządzania incydentami.

3. Obowiązek informacyjny

3.1. W przypadku zbierania danych od osoby, której dane dotyczą, podczas pozyskiwania danych osobowych podaje się informacje, o których mowa w art. 13 RODO, chyba że osoba, której dane dotyczą dysponuje już tymi informacjami. Wzór klauzuli informacyjnej stanowi **załącznik nr 8.**

3.2. Zakres przekazywanych informacji obejmuje:

a) pełną nazwę i dane kontaktowe administratora danych;
b) dane kontaktowe inspektora ochrony danych;
c) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
d) wskazanie prawnie uzasadnionych interesów, jeśli są podstawą przetwarzania;
e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców;
f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
g) okres, przez który dane osobowe będą przechowywane lub kryteria ustalania tego okresu;
h) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
i) jeżeli przetwarzanie odbywa się na podstawie wyrażonej zgody – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
j) informacje o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;
k) informację czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
l) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3.3. W przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą, osobie której dane dotyczą podaje się informacje, o których mowa w art. 14 RODO. Wówczas należy przekazać następujące informacje:

a) pełną nazwę i dane kontaktowe administratora danych;
b) dane kontaktowe inspektora ochrony danych;
c) cele przetwarzania oraz podstawę prawną przetwarzania;
d) kategorie odnośnych danych osobowych;
e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców;

f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej;
g) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
h) prawnie uzasadnione interesy, jeśli są podstawą przetwarzania;
i) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
j) jeżeli przetwarzanie odbywa się na podstawie wyrażonej zgody, to informacje o prawie do jej cofnięcia w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
k) informacje o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;
l) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
m) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3.4. Informacje, o których mowa w punkcie 3.3 (przy pozyskiwaniu danych z innego źródła) podaje się:
a) w rozsądnym terminie po pozyskaniu danych osobowych – do 30 dni, lub
b) najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą, lub
c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

3.5. Spełnianie obowiązku informacyjnego odbywa się poprzez:
a) umieszczanie na wzorach dokumentów (wniosków, kwestionariuszy, umów, itp.) klauzul informacyjnych;
b) umieszczenie klauzul w ogólnodostępnym miejscu, gdzie przyjmowani są interesariusze;
c) umieszczenie klauzul na stronie internetowej;
d) przesyłanie klauzul w formie wiadomości elektronicznych lub tradycyjnych, w odpowiedzi na kontakt osoby;
e) przekazywanie słowne treści klauzul, jeśli nie jest możliwe zapoznanie osoby przez powyższe sposoby.

3.6. Odrębny dokument nie jest wymagany jeśli osoba korzysta ze wzorów wniosków lub umów, na których ujęto treść klauzuli.

3.7. W ramach określonego celu przetwarzania obowiązek informacyjny względem danej osoby realizuje się raz.

3.8. Obowiązek podania informacji nie ma zastosowania, gdy:
- Osoba, której dane dotyczą, dysponuje już tymi informacjami,
- Udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku,
- Proces pozyskiwania danych jest wyraźnie uregulowanym prawem Unii Europejskiej lub prawem państwa członkowskiego, lub

- Dane muszę pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie UE lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

3.9. Za spełnianie obowiązku informacyjnego względem osób, których dane są przetwarzane w Starostwie, odpowiedzialna jest każda osoba posiadające upoważnienie do przetwarzania danych osobowych.

3.10. Nadzór nad powyższym procesem, tj. poprawną realizacją obowiązku informacyjnego prowadzą odpowiednio KKO oraz IOD.

4. Postępowanie z danymi nadmiarowymi i anonimizacja danych

4.1. Względem celu w jakim przetwarzane są dane osobowe określony został maksymalny zakres danych niezbędny do jego realizacji.

4.2. Niezależnie od podstaw prawnych dla realizowanych celów osoby mogą kierować do Starostwa pisma zawierające dane nadmiarowe względem tych celów.

4.3. Dopuszcza się niezwłoczne zastosowanie anonimizacji lub usunięcia przekazanych dokumentów z zasobów Starostwa.

4.4. Powyższe dokonuje się poprzez:

a) zamazanie danych nadmiarowych na dokumencie zawierającym również dane niezbędne do realizacji celu, przy czym zamazanie musi zapewniać brak możliwości odtworzenia danych;

b) usunięcie danych poprzez zniszczenie w niszczarce dokumentu lub usunięcie plików z komputera lub poczty elektronicznej, w tym również z „kosza";

c) odesłanie nadmiarowych danych – jeśli są one w formie oryginału.

4.5. W przypadku stwierdzenia powtarzających się sytuacji przekazywania nadmiarowych danych w konkretnych celach, Kierownik wydziału wraz z IOD podejmuje wybrane działania:

a) opracowuje formularze ograniczające podawanie nadmiarowych danych;

b) wskazuje w formie komunikatu na jasne warunki podejmowania decyzji w ramach realizacji celu, tak aby bezpośrednio z nich wynikał brak zasadności podawania dodatkowych danych;

c) zwraca się do osób z prośbą o nieprzekazywanie danych nadmiarowych

5. Realizacja praw osób, których dane dotyczą

5.1. Osobom, których dane są przetwarzane przysługują prawa wynikające z rozdziału III RODO. Są to prawa do żądania od Starosty Nidzickiego, jako administratora danych, dostępu do swoich danych osobowych oraz informacji o ich przetwarzaniu, prawa do ich sprostowania, usunięcia, przeniesienia, ograniczenia przetwarzania lub prawa do wniesienia sprzeciwu wobec przetwarzania.

5.2. Powyższe realizuje się w oparciu o „Procedurę realizacji praw osób, których dane dotyczą".

5.3. W przypadku wątpliwości co do zakresu udzielanych informacji lub ich zasadności, wniosek należy skonsultować z KKO lub IOD.

6. Zasady udostępniania danych osobowych

6.1. Starostwo udostępnia przetwarzane dane osobowe tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

6.2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej.

6.3. Wniosek powinien zawierać informacje, umożliwiające wyszukanie żądanych danych osobowych, wskazywać ich zakres i przeznaczenie oraz podstawę prawną.

6.4. Wniosek jest rozpatrywany przez KKO oraz w razie wątpliwości z IOD.

6.5. W sytuacjach spornych, decyzję w sprawie udostępnienia podejmuje Starosta Nidzicki.

6.6. Starosta, IOD lub KKO może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą, innych osób lub byłoby niezgodne z przepisami prawa.

7. Zasady powierzenia danych osobowych

7.1. Starosta Nidzicki, jako administrator danych, może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej lub na podstawie przepisów prawa, które to powierzenie regulują.

7.2. Umowa powierzenia jest wymagana w każdym przypadku, kiedy występuje przekazanie danych osobowych lub ich gromadzenie przez podmiot zewnętrzny.

7.3. Umowa o której mowa w punkcie powyżej przedstawia wzór stanowiący **Załącznik nr 4** do niniejszej polityki.

7.4. Umowa powierzenia nie znajduje zastosowania, w przypadku, gdy pracownik pomiotu zewnętrznego uzyskuje dostęp do danych osobowych, jednak przetwarzanie odbywa się w obrębie Starostwa. Wówczas możliwe jest wydanie upoważnienia.

7.5. Zawarta z podmiotem zewnętrznym umowa powierzenia, w związku z RODO czyni ten podmiot Podmiotem Przetwarzającym (PP). Umowa, musi zawierać poniższe elementy:

a) cel przetwarzania, z zastrzeżeniem zakazu wykorzystania danych w innym celu;

b) zakres, kategorie oraz charakter powierzanych danych;

c) odpowiedzialność stron, w tym za przestrzeganie postanowień umownych oraz przestrzeganie obowiązujących przepisów prawa – zwłaszcza w zakresie wdrożenia odpowiednich środków technicznych i organizacyjnych zabezpieczających dane osobowe;

d) konieczność upoważnienia przez PP, osób przetwarzających dane w jego imieniu oraz zobowiązanie ich do zachowania poufności;

e) zakaz korzystania z podwykonawców bez pisemnej zgody lub aneksu do umowy;

f) konieczność uczestniczenia PP w wypełnianiu obowiązków ciążących na Staroście Nidzickim, jako administratorze danych, w tym realizacji praw osób, których dane dotyczą oraz przekazywania informacji o sposobach przetwarzania oraz informacji potrzebnych do szacowania ryzyka i oceny skutków naruszeń;

g) zgłaszanie wszelkich incydentów lub podejrzeń incydentów, z zapewnieniem wszystkich niezbędnych informacji do poprawnej realizacji zgłaszania incydentów zgodnie z przepisami prawa;

h) sposób potwierdzania przestrzegania przepisów prawa i zasad bezpieczeństwa, w tym umożliwienie monitorowania, audytowania PP;

i) konieczność usunięcia lub zwrócenia powierzonych danych osobowych w przypadku wygaśnięcia umowy lub jej rozwiązania.

7.6. W ramach zawartych umów powierzenia prowadzi IOD prowadzi rejestr podmiotów przetwarzających powierzone dane z uwzględnieniem podwykonawców (jeśli występują). Przedmiotowy rejestr prowadzony jest zgodnie z **Załącznikiem nr 3**.

8. Ewidencjonowanie procesów przetwarzania danych osobowych

8.1. ADO prowadzi rejestr czynności przetwarzania, w tym rejestr kategorii czynności przetwarzania dokonywanych w imieniu Starostwa.

8.2. Osoby odpowiedzialne za procesy przetwarzania danych osobowych są zobowiązani do zgłoszenia do IOD:

a) planowanego utworzenia nowych procesów danych osobowych lub usunięcia istniejących;

b) wnoszenia zmian w procesach już istniejących, np. rozszerzenia lub zmniejszenia zakresu procesów, co może wynikać z przepisów prawa;

c) planowanych zmian w zakresie procesów przetwarzania danych, w tym utworzenia nowych lub zakończenia istniejących.

8.3. Na podstawie powyższych informacji IOD dokonuje aktualizacji prowadzonego Rejestru Czynności Przetwarzania lub opiniuje planowane zmiany pod kątem wdrożenia dodatkowych zabezpieczeń.

8.4. Rejestry wskazane w punkcie 8.1 przyjmują formę pisemną, w tym również postać elektroniczną oraz prowadzone są zgodnie z **Załącznikiem nr 6** do niniejszej polityki.

9. Ochrona pomieszczeń

9.1. Wszystkie pomieszczenia, w których przetwarzane są dane osobowe zostały wyposażone w drzwi z zamkiem oraz posiadają czujki systemu alarmowego.

9.2. Dostęp do budynku jest monitorowany za pomocą systemu alarmowego.

9.3. Zastosowano dodatkowe zabezpieczenia w postaci krat w oknach.

9.4. Przebywanie w pomieszczeniach, w których przetwarzane są dane osobowe, osób trzecich jest możliwe tylko w obecności osoby upoważnionej. W szczególności niedozwolone jest pozostawianie bez nadzoru osób trzecich w tym pomieszczeniach.

9.5. Pomieszczenia te, powinny być zamykane na czas nieobecności w nich osób upoważnionych, w sposób uniemożliwiający uzyskanie dostępu do nich osób trzecich.

9.6. Przy opuszczaniu pomieszczeń i budynku, osoba ostatnia powinna się upewnić, że zostały zamknięte drzwi.

10. Wydruki dokumentów zawierających dane osobowe

10.1. Dokumentacja zawierająca dane osobowe powinna pozostawać w obrębie obszarów przetwarzania oraz podlegać bezwzględnej ochronie przed możliwością wglądu osób trzecich w treść dokumentów.

10.2. Drukarki nie mogą być pozostawione bez kontroli, jeśli są lub wkrótce będą drukowane na nich dane osobowe z systemu informatycznego, o ile dostęp osób postronnych do pomieszczeń drukarek nie jest odpowiednio ograniczony.

10.3. Dokumentację zawierającą dane osobowe należy przechowywać w szafach lub szufladach zamykanych na klucz.

10.4. Klucze, o których mowa wyżej posiadają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z upoważnieniem.

10.5. Wydruki, notatki, kserokopie dokumentów itp. niewykorzystane, a zawierające dane osobowe, muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści.

11. Sankcje

11.1. Nieprzestrzeganie zasad bezpieczeństwa opisanych w dokumentacji SZBI oraz przepisów prawa określających ochronę danych osobowych stanowi naruszenie obowiązków pracowniczych i może być przyczyną postępowania dyscyplinarnego lub wiązać się z konsekwencjami określonymi przepisami Ustawy lub RODO.

12. Wykaz załączników

- Załącznik nr 1 – Upoważnienie do przetwarzania danych osobowych
- Załącznik nr 2 – Oświadczenie osoby upoważnionej do przetwarzania danych osobowych
- Załącznik nr 2a – Oświadczenie pozostałych pracowników
- Załącznik nr 3 – Rejestr podmiotów przetwarzających powierzone dane osobowe
- Załącznik nr 4 – Wzór umowy powierzenia danych osobowych
- Załącznik nr 5 – Ewidencja osób upoważnionych do przetwarzania danych osobowych
- Załącznik nr 6 – Rejestr czynności przetwarzania
- Załącznik nr 7 – Wniosek o nadanie/zmianę/cofnięcie* uprawnień do przetwarzania danych osobowych
- Załącznik nr 8 - Wzór Klauzuli informacyjnej.

Nidzica, dnia ..... r.

.....

Upoważnienie Nr ..../.....

do przetwarzania danych osobowych

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 (ogólne rozporządzenie o ochronie danych) Dz.U.UE.L.2016 poz. 119 str. 1, upoważniam Panią/Pana:

.....

(imię i nazwisko osoby upoważnionej)

zatrudnioną (ego) w Starostwie Powiatowym w Nidzicy w Wydziale .....

na stanowisku .....

do przetwarzania danych osobowych w systemie nieinformatycznym i systemie informatycznym w zakresie:

.....

.....,

w granicach nieprzekraczających ustalonego zakresu obowiązków.

Osoba upoważniona do przetwarzania danych w systemie informatycznym posługuje się identyfikatorem dostępu .....

Upoważnienie wydaje się na okres **od dnia** ..... **do dnia** .....

.....

Podpis Administratora Danych Osobowych

Rozumiem zakres nadanego upoważnienia oraz zobowiązuję się do zachowania poufności danych osobowych i innych informacji nie będących danymi jawnymi, zarówno w trakcie jak i po ustaniu stosunku pracy.

.....

Podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam(em) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z Ustawą o ochronie danych osobowych oraz Rozporządzeniem UE 2016/679.

Oświadczam ponadto, że zapoznałem(łam) się z wewnętrzną Polityką bezpieczeństwa informacji, Polityką bezpieczeństwa danych osobowych, Instrukcją zarządzania systemem informatycznym oraz procedurami powiązanymi. Zobowiązuje się przestrzegać opisanych w tej dokumentacji zasad bezpieczeństwa informacji, a w szczególności oświadczam, co następuje:

1) będące w mojej dyspozycji dane osobowe będę zabezpieczać przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osoby nieupoważnione, przetwarzaniem ich z naruszeniem ustawy o ochronie danych osobowych, utratą, uszkodzeniem lub zniszczeniem,
2) nie będę udostępniał swoich danych do logowania innym osobom,
3) nie będę pozostawiać otwartego programu po opuszczeniu stanowiska pracy oraz nie będę pozostawiać dokumentacji z danymi osobowymi poza obszarami chronionymi.

Świadomy(a) odpowiedzialności służbowej i karnej oświadczam, że znane mi dane osobowe będę przetwarzać zgodnie z prawem oraz z dochowaniem należytej staranności, przestrzeganiem wewnętrznych zasad bezpieczeństwa oraz zachowaniem poufności tych danych również po ustaniu zatrudnienia.

.....

(data i podpis osoby upoważnionej)

Oświadczenie

Oświadczam, że zapoznałam(em) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z Ustawą o ochronie danych osobowych oraz Rozporządzeniem UE 2016/679.

Ponadto oświadczam, że zapoznałem(łam) się z wewnętrzną Polityką bezpieczeństwa informacji, Polityką bezpieczeństwa danych osobowych, Instrukcją zarządzania systemem informatycznym oraz procedurami powiązanymi. Zobowiązuje się przestrzegać opisanych w tej dokumentacji zasad bezpieczeństwa informacji, a w szczególności oświadczam, że zobowiązuję się do:

- ✓ niewykorzystywania danych osobowych oraz innych informacji w celach pozasłużbowych, o ile informacje te nie są jawne,
- ✓ zachowania w tajemnicy sposobów zabezpieczenia danych osobowych oraz innych informacji, o ile informacje te nie są jawne,
- ✓ informowania o naruszeniach zabezpieczeń danych osobowych w przypadku ich stwierdzenia oraz zgłaszania źle funkcjonujących zabezpieczeń fizycznych

Zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam lub będę miał(a) dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych, zarówno w trakcie wiążącego mnie stosunku pracy oraz po jego ustaniu.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy, naruszenie przepisów karnych w zakresie ochrony danych osobowych lub za ciężkie naruszenie obowiązków umownych w przypadku umowy cywilnoprawnej.

_____

(data i podpis)

Rejestr podmiotów przetwarzających powierzone dane osobowe

Lp.	Nazwa podmiotu	Zakres świadczonej usługi	Oznaczenie umowy	Podwykonawcy (podać jeśli występują)

Wzór umowy powierzenia przetwarzania danych osobowych

Umowa nr .....

Zawarta w dniu ..... r. w ..... pomiędzy:

..... zwaną w dalszej części niniejszej umowy „Zleceniodawcą"

reprezentowanym przez:

.....

a

..... zwanym w dalszej części niniejszej umowy „Wykonawcą"

reprezentowanym przez:

.....

o następującej treści:

§ 1

Powierzenie przetwarzania danych osobowych

1. W związku z realizacją umowy nr ..... z dnia ..... r. pomiędzy ....., a ....., o ..... . Zleceniodawca powierza Wykonawcy w trybie art. 28 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, zwanego dalej „Rozporządzeniem", przetwarzanie danych osobowych.
2. Zleceniodawca oświadcza, że jest administratorem danych, które powierza.
3. Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych w zakresie i celu określonym w § 2.

§ 2

Zakres i cel przetwarzania danych

1. Wykonawca będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące kategorie danych osobowych klientów (lub kontrahentów, pracowników, itp.):
   a. imię i nazwisko,
   b. numer ewidencyjny PESEL,
   c. seria i numer dowodu osobistego,
   d. ..... .
   e. .....

2. Powierzone przez Zleceniodawcę dane osobowe będą przetwarzane przez Wykonawcę wyłącznie w celu wykonywania przez Wykonawcę na rzecz Zleceniodawcy usług szczegółowo opisanych w umowie, o której mowa w § 1 ust. 1 i w sposób zgodny z niniejszą Umową. W szczególności przetwarzanie dotyczy ..... (wskazać z umowy, np. tworzenie kopii zapasowych, pozyskiwanie zgód od klientów, itp.)
3. Przetwarzanie będzie realizowane w (formie elektronicznej lub tradycyjnej)

§ 3

Sposób wykonania Umowy w zakresie przetwarzania danych osobowych

1. Wykonawca zobowiązuje się, przy przetwarzaniu danych osobowych, o których mowa w § 2 ust 1, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych adekwatnych do zagrożeń związanych z przetwarzaniem danych.
2. Wykonawca oświadcza, że przyjęte przez niego środki zabezpieczeń umożliwiają:
    a. zachowanie poufności, integralności i dostępności danych powierzonych
    b. znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają odpowiedni poziom bezpieczeństwa poprzez stosowanie uwierzytelniania do kontroli dostępu, stosowanie zabezpieczeń kryptograficznych oraz stosowanie kopii zapasowych.
    c. stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Rozporządzenia, zmianą, utratą, uszkodzeniem lub zniszczeniem, w zakresie, za który odpowiada Wykonawca.
3. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami powszechnie obowiązującego prawa, które chronią prawa osób, których dane dotyczą.
4. Wykonawca upoważni osoby mu podległe do przetwarzania danych osobowych w ramach realizacji niniejszej umowy oraz zobowiąże ich do zachowania poufności.
5. Wykonawca zobowiązuje się niezwłocznie zawiadomić Zleceniodawcę o:
    a. każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba, że zakaz zawiadomienia wynika z przepisów prawa, a szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienia poufności wszczętego dochodzenia,
    b. każdym nieupoważnionym dostępie do danych osobowych i potencjalnym naruszeniem bezpieczeństwa informacji,
    c. każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.
6. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej Umowy poprzez przeprowadzenie zapowiedzianych na 7 dni kalendarzowych wcześniej doraźnych kontroli dotyczących przetwarzania danych osobowych przez Wykonawcę oraz żądania składania przez niego pisemnych wyjaśnień. Kontrola taka może być wykonana przez podmiot zewnętrzny, posiadający do tego uprawnienia, wynajęty do tego zadania przez Zleceniodawcę.
7. Na zakończenie kontroli, o których mowa w ust. 6, przedstawiciel Zleceniodawcy sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. Wykonawca może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony.

8. Wykonawca zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
9. Wykonawca zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie Zleceniodawcy dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.
10. Dopuszcza się korzystanie z podwykonawców wymienionych w załączniku nr 1, do niniejszej umowy. Zmiany w zakresie podwykonawców muszą być przekazywane pisemnie do Zleceniodawcy oraz skutkować aneksem załącznika. Jednocześnie Zleceniobiorca zobowiązuje się zapewnić, że podwykonawca wypełni postanowienia niniejszej umowy, w tym w szczególności zapewni środki zabezpieczające w celu zachowania poufności i integralności danych, zgodne z niniejszą umową.

§4

Odpowiedzialność Wykonawcy

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie osobom nieupoważnionym.
2. W przypadku naruszenia przepisów Rozporządzenia lub niniejszej Umowy z przyczyn leżących po stronie Wykonawcy, w następstwie, czego Zleceniodawca, jako administrator danych osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Wykonawca zobowiązuje się pokryć Zleceniodawcy poniesione z tego tytułu straty i koszty.

§5

Czas obowiązywania Umowy powierzenia

Niniejsza Umowa powierzenia zostaje zawarta na czas obowiązywania umowy, o której mowa w § 1 ust. 1 niniejszej umowy.

§ 6

Warunki wypowiedzenia Umowy

1. Zleceniodawca ma prawo rozwiązać niniejszą Umowę bez zachowania terminu wypowiedzenia, gdy Wykonawca:
   a. wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
   b. powierzył przetwarzanie danych osobowych podwykonawcom bez zgody Zleceniodawcy,
   c. nie zaprzestanie niewłaściwego przetwarzania danych osobowych,
   d. zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności niespełniania wymagań określonych w §3.
2. Rozwiązanie niniejszej Umowy przez Zleceniodawcę jest równoznaczne z wypowiedzeniem umowy, o której mowa w § 1 ust. 1.

§ 7

Rozwiązanie Umowy

Wykonawca, w przypadku wygaśnięcia umowy, o której mowa w §1 ust.1 i niniejszej umowy, zobowiązuje się w terminie ustalonym ze Zleceniodawcą, nie później jednak niż w ciągu 30 dni od daty rozwiązania umowy, o której mowa w §1 ust.1, zwrócić Zleceniodawcy wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie usunąć je z nośników

elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazanym Zleceniodawcy protokołem.

§8

Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§9

W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy Kodeksu Cywilnego.

§10

Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Zleceniodawcy.

§ 11

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

....

za Zleceniodawcę **za Wykonawcę**

Załącznik nr 1

Wykaz podwykonawców uczestniczących w procesie przetwarzania danych osobowych powierzonych, w związku z realizacją niniejszej umowy, z zachowaniem wymagań §3 ust. 10.

Nazwa podmiotu	Adres podmiotu	NIP	Zakres powierzenia
			Zgodny z przedmiotem umowy.

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Stanowisko służbowe	Wykaz czynności przetwarzania wynikających z upoważnienia	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator *(Jeżeli dane są przetwarzane w systemie informatycznym)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
...						

Nidzica, dd–mm–rr

Załącznik Nr 6 do Polityki bezpieczeństwa

Nazwa oraz dane kontaktowe	Starosta Nidzicki, ul. Traugutta 23, 13-100 Nidzica, tel/fax +48 (89) 625-32-79, sekr
Dane kontaktowe Inspektora Ochrony	iod@powiatnidzicki.pl

numer procesu	Nazwa procesu	cele przetwarzania	opis kategorii osób, których dane dotyczą	kategorie danych osobowych	kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
...					

etariat@powiatnidzicki.pl, NIP: 9840088817, REGON: 510750380

gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej	jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych	jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.	Podstawa prawna RODO	Przepis prawa	Sposób realizacji obowiązku informacyjnego

.....
pieczęć nagłówkowa

Wniosek o nadanie/zmianę/ cofnięcie* uprawnień do przetwarzania danych osobowych

Administrator
Danych Osobowych

NINIEJSZYM WNOSZĘ O:

1. **nadanie upoważnienia** do przetwarzania danych osobowych Pani/Panu .....

na okres od dnia ..... do dnia ..... zatrudnionego w Wydziale .....

..... Starostwa Powiatowego w Nidzicy

na stanowisku .....

Zakres upoważnienia .....

Wskazanie procesów przetwarzania jakich może dokonywać na danych osobowych określona w upoważnieniu osoba. W odniesieniu do systemu informatycznego należy wskazać określoną rolę/uprawnienia jaką dany użytkownik ma pełnić w danym module/modułach.

2. **zmianę upoważnienia nr.....z dnia** ..... do przetwarzania danych osobowych Pani/Panu .....

zatrudnionego w Wydziale ..... Starostwa Powiatowego w

Nidzicy na stanowisku..... w związku z .....

Zakres upoważnienia:

Wskazanie procesów przetwarzania jakich może dokonywać na danych osobowych określona w upoważnieniu osoba. W odniesieniu do systemu informatycznego należy wskazać określoną rolę/uprawnienia jaką dany użytkownik ma pełnić w danym module/modułach.

3. **cofnięcia upoważnienia nr.....z dnia** ..... do przetwarzania danych osobowych Pani/Panu .....

zatrudnionego w Wydziale ..... Starostwa Powiatowego w

Nidzicy na stanowisku..... w związku z .....

.....
(podpis Kierownika Komórki Organizacyjnej)

*niepotrzebne należy wykasować (w przypadku wersji elektronicznej) lub skreślić (w przypadku wersji papierowej)

Klauzule informacyjne dla Starostwa Powiatowego w Nidzicy

Dotyczy realizacji procesu nr .....:

.....

Zgodnie z artykułem 13 i 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), pragniemy dopełnić obowiązku informacyjnego przekazując Państwu poniższe dane:

Administratorem Państwa danych osobowych w Starostwie Powiatowym w Nidzicy jest Starosta Nidzicki z siedzibą przy ul. Traugutta 23, 13-100 Nidzica. Mogą się Państwo z nami skontaktować przy pomocy numeru telefonu: +048 (89) 625-32-79 lub mailowo: sekretariat@powiatnidzicki.pl Administrator wyznaczył Inspektora Ochrony Danych, z którym kontakt możliwy jest za pośrednictwem adresu e-mail: iod@powiatnidzicki.pl

Celem przetwarzania danych jaki realizuje Administrator jest .....
Państwa dane osobowe są przetwarzane na podstawie przepisów prawa, które określa ustawa o .....
Podanie danych jest dobrowolne, jednak niezbędne do zrealizowania celu.
Dane nie będą udostępniane innym podmiotom niż uprawnionym na podstawie przepisów prawa.
Dane osobowe będą przetwarzane przez ..... lat.

W związku z przetwarzaniem danych osobowych, na podstawie przepisów prawa, posiadają Państwo prawo do dostępu oraz do sprostowania podanych danych. Przysługuje Państwu prawo do żądania usunięcia lub ograniczenia przetwarzania oraz prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych. Przysługuje Państwu również prawo wniesienia skargi do Urzędu Ochrony Danych Osobowych. W ramach realizowanych celów przetwarzania nie występuje profilowanie, a dane nie będą transferowane poza Polskę. Mogą Państwo skorzystać z przedstawionych praw, kontaktując się z Administratorem na powyższe dane kontaktowe.

Procedura zarządzania incydentami

1. Cel i zakres dokumentu

Celem procedury jest zdefiniowanie działań, których realizacja pozwala na poprawne zgłaszanie, ocenę oraz podjęcie kroków zapewniających minimalizację negatywnych skutków incydentów.

2. Rodzaje zdarzeń związanych z bezpieczeństwem informacji

2.1. Zdarzenia zakwalifikowane jako incydenty, naruszenia ochrony danych osobowych lub uzasadnione podejrzenia naruszeń zabezpieczeń systemu zarządzania bezpieczeństwem informacji to m. in.:

a) sytuacje losowe lub nieprzewidywalne oddziaływanie czynników zewnętrznych na zasoby systemu np. pożar, zalane pomieszczenia, uszkodzenia wskutek prowadzonych prac remontowych;

b) awarie sprzętu lub oprogramowania, wpływające na bezpieczeństwo informacji;

c) pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub niepożądaną modyfikację w systemie;

d) ujawnienie osobom nieuprawnionym informacji objętych ochroną lub ujawnienie procedur przetwarzania informacji;

e) uzyskanie dostępu do informacji przez osobę, w tym pracownika, nieposiadającego stosowanego uprawnienia;

f) rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji (zagubienie dokumentów, niezabezpieczenie obszaru przetwarzania umożliwiające dostęp osób trzecich, prace w celach prywatnych, itp.).

3. Zgłaszanie i wstępna ocena zdarzeń

3.1. W przypadku podejrzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych dla ochrony przetwarzanych danych przez ADO, bezwzględnie na zajmowane stanowisko, każdy pracownik, który jako pierwszy stwierdził naruszenie lub możliwość naruszenia, zobowiązany jest do natychmiastowego zawiadomienia bezpośredniego przełożonego oraz IOD.

3.2. KKO dokonuje wstępnej oceny zgłoszenia, o którym mowa w punkcie 3.1 oraz określa jego zasadność.

3.3. Zgłoszenia „fałszywe" mogą wynikać z prowadzonych prac w Urzędzie, np. remontowych lub informatycznych oraz dotyczyć błędów użytkowników lub innych sytuacji nie wpływających negatywnie na bezpieczeństwo informacji.

3.4. Podejrzenia incydentów w zakresie obszaru informatycznego należy zgłaszać bezpośrednio do ASI. Zdarzenia mogą dotyczyć funkcjonowania sieci wewnętrznej, komunikacji oraz systemów informatycznych. Jeśli ASI ocenia zdarzenie jako zasadne, to przekazuje te informacje do IOD.

3.5. Zgłoszenia „fałszywe" mogą wynikać z prowadzonych prac w Starostwie, dotyczyć błędów użytkowników lub innych sytuacji nie wpływających negatywnie na bezpieczeństwo informacji.

3.6. O wszystkich zdarzeniach mogących wpływać na bezpieczeństwo danych osobowych musi zostać poinformowany IOD.

3.7. Pełnego zgłoszenia incydentu, jeśli to możliwe, dokonuje się w formie mailowej. Jeśli incydent ma wpływ na działanie systemu operacyjnego lub komunikacji sieciowej, zgłoszenia należy dokonać inna dostępną ścieżką komunikacji.

3.8. W jasnych sytuacjach, np. związanych z pożarem, włamaniem, należy powiadomić niezwłocznie odpowiednie organy władzy.

3.9. Zgłoszenie incydentu niezależnie od formy powinno w pierwszej kolejności wskazywać na istotę problemu, tak aby umożliwić szybką reakcję. W drugiej kolejności należy zapewnić jak najszerszy zakres informacji, tj. zgłoszenie powinno zawierać:

a) datę i czas wystąpienia lub stwierdzenia incydentu;
b) osoby uczestniczące w zdarzeniu;
c) miejsce wystąpienia incydentu;
d) rodzaj incydentu (w sposób ogólny, np. pożar, włamanie, usunięcie prawidłowych dokumentów);
e) zasoby objęte incydentem (w sposób ogólny, np. dokumenty, szafy, nośniki itp.);
f) dokładny opis zdarzenia – uwzględniając informacje o przyczynach zdarzenia lub podejrzeń przyczyn zdarzenia, możliwej eskalacji, innych uczestnikach zdarzeniach oraz podjętych działaniach związanych ze zdarzeniem.

3.10. Powyższy zakres zgłoszenia może zostać pominięty, jeśli wymaga tego dana sytuacja. Możliwość pominięcia szczegółowego opisu określa osoba przyjmująca zgłoszenie. Niezależnie od decyzji, szczegółowy opis zdarzenia musi zostać opracowany w późniejszym czasie, na potrzeby poprawnej realizacji procesu oceny naruszenia.

4. Ocena i postępowanie z incydentami

4.1. Opisany proces dotyczy pracowników pełniących rolę przełożonych, tj. KKO, IOD oraz ASI.

4.2. W momencie otrzymania zgłoszenia incydentu należy określić:

a) Zakres informacji objętych zdarzeniem – kategorie danych, jak wiele danych zostało objętych zdarzeniem, kategorie osób oraz występowanie danych wrażliwych.
b) Wysokość ryzyka naruszenia praw i wolności osób, których dane zostały naruszone, z uwzględnieniem stosowanych zabezpieczeń w zakresie naruszonych danych.
c) Czy zdarzenie się zakończyło, czy trwa nadal?
d) Czy zdarzenie może wystąpić ponownie?
e) Możliwości zatrzymania lub ograniczenia zdarzenia.
f) Konieczność powiadomienia specjalistów zewnętrznych.

4.3. Biorąc pod uwagę powyższą ocenę sytuacji, należy przekazać osobie zgłaszającej kroki jakie powinna podjąć. W zależności od sytuacji może to być polecenie:

a) zabezpieczenia miejsca zdarzenia;
b) przekazania instrukcji innym osobom;
c) wezwania organów władzy lub specjalistów zewnętrznych;
d) zabezpieczenia dowodów zdarzenia poprzez tworzenie print-screen'ów, robienie zdjęć i nagrań, kopiowanie plików, zabezpieczenie aktywów;
e) korzystania z zasobów w ograniczony sposób;
f) nie podejmowania żadnych dodatkowych czynności;
g) kontynuowania pracy.

5. Podejmowanie działań dotyczących zdarzenia

5.1. Działania mogą obejmować:

a) wdrożenie dodatkowych zabezpieczeń;
b) przeszkolenie pracowników;
c) wyciąganie konsekwencji do osób naruszających bezpieczeństwo informacji;
d) przeprowadzenie szczegółowych analiz i testów związanych z naruszeniem.

5.2. Działania dotyczące zdarzeń naruszających bezpieczeństwo przetwarzanych danych osobowych muszą obejmować:
   a) zgłoszenie naruszenia do Prezesa Urzędu Ochrony Danych Osobowych w ciągu 72 godzin;
   b) rozważenie zgłoszenia naruszenia do osób, których dane dotyczą.

5.3. W sytuacjach, gdzie ma to zastosowanie, osoby zgłaszające zostają poinformowane o zakończeniu postępowania ze zdarzeniem – dotyczy np. sytuacji, w których poinformowano użytkownika o zaprzestaniu pracy.

6. Dokumentowanie zdarzeń

6.1. Wszelkie naruszenia ochrony danych osobowych zostają obszernie dokumentowane, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w stopniu umożliwiającym weryfikowanie przestrzegania RODO przez Prezesa Urzędu.

6.2. Dokumentacja powinna się składać ze zgłoszenia od pracownika, podjętych środków tymczasowych, pełnej oceny dokonanej przez IOD i ASI lub specjalistów zewnętrznych, szczegółowego opisu podjętych działań.

6.3. Dokumentacja musi umożliwiać późniejszą weryfikację i prześledzenie podejmowanych działań, w tym być możliwa do udostępnienia podmiotom kontrolującym.

6.4. W związku z powyższym, ADO prowadzi rejestr incydentów ochrony danych, w oparciu o wzór stanowiący **Załącznik nr 7** do polityki bezpieczeństwa danych osobowych.

7. Zgłoszenie naruszenia do organu nadzorczego oraz osób, których dane dotyczą

7.1. W razie stwierdzenia, że naruszenie ochrony danych osobowych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych należy niezwłocznie zawiadomić Prezesa Urzędu, jednak nie później niż w ciągu 72 godzin od stwierdzenia naruszenia. Jeżeli zawiadomienia nie można dokonać we wskazanym terminie, zawiadomienie powinno być dokonywane sukcesywnie, z uwzględnieniem posiadanych informacji i bez zbędnej zwłoki. W przypadku zawiadomienia przekazanego Prezesowi Urzędu po wskazanym terminie, ADO dołącza do zawiadomienia wyjaśnienie przyczyn opóźnienia.

7.2. Dopuszcza się wykonywanie sukcesywnych zgłoszeń cząstkowych, jeśli pełne zgłoszenie nie jest możliwe do przekazania.

7.3. Zgłoszenie, o którym mowa musi co najmniej:
   a) opisywać charakter naruszenia ochrony danych osobowych (w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie) – dane wynikające z wewnętrznego zgłoszenia incydentu przez pracownika oraz ich dalszej analizy przez IOD opisanej w punkcie 4;
   b) zawierać imię i nazwisko oraz dane kontaktowe IOD;
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   d) opisywać zastosowane lub proponowane środki w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków;

7.4. Jeśli w procesie oceny z punktu 4, określono wysokie ryzyko naruszenia wolności i praw osób, których dane dotyczą należy te osoby powiadomić o naruszeniu.

7.5. Powiadomienie musi być opracowane prostym i zrozumiałym językiem, w tym nie może być oparte na wypisaniu dotyczących przepisów prawa, lecz musi je w przystępny sposób wyjaśniać.

7.6. Powiadomienie obejmuje informacje o:
   a) danych kontaktowych do ADO, w celu uzyskania informacji o naruszeniu;

b) możliwych konsekwencjach naruszenia, względem osób, których dane dotyczą;
c) podjętych i planowanych środkach zaradczych ograniczających powyższe skutki.

Rejestr incydentów bezpieczeństwa

Incydent / Zdarzenie	Data zakończenia	Opis zdarzenia (uczestnicy, przyczyny, zakres obejmowania)	Działanie korygujące/ zapobiegawcze	Ocena skuteczności	Zgłoszenie do Urzędu Ochrony Danych Osobowych	Zgłoszenie do osób, których dane dotyczą

Procedura zarządzania zmianą

1. Cel procedury

Celem procedury jest opisanie zasad wprowadzania zmian w Starostwie w celu ograniczania negatywnego wpływu na bezpieczeństwo informacji. Procedura pozwala na realizacje zasad ochrony domyślnej „Privacy-by-default" oraz poprawnego projektowania ochrony przetwarzanych danych „Privacy-by-design".

2. Zarządzanie zmianami

2.1. Potrzeba zastosowania zasad zarządzania zmianami może wynikać z:

a) konieczności dostosowania istniejących procesów przetwarzania lub wprowadzenia nowych;
b) zgłoszenia przez pracownika stwierdzonej niedoskonałości SZBI;
c) analizy występujących incydentów wskazującej na istnienie trendów;
d) zmian prawnych;
e) zmian w otoczeniu Starostwa mających wpływ na bezpieczeństwo informacji;
f) znaczących zmian w strukturze organizacyjnej lub zmian wpływających na przyjęty podział obowiązków w ramach SZBI;
g) zmian w zakresie stosowanych zabezpieczeń, wynikających z rozwoju technologicznego i pojawiania się nowych zagrożeń;

2.2. Planowanie wprowadzenia zmian uwzględnia analizę wpływu na bezpieczeństwo informacji.

2.3. Analiza jest przeprowadzana poprzez określenie wszystkich potencjalnych czynników związanych z bezpieczeństwem informacji, jakie mogą być pośrednio lub bezpośrednio związane z wprowadzaną zmianą.

2.4. W szczególności podczas analizowania wpływu należy wziąć pod uwagę:

a) sytuacje powstawania nowych procesów przetwarzania danych osobowych;
b) wykorzystywanie nowych technologii oraz związanych z nimi potencjalnych zagrożeń;
c) zmiany w wykorzystywaniu środków zabezpieczeń informacji, tj. sposoby ich transmisji, miejsca ich przechowywania;
d) doniesienia od innych podmiotów lub z Internetu, dotyczące awaryjności planowanych rozwiązań, np. w zakresie systemów informatycznych lub urządzeń.
e) skalę oraz kontekst przetwarzanych danych, w tym występowanie danych osobowych wrażliwych zgodnie z art. 9 lub 10 RODO.

2.5. W zależności od rodzaju zmian, rozważa się korzystanie ze specjalistów zewnętrznych.

2.6. Planowane zmiany ocenia Kierownik Komórki Organizacyjnej.

2.7. Jeśli wstępna ocena nie wskazuje na żadne, nawet potencjalne ryzyko wpływu na bezpieczeństwo przetwarzanych danych, dalsze konsultacje nie są wymagane.

2.8. Jeśli istnieje potencjalny wpływ na bezpieczeństwo danych osobowych, należy poinformować IOD, w celu przeprowadzenia szczegółowej oceny.

2.9. W przypadku, kiedy zmiany dotyczą rozwiązań informatycznych, w konsultacjach powinien uczestniczyć ASI.

2.10. Do przeprowadzania analizy wpływu można wykorzystać zasady opisane w Procedurze przeprowadzania szacowania ryzyka i oceny skutków, a w szczególności rozważa się korzystanie ze specjalistów zewnętrznych.

2.11. Wdrożone zmiany należy zweryfikować pod kątem założonego poziomu bezpieczeństwa informacji

Procedura realizacji praw osób, których dane dotyczą

1. Cel i zakres dokumentu

Celem procedury jest zdefiniowanie działań, pozwalających na poprawną realizację praw osób, których dane dotyczą.

2. Ogólne zasady realizacji

2.1. Osoba, której dane dotyczą, ma prawo zgłoszenia do Urzędu chęci skorzystania z poniższych praw, przysługujących jej na mocy 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 (nazywanego dalej RODO).

2.2. Informacja o chęci skorzystania z przysługującego prawa (dalej nazywana wnioskowaniem) przyjmuje formę pisemną, wykorzystującą przyjęty wzór wniosku udostępniony przez Starostwo. Wzór wniosku określa **Załącznik nr 1** do niniejszej procedury.

2.3. W przypadkach, kiedy wniosek składany jest bez wykorzystania formularza, o którym mowa w pkt. 2.2 należy ustalić z jakich praw wnioskodawca chce skorzystać.

2.4. Po wpłynięciu wniosku, powinien on zostać zadekretowany oraz przekazany do IOD.

2.5. IOD sporządza kopię wniosku oraz zgodnie z obiegiem dokumentów przekazuje ją do wszystkich komórek organizacyjnych w Starostwie.

2.6. W ramach każdej komórki, Kierownik Komórki Organizacyjnej (dalej KKO) lub wyznaczony pracownik weryfikuje, czy są przetwarzane dane wnioskodawcy, a następnie przygotowuje informacje potrzebne do zrealizowania wniosku w zależności od wnioskowanego prawa.

2.7. Komórki, których wniosek nie dotyczy pisemnie informują o tym IOD, że nie przetwarzają danych wnioskodawcy.

2.8. Komórki organizacyjne, których wniosek dotyczy realizują działania zgodnie z opisem kolejnych punktów niniejszej procedury, jednak nie wysyłają odpowiedzi wnioskodawcy, tylko przekazują ją do IOD.

2.9. Przekazanie wniosku można zrealizować za pośrednictwem służbowej poczty elektronicznej lub tradycyjnie, w zależności od formy złożenia wniosku.

2.10. Po zgromadzeniu danych od komórek organizacyjnych, których wniosek dotyczył, IOD odpowiada osobie, która złożyła wniosek.

3. Prawo dostępu przysługujące osobie, której dane dotyczą (prawo do uzyskania informacji)

3.1. Osoba, której dane osobowe są przetwarzane, ma prawo do uzyskania dostępu oraz uzyskania informacji dotyczących przetwarzania jej danych oraz przysługujących jej praw.

3.2. Jeżeli osoba fizyczna zażąda informacji na temat przetwarzania dotyczących jej danych osobowych, należy udzielić jej informacji, o których mowa w art. 15 ust. 1 i 2 RODO, chyba że udzielenie takich informacji stałoby w sprzeczności z prawem Unii Europejskiej lub

prawem państwa członkowskiego, w szczególności z ustawowym obowiązkiem zachowania tajemnicy.

3.3. Powyższe realizuje się w odpowiedzi na wniosek osoby, w formie wzoru stanowiącego **Załącznik nr 2** do niniejszej procedury.

3.4. Po ustaleniu procesów, w których dane osoby wnioskującej są przetwarzane, należy wypełnić wzór zgodnie z informacjami znajdującymi się w Rejestrze Czynności Przetwarzania.

3.5. Udzielając informacji, w trybie ust. 28 należy przekazać kopię danych osobowych podlegających przetwarzaniu. Za powyższe działania jest odpowiedzialny KKO.

3.6. W związku z powyższym należy przygotować wyciąg informacji o osobie z danego systemu w formie powszechnie możliwej do odczytania. Rodzaj pliku można ustalić z wnioskującym, chyba że znajduje się on na przekazanym wniosku.

3.7. W przypadku powyższego wniosku, gdy przetwarzanie dotyczy formy tradycyjnej możliwe jest przekazanie kopii dokumentów lub przepisanie danych znajdujących się na dokumentach.

3.8. IOD lub wyznaczony pracownik weryfikuje, czy osoba wnioskująca występowała już z wnioskiem o uzyskanie kopii danych. Starostwo posiada prawo do wyznaczenia opłaty za kolejne wnioski dotyczące powyższego prawa.

3.9. Podczas przyznawania dostępu do danych, należy zweryfikować, czy nie zostają udostępnione dane innych osób, co mogłoby powodować naruszenie ochrony danych tych osób.

4. Prawo do sprostowania danych

4.1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych.

4.2. Po otrzymaniu wniosku o realizacje powyższego prawa, wyznaczony pracownik, który odpowiedzialny jest za przetwarzanie danych, na żądanie osoby uzupełnia dane osobowe zgodnie z zakresem wskazanym na wniosku, chyba że żądany zakres danych osobowych nie będzie adekwatny do celów, w których dane są przetwarzane.

5. Prawo do usunięcia danych („prawo do bycia zapomnianym")

5.1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego usunięcia dotyczących jej danych osobowych, a Starostwo ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,

c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,

d) dane osobowe były przetwarzane niezgodnie z prawem,

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego któremu podlega Starostwo,

5.2. Wnioskowanie na podstawie powyższego prawa osoby, której dane dotyczą nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji,
b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa, któremu podlega Starostwo,
c) do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Staroście,
d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych o ile realizacja wniosku uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania,
e) do ustalenia, dochodzenia lub obrony roszczeń,

5.3. Pracownik otrzymujący wniosek do realizacji powyższego prawa jest zobowiązany zweryfikować wstępnie zasadność wniosku względem podpunktów 5.1 od a) do e). Jeśli żaden z elementów nie zachodzi w danym przypadku, wniosek zostaje odrzucony.

5.4. Jeśli wniosek jest zasadny, pracownik weryfikuje występowanie jednego z wyjątków z podpunktów 5.2 od a) do d). Jeśli zachodzi jeden z wyjątków, wniosek zostaje odrzucony.

5.5. Bez względu na to, czy wniosek zostaje odrzucony lub przekazany do realizacji należy poinformować o tym IOD.

5.6. Dane osobowe, osoby wnioskującej, należy usunąć ze wszystkich baz danych w systemach informatycznych, jak również z tradycyjnych nośników.

5.7. Usunięcie informacji elektronicznych może zostać zrealizowane poprzez skasowanie rekordów baz danych, wiadomości elektronicznych lub dokumentów elektronicznych lub nadpisanie tych danych losowymi znakami.

5.8. Rekordy w systemach informatycznych mogą zostać nadpisane z pozostawieniem numeru identyfikacyjnego klienta.

5.9. Po usunięciu danych należy pozostawić informacje o ID rekordu (lub inny identyfikator przypisany do danych osoby) w bazie danych w danym systemie, jeśli konieczne jest zastosowanie zapisów punktu 5.10.

5.10. Dopuszcza się pozostawienie danych osobowych w wykonanych kopiach zapasowych, jednak należy niezwłocznie po odtworzeniu bazy danych z kopii usunąć te dane osobowe przy użyciu pozostawionego numeru klienta. Rozwiązanie należy stosować tylko i wyłącznie, gdy wykonanie wniosku osoby, może negatywnie wpływać na działalnie Starostwa.

6. Prawo do ograniczenia przetwarzania

6.1. Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania w następujących przypadkach:
a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający Urzędowi sprawdzić prawidłowość tych danych;
b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
c) przetwarzanie nie jest potrzebne do założonych celów, ale dane osobowe są potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy występują prawnie uzasadnione podstawy, które są nadrzędne wobec sprzeciwu osoby, której dane dotyczą.

6.2. W przypadku wnioskowania o realizację powyższego prawa, dopuszcza się przetwarzanie danych osobowych jedynie w zakresie przechowywania lub w zakresie weryfikacji zasadności wniosku.

6.3. W przypadku braku zasadności wniosku, uwzględniając opisane wyżej przypadki, należy przekazać taką informację bezpośrednio do IOD.

6.4. Zasadne wnioski należy wykonać poprzez zaprzestanie przetwarzania, za wyjątkiem przechowywania danych. Jeśli zaprzestanie przetwarzania nie jest możliwe, należy zastosować pseudonimizację, tj. przetwarzać dane ograniczone do numeru identyfikacyjnego nie stanowiącego danych osobowych.

6.5. Ograniczenie przetwarzania stosuje się aż do momentu wypełnienia warunków określonych w 6.1.

7. Prawo do przenoszenia danych

7.1. Powyższe prawo nie ma zastosowania w przypadku procesów, w których przetwarzanie jest realizowane w interesie publicznym.

7.2. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła do przetwarzania, oraz ma prawo przesłać te dane osobowe innemu Podmiotowi, jeżeli:

a) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy;

b) przetwarzanie odbywa się w sposób zautomatyzowany.

7.3. Wykonując prawo do przenoszenia danych, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane bezpośrednio do innego Podmiotu, o ile jest to technicznie możliwe.

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

7.5. Pracownik po otrzymaniu wniosku o realizację powyższego prawa, weryfikuje, czy zachodzą podstawy z punktów 7.2 od a) do b).

7.6. Za przetwarzanie zautomatyzowane nie należy uznawać dokumentów tradycyjnych lub dokumentów w wersji elektronicznej – np. skanów w plikach .pdf lub wypełnionych wzorach w plikach .doc.

7.7. Zasadne wnioski są realizowane. W przypadku problemów z eksportem danych, pracownik przekazuje wniosek do ASI w celu wyeksportowania danych w formie pliku .csv lub innej formie wskazanej przez wnioskującego.

7.8. ASI określa możliwość udostępnienia danych z systemu informatycznego, np. poprzez przesłanie w formie zaszyfrowanego pliku pocztą elektroniczną.

8. Prawo do sprzeciwu

8.1. Wniosek o realizacje powyższego prawa należy wykonać z zastrzeżeniem sytuacji, w której istnieją ważne i prawnie uzasadnione podstawy przetwarzania nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

8.2. Innymi sytuacjami ograniczającymi realizacje wyrażonego sprzeciwu są obowiązki wynikające z przepisów prawa.

8.3. Sprzeciw wobec przetwarzania, jeśli jest możliwy do wykonania, skutkuje zastosowaniem Prawa do usunięcia danych.

9. Prawo do niepodlegania profilowaniu

9.1. Zautomatyzowane podejmowanie decyzji lub profilowanie, o którym mowa powyżej nie występuje w procesach realizowanych przez Starostwo, przez co prawo nie ma zastosowania.

9.2. Złożony wniosek należy automatycznie odrzucić.

Wniosek o skorzystanie z praw osób, których dane dotyczą

Dane osoby wnioskującej :

.....
(imię i nazwisko)

.....
(adres zamieszkania)

.....
(PESEL)

Niniejszym wnioskiem, wyrażam chęć skorzystania z przewidzianego przepisami Rozporządzenia UE 2016/679 *:

- ☐ Prawa dostępu do informacji o przetwarzaniu danych, wynikającego z artykułu 15 Rozporządzenia UE 2016/679
- ☐ Prawa do uzyskania kopii danych, wynikającego z artykułu 15 ust. 3 Rozporządzenia UE 2016/679
  - Proszę wybrać format danych*: odt, ods, xls, doc, pdf, csv, wersja papierowa
- ☐ Prawa do sprostowania danych, wynikającego z artykułu 16 Rozporządzenia UE 2016/679
  - Proszę podać dane do aktualizacji: (np. dane kontaktowe, nazwisko, itp.)
- ☐ Prawa do usunięcia danych, wynikającego z artykułu 17 Rozporządzenia UE 2016/679
- ☐ Prawa do ograniczenia przetwarzania, wynikającego z artykułu 18 Rozporządzenia UE 2016/679
  - Proszę podać powód ograniczenia przetwarzania: .....
- ☐ Prawa do przenoszenia danych, wynikającego z artykułu 20 Rozporządzenia UE 2016/679
- ☐ Prawa sprzeciwu, wynikającego z artykułu 21 Rozporządzenia UE 2016/679
- ☐ Prawa do niepodlegania pod decyzje oparte na zautomatyzowanym przetwarzaniu, wynikającego z artykułu 22 Rozporządzenia UE 2016/679

Rozumiem, że na potrzeby rozpatrzenia wniosku i jego dalszej realizacji może być wymagane podanie dodatkowych danych mnie identyfikujących.

*niepotrzebne należy wykasować (w przypadku wersji elektronicznej) lub skreślić (w przypadku wersji papierowej)

Informacja o przetwarzaniu danych osobowych

W odpowiedzi na Pana/i wniosek przekazujemy informacje dotyczące przetwarzania danych osobowych, zgodnie z artykułem 15 Rozporządzeniu UE 2016/679:

1. **Cele przetwarzania danych osobowych:** .....
2. **Kategorie odnośnych danych osobowych:** .....
3. **Informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione:** .....
4. **Informacje o odbiorcach w państwach trzecich lub organizacjach międzynarodowych:** .....
5. **Planowany okres przechowywania danych osobowych lub kryteria ustalania tego okresu:** .....
6. **Źródło pozyskania danych:** .....
7. **Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu:** W ramach przetwarzania danych nie występuje zautomatyzowane podejmowanie decyzji ani profilowanie.

Informujemy jednocześnie, że przysługują Państwu prawa przewidziane w Rozporządzeniu UE 679/2016 w artykułach 15 – 21, w tym prawo do żądania sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz prawo do wniesienia sprzeciwu wobec takiego przetwarzania. Przysługuje Państwo prawo do wniesienia skargi do Urzędu Ochrony Danych Osobowych.

.....
(data, podpis osoby odpowiedzialnej za powyższe informacje)

Instrukcja zarządzania systemem informatycznym

1. Cel i zakres dokumentu

Instrukcja dotyczy zabezpieczania informacji przetwarzanych w systemach informatycznych oraz informacji w formie elektronicznej. Instrukcja jest stosowana w Starostwie przez wszystkie osoby przetwarzające dane osobowe.

2. Zarządzanie dostępem użytkowników

2.1. Nadawanie uprawnień w systemach informatycznych realizują ASI.

2.2. Przydzielenie uprawnień użytkownikowi do zasobów sieci wewnętrznej oraz do systemów informatycznych realizuje ASI na podstawie wniosku od KKO – Załącznik nr 7 do Polityki bezpieczeństwa danych osobowych, oraz formularza określającego uprawnienia użytkownika.

2.3. W przypadku gdy osoba ma uzyskać dostęp do systemów zarządzanych przez różnych administratorów, zgłoszenie o nadanie uprawnień dokonuje się do każdego z nich.

2.4. ASI przed przydzieleniem dostępu sprawdza u IOD czy dana osoba ma upoważnienie do przetwarzania danych osobowych, chyba że dane uprawnienie nie jest związane z przetwarzaniem danych osobowych.

2.5. ASI nadaje zakres uprawnień odpowiedni do zajmowanego przez nowego użytkownika stanowiska, a w razie potrzeb potwierdza ten zakres z KKO.

2.6. Nadanie uprawnień w systemie informatycznym może zostać zrealizowane wyłącznie, gdy osoba posiada pisemne upoważnienie do przetwarzania danych osobowych w Starostwie.

2.7. ASI, który nadał uprawnienia w podlegającym mu systemie, przekazuje informacje do IOD o:

a) Nazwach systemów informatycznych;
b) Datach nadania uprawnień w systemach;
c) Nazwach przydzielonych loginów;
d) Zakresach uprawnień w systemach, np. profilach lub możliwych działań – odczyt, modyfikacja, usuwanie.

2.8. Natychmiast po utracie podstawy do posiadanych uprawnień, będącego wynikiem np. zmiany stanowiska lub zwolnienia z pracy, uprawnienia podlegają niezwłocznej aktualizacji lub zlikwidowania dostępu.

2.9. Podniesione uprawnienia, np. administracyjne, muszą być ściśle ograniczone do osób, które bezpośrednio odpowiadają za administrację poszczególnych systemów informatycznych i ich bezpieczeństwo.

3. Stosowane metody i środki uwierzytelnienia

3.1. Metoda uwierzytelnienia polega na ograniczeniu dostępu do poszczególnych systemów informatycznych poprzez konieczność podania informacji uwierzytelniających, tj. loginu oraz hasła.

3.2. Login jest niepowtarzalny dla każdego użytkownika systemu informatycznego.

3.3. Hasła użytkowników systemu informatycznego mają długość minimum 8 znaków i muszą zawierać przynajmniej jedną małą, jedną dużą literę, jedną cyfrę oraz znak specjalny. Zalecaną długością hasła jest 12 znaków.

3.4. W celu pierwszego logowania użytkownik systemu informatycznego posługuje się hasłem tymczasowym lub hasło jest ustanawiane przy pierwszym logowaniu. Niezależnie, każdy użytkownik jest zobowiązany do zmiany hasła tymczasowego oraz ustanowienia własnego hasła spełniającego wyżej wymienione wymogi.

3.5. Użytkownik systemu informatycznego zachowuje hasło w tajemnicy w czasie jego obowiązywania oraz po ustaniu jego ważności.

3.6. Zabronione jest zapisywanie haseł do systemów informatycznych, zaszyfrowanych informacji lub innych haseł dostępowych wykorzystywanych przez osoby uprawnione i przechowywanie tych haseł w obrębie stanowiska, w tym również w postaci elektronicznej, niezaszyfrowanej.

3.7. Hasła użytkowników w systemach informatycznych zmienia się nie rzadziej niż co 30 dni. Za okresową zmianę haseł odpowiedzialni są użytkownicy systemów informatycznych.

3.8. Hasła do kont administracyjnych podlegają zabezpieczeniu poprzez ich spisanie oraz umieszczenie w zamkniętej kopercie dostępnej dla Administratora Danych Osobowych. Konta administracyjne dotyczą eksploatowanych systemów informatycznych oraz urządzeń sieciowych.

4. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

4.1. Podczas rozpoczęcia pracy użytkownik powinien:

a) Zweryfikować stan stosowanych zabezpieczeń, a podejrzenia naruszeń zgłosić zgodnie z Procedurą zarządzania incydentami.

b) Włączyć komputer, zalogować się do systemu operacyjnego poprzez podanie loginu i hasła.

c) Zweryfikować uruchomienie się systemu antywirusowego.

d) Zalogować się do systemu informatycznego, do którego użytkownik ma uprawnienia.

4.2. Podczas zawieszania pracy, użytkownik powinien:

a) Zablokować stacje roboczą poprzez kombinacje klawiszy (Windows + L).

4.3. Podczas zakończenia pracy, użytkownik powinien:

a) Wylogować się z systemów informatycznych.

b) Zamknąć system operacyjny oraz wyłączyć komputer.

c) Wyłączyć listwy zasilające oraz urządzenia peryferyjne.

d) Zabezpieczyć dokumentację i nośniki wymienne zawierające informacje objęte ochroną do zamykanych szaf i szuflad lub archiwów.

e) Zamknąć okna oraz drzwi i przekazać klucz w ustalone wewnętrznie miejsce.

5. Zarządzanie kopiami zapasowymi

5.1. W Starostwie zastosowano wirtualizację maszyn serwerowych.

5.2. Kopie zapasowe baz danych oraz systemów informatycznych są tworzone codziennie za pomocą rozwiązań programowych Xopero.

5.3. Kopie są tworzone na macierz dyskową serwera.

5.4. Procesem tworzenia kopii zarządza ASI, który posiada szczegółowy harmonogram kopii.

5.5. Harmonogram kopii musi zapewniać minimalizacje ilości utraconych danych w przypadku zdarzenia awaryjnego powodującego utracenie bazy danych systemu.

5.6. Dodatkowe kopie bezpieczeństwa są wykonywane na dysk zewnętrzny, w szczególności dotyczy się to baz danych, tj. EWOPIS, EWMAPA, REJCEN, OŚRODEK. Przy czym kwartalnie tworzone są kopie przyrostowe, a raz w tygodniu pełne kopie baz danych.

5.7. Kopie o których mowa w punkcie poprzednim przechowuje się w oddalonej od siedziby Starostwa lokalizacji, tj. Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej w Nidzicy przy ul. Olsztyńskiej 28.

5.8. Dysk zewnętrzny USB, na który wykonywane są kopie zapasowe musi zostać odłączony na czas nieużywania oraz powinien podlegać szyfrowaniu.

5.9. Okresowo należy przeprowadzać weryfikację poprawności utworzonych kopii oraz sprawdzać pod kątem ich przydatność do odtworzenia w przypadku awarii systemu. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza ASI.

6. Zarządzanie nośnikami wymiennymi

6.1. Czytniki nośników wymiennych, tj. pendrive, dysk zewnętrzny, płyty optyczne, są możliwe do wykorzystywania, ze względu na brak blokowania.

6.2. Zabronione jest korzystanie z obcych pendrive'ów, np. znalezionych na terenie Starostwa. Pracownicy nie powinni również wykorzystywać nośników prywatnych.

6.3. Kopiowanie informacji objętych ochroną na nośniki wymienne powinno być realizowane tylko i wyłącznie w uzasadnionych przypadkach. Dopuszczalnymi sytuacjami są np. tymczasowe kopie realizowane w związku z naprawą sprzętu lub przenoszenie danych pomiędzy komputerami. W każdym przypadku należy zapewnić niezwłoczne usunięcie danych.

6.4. Każdy nośnik zawierający informacje objęte ochroną, który opuszcza obszar przetwarzania musi zostać objęty szyfrowaniem. Szyfrowanie odbywa się przy użyciu metod wymienionych w punkcie 12.

7. Sposób zabezpieczenia systemu informatycznego przed szkodliwym oprogramowaniem

7.1. W systemach operacyjnych zainstalowano oprogramowanie antywirusowe.

7.2. Niezależnie od sposobu zabezpieczenia przed edycją ustawień oprogramowania antywirusowego, użytkowników obowiązuje zakaz ingerencji w konfiguracje oprogramowania antywirusowego.

7.3. Oprogramowanie antywirusowe jest zabezpieczone przed zmianą konfiguracji ze względu na ograniczony poziom uprawnień użytkowników.

7.4. Użytkownikom nie wolno samodzielnie instalować programów w systemach operacyjnych, niezwiązanych z pracą, w tym też programów darmowych. Potrzeba nowego oprogramowania powinna zostać zatwierdzona przez przełożonego oraz ASI.

7.5. Użytkownikom nie wolno wgrywać oraz pobierać plików niezwiązanych z realizacją obowiązków służbowych.

7.6. W przypadku stwierdzenia pojawienia się szkodliwego oprogramowania, każdy użytkownik powinien niezwłocznie powiadomić o tym fakcie ASI lub przełożonego.

7.7. Zasady dotyczące zarządzania nośnikami wymiennymi, korzystania z poczty elektronicznej i Internetu oraz ochrony sprzętu i oprogramowania również ograniczają ryzyka związane ze szkodliwym oprogramowaniem.

7.8. Oprogramowanie eksploatowane w Starostwie jest regularnie aktualizowane. Dotyczy to również mniej istotnego oprogramowania oraz firmware'ów na urządzeniach sieciowych.

7.9. Użytkownik powinien zgłaszać aktualizacje nie mogące się zainstalować lub informujące o błędzie.

8. Rejestrowanie działań użytkowników i monitorowanie

8.1. Działania użytkowników podlegają rejestrowaniu w logach eksploatowanych systemów informatycznych.

8.2. Gromadzone logi obejmują logowanie się użytkownika do systemu informatycznego oraz uzyskanie dostępu do poszczególnych informacji lub zakresie wykonywanych zmian w ramach tego systemu.

8.3. Przegląd logów dotyczących funkcjonowania systemów informatycznych oraz sieci Starostwa jest realizowany w razie potrzeb przez ASI.

8.4. Logi systemów przetwarzających dane osobowe podlegają przeglądom w przypadku podejrzenia naruszeń lub wadliwego działania systemu.

9. Procedury wykonywania przeglądów i konserwacji oraz zasady wycofywania sprzętu

9.1. Sprzęt podlega przeglądowi i pracom konserwacyjnym, w przypadku zgłoszeń od użytkowników oraz w ramach zaplanowanych działań.

9.2. Przeglądy w zależności od zdarzenia obejmują czyszczenie fizyczne, przegląd oprogramowania lub dodatkowe prace serwisowe, tj. wymianę past przewodzących.

9.3. Podczas zewnętrznych prac serwisowych, prowadzony jest nadzór ASI lub osoby upoważnionej przez wyznaczonego pracownika. Nadzór nie jest wymagany, jeśli nie ma możliwości uzyskania dostępu do informacji lub zawarto umowę, o której mowa w następnym punkcie.

9.4. Prace serwisowe prowadzone na zewnątrz organizacji są realizowane po usunięciu dysków twardych z komputera. Jeśli nie jest to możliwe do wykonania, na prace serwisowe zawierana jest umowa zgodnie z Zasadami powierzania danych osobowych opisanymi w Polityce Bezpieczeństwa danych osobowych.

9.5. Sprzęt przeznaczony do utylizacji zostaje pozbawiony dysków twardych. Wykręcone dyski są składowane przez ASI oraz podlegają zabezpieczeniu do czasu ich zbiorczego zniszczenia. Dyski niszczone są w sposób fizyczny lub przekazywane do wyspecjalizowanych podmiotów zewnętrznych.

9.6. Jeśli to możliwe, dysk przed przechowaniem zostaje sformatowany.

9.7. Dyski z danymi nie mogą być przechowywane bezterminowo.

10. Ochrona sprzętu i oprogramowania

10.1. Sprzęt komputerowy używany w Starostwie powinien być fizycznie chroniony przed kradzieżą, zniszczeniem lub niewłaściwym używaniem. Bezpośrednio odpowiedzialny za to jest w czasie pracy użytkownik tego sprzętu.

10.2. Użytkownicy nie mogą sami demontować podzespołów jednostek centralnych zestawów komputerowych (dyski, procesory, pamięci operacyjne, karty sieciowe, karty graficzne, itp.). Wykonuje to tylko ASI lub inne uprawnione osoby.

10.3. Sprzęt komputerowy używany w systemie informatycznym nie może być przekazywany między komórkami organizacyjnymi bez wiedzy ASI.

10.4. Każde urządzenie używane w systemie informatycznym musi być oznaczone w celu jego identyfikacji.

10.5. Inwentaryzacji sprzętu komputerowego i oprogramowania dokonuje ASI, który okresowo kontroluje stan poszczególnych stanowisk komputerowych oraz środków trwałych.

10.6. Ewidencja sprzętu komputerowego i oprogramowania jest prowadzona w wersji papierowej oraz elektronicznie, w programie komputerowym Ewida Standard.

10.7. Wszystkie stacje robocze pracujące w systemie informatycznym muszą być zgodne ze sprzętową oraz programową konfiguracją zalecaną przez ASI.

10.8. W systemie informatycznym może być używane wyłącznie oprogramowanie licencjonowane przez posiadacza praw autorskich. Oprogramowanie może być używane tylko zgodnie z prawami licencji.

10.9. Użytkownikom nie wolno samodzielnie instalować programów ani podejmować prób instalacji.
10.10. Zabronione jest wykorzystywanie programów w wersji bezinstalacyjnej.

11. Praca zdalna oraz zarządzanie urządzeniami mobilnymi

11.1. Pracownicy, którym powierzono sprzęt mobilny, są uprawnieni do wynoszenia go poza obszar przetwarzania, jeśli jest to uzasadnione wykonywanymi obowiązkami. W innych przypadkach lub kiedy wynoszenie ma charakter sporadyczny należy poinformować o tym fakcie przełożonego lub ASI.

11.2. Urządzenia mobilne są wyposażone w mechanizmy szyfrujące, jeśli występuje na nich przetwarzanie informacji. Szyfrowanie dysków jest realizowane przez funkcje systemu operacyjnego, dedykowane rozwiązania producenta sprzętu lub zewnętrzne programy.

11.3. W zależności od wykorzystywanego rozwiązania, użytkownik urządzenia przenośnego może być zobowiązany do wykonania dwustopniowego logowania. W przypadku logowania dwustopniowego, oba hasła muszą spełniać wymagania opisane w niniejszej Instrukcji. Zmiana hasła do odszyfrowania nie jest konieczna co 30 dni – jednak dopuszczalne jest wykorzystywanie jednego hasła do obu logowań.

11.4. Pracownik jest zobowiązany do zapewnienia odpowiedniej ochrony fizycznej sprzętu mobilnego, w szczególności poprzez niepozostawianie go bez nadzoru oraz bezpieczny transport i eksploatację z uwagą na czynniki środowiskowe, tj. zalanie lub przegrzanie.

11.5. Komunikacja z siecią wewnętrzną nie jest realizowana przez użytkowników. Wyjątki mogą stanowić wyłącznie sytuacje nadzoru autorskiego realizowanego przez zdalny pulpit lub dedykowane połączenie, dostępne jedynie na czas nadzoru.

11.6. Obowiązuje zakaz ustawiania dostępów zdalnych do sieci wewnętrznej bez wiedzy ASI.

11.7. Wykonując pracę poza miejscem przetwarzania, użytkownik powinien ograniczać ryzyko wglądu w wyświetlane informacje osobom nieupoważnionym.

11.8. Dostęp do sprzętu mobilnego powinna mieć jedynie uprawniona osoba. Obowiązuje zakaz dopuszczania osób trzecich do sprzętu komputerowego.

12. Zabezpieczenia kryptograficzne

12.1. Szyfrowanie danych jest stosowane jako dodatkowe zabezpieczenie informacji objętych ochroną.

12.2. Szyfrowanie jest wykorzystywane na urządzeniach mobilnych oraz na nośnikach wymiennych zawierających informacje objęte ochroną.

12.3. Hasła wykorzystywane do szyfrowania muszą spełniać wymogi złożoności wskazane w niniejszej Instrukcji.

12.4. Komunikacja zewnętrzna jest szyfrowana poprzez zastosowanie protokołu SSL lub HTTPS w poczcie elektronicznej.

12.5. Szyfrowanie plików realizuje się poprzez programy do archiwizacji lub dedykowane programy szyfrujące.

13. Zasady korzystania z Internetu oraz poczty elektronicznej

13.1. Przed wysłaniem wiadomości zawierającej informacje objęte ochroną, należy się upewnić, że podmiot odbierający jest do nich uprawiony. Uprawnienie może wynikać z upoważnienia, zawartej umowy lub porozumienia lub z przepisów prawa.

13.2. Wysyłając wiadomości elektroniczne należy sprawdzić poprawność wprowadzonego adresu mailowego oraz załączonych plików.

13.3. Weryfikacja wysyłanych treści oraz adresatów dotyczy również innych kanałów komunikacji. W szczególności w przypadku faxu, należy zweryfikować obecność osoby odbierającej przy urządzeniu.

13.4. W przypadku przesyłania informacji objętych ochroną na ogólne skrzynki pocztowe lub na zewnętrzne udziały sieciowe, chmury lub przesyłania danych wrażliwych należy zastosować dodatkową ochronę kryptograficzną, tj. szyfrowanie plików oraz ich przesyłanie jako załączników.

13.5. Szyfrowanie załączanych plików dokonuje się poprzez ich spakowanie w archiwum oraz ustalenie hasła, np. w programie 7-zip. Hasło do archiwum powinno być przesyłane inną drogą niż zaszyfrowane archiwum.

13.6. Wiadomości przychodzące należy zweryfikować poprzez:

a) weryfikację adresu mailowego nadawcy;
b) analizę treści pod kątem prób wyłudzeń informacji;
c) poprawność załączonych w treści linków – przed kliknięciem, poprzez zawieszenie kursora nad linkiem i weryfikacje wyświetlonego adresu;
d) obecność szyfrowanych załączników – w szczególności faktur;
e) obecność plików wykonywalnych w załącznikach.

13.7. Należy unikać podłączania się do sieci udostępnianej publicznie za pośrednictwem ogólnodostępnych hotspotów Wi-Fi.

13.8. Dostępność stron internetowych może być ograniczona przez stosowane urządzenia sieciowe oraz może podlegać monitorowaniu.

13.9. Nie należy odwiedzać stron o treściach naruszających przepisy prawa.

13.10. Użytkownikom nie wolno pobierać plików niezwiązanych z realizacją obowiązków służbowych.

13.11. Należy zwrócić szczególną uwagę na adres stron internetowej przed podaniem danych do logowania lub przez wypełnianiem formularzy dotyczących danych osobowych. Strona internetowa powinna zapewniać szyfrowaną komunikację protokołem HTTPS.

Procedura przeprowadzania szacowania ryzyka i oceny skutków

1. Cel procedury

Celem procedury jest opisanie zasad przeprowadzania szacowania ryzyka utraty bezpieczeństwa informacji na podstawie normy PN-ISO/IEC 27005:2014 oraz przeprowadzania oceny skutków dla danych osobowych.

2. Szacowanie ryzyka

2.1. Szacowanie ryzyka utraty bezpieczeństwa informacji, przeprowadzane w związku z wprowadzaną zmianą, obejmuje:

a) określenie aktywów objętych planowaną zmianą;
b) określenie zagrożeń oraz podatności dla powyższych aktywów;
c) określenie prawdopodobieństw oraz skutków wystąpienia zagrożeń.

2.2. Powyższa analiza stanowi szacowanie ryzyka utraty bezpieczeństwa informacji, w oparciu o normę PN-ISO/IEC 27005:2014. Szacowanie przeprowadzane jest metodą jakościową z przypisaniem wartości:

a) „z" od 1 – 5 dla zagrożeń;
b) „p" od 1 – 5 dla prawdopodobieństw;

2.3. Dla prawdopodobieństw przyjmuje się poniższą skalę:

a) Nieprawdopodobne – 1
b) Mało prawdopodobne – 2
c) Prawdopodobne – 3
d) Bardzo prawdopodobne – 4
e) Prawie pewne – 5

2.4. Dla zagrożeń przyjmuje się poniższą skalę:

a) Znikome starty finansowe i brak konsekwencji prawnych – 1
b) Straty finansowe i brak konsekwencji prawnych – 2
c) Straty finansowe lub możliwe konsekwencje prawne – 3
d) Znaczne starty finansowe lub konsekwencje prawne – 4
e) Znaczne naruszenie przepisów prawa – 5

2.5. Wynikiem przeprowadzonego szacowania dla danej grupy aktywów jest wynik mnożenia z*p z wartościami od 1 do 25.

2.6. Szacowanie przeprowadza Inspektor Ochrony Danych.

2.7. W przypadku wskazania wysokiego ryzyka przy dużym prawdopodobieństwie wystąpienia zagrożenia (oznacza to wyniki szacowania w przedziale 20-25) należy przeprowadzić ocenę skutków naruszenia bezpieczeństwa danych osobowych, zgodnie z opisem pkt 3.

2.8. Ocenę skutków przeprowadza się określając skutki wystąpienia zagrożenia wskazanego w szacowaniu ryzyka. Do oceny skutków należy wziąć pod uwagę takie czynniki jak motywy osób naruszających bezpieczeństwo informacji, możliwości wykorzystania danych osobowych, w tym ich sprzedaży lub zaciągnięcia zobowiązań finansowych oraz prawdopodobieństwo wykorzystania danych do przejęcia kont bankowych, itp.

2.9. Wyniki szacowania ryzyka pozwalają podjąć decyzję zgodnie z czterema wariantami postępowania z ryzykiem:
   a) redukowanie ryzyka - poprzez wdrażanie dodatkowych lub rozszerzanie obecnych zabezpieczeń;
   b) akceptowanie ryzyka – niepodejmowanie innych działań ze względu na wystarczająco niski poziom ryzyka lub nieadekwatność kosztów potrzebnych zabezpieczeń;
   c) unikanie ryzyka – rezygnacja z aktywów generujących dane ryzyko;
   d) transfer ryzyka – przeniesienie odpowiedzialności na inny podmiot np. poprzez wykupienie ubezpieczenia od szkód;

2.10. Proces szacowania ryzyka jest przeglądany regularnie, zaś przeprowadzanie szacowania powinno się odbywać każdorazowo przy zmianach w zakresie procesów przetwarzania.

2.11. Wymagane jest udokumentowanie każdego procesu szacowania ryzyka lub jego przeglądu, oraz udokumentowanie decyzji dotyczących postępowania z tym ryzkiem.

2.12. Jeśli dokonany przegląd wskazuje na zmiany w wysokości ryzyka należy zweryfikować konieczność przeprowadzenia oceny skutków.

2.13. Wyniki szacowania zostają udokumentowane zgodnie z **Załącznikiem nr 1** do niniejszej procedury.

2.14. W ramach podsumowania przeglądu i podjętych działań należy udokumentować planowane działania i ocenić stopień ich realizacji oraz wskazać na zmiany względem wcześniejszego szacowania ryzyka.

3. Ocena skutków naruszeń

3.1. Ocenę skutków przeprowadza się określając skutki wystąpienia zagrożenia wskazanego w szacowaniu ryzyka, z perspektywy osób, których dane dotyczą.

3.2. Do oceny skutków należy wziąć pod uwagę takie czynniki jak:
   a) motywy osób naruszających bezpieczeństwo informacji;
   b) możliwości wykorzystania danych osobowych w celach marketingowych;
   c) możliwości wykorzystania danych osobowych w celu nękania lub zastraszania osoby, wykorzystując pozyskane dane zwłaszcza w zakresie danych finansowych oraz danych wrażliwych;
   d) możliwości wykorzystania danych osobowych w celu szykanowania lub wykluczenia społecznego, zwłaszcza ze względu na naruszenie danych wrażliwych;
   e) możliwości wykorzystania danych osobowych w celu zaciągnięcia zobowiązań finansowych;
   f) możliwości wykorzystania danych osobowych do przejęcia kont bankowych lub kont portali internetowych, a w szczególności kont poczty elektronicznej ze względu na ich potencjalne powiązane z innymi kontami internetowymi;
   g) możliwość naruszenia prawa do prywatności lub naruszenia ochrony dóbr osobistych;

3.3. Ocena skutków jest wymagana niezależnie od wyników szacowania, w przypadkach:
   a) kiedy w procesach przetwarzania użyto nowych technologii;
   b) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu i jest podstawą decyzji wywołujących skutki prawne lub w podobny sposób znacząco wpływających na osobę fizyczną;
   c) przetwarzania na dużą skalę danych „wrażliwych";
   d) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

e) procesów przetwarzania wskazanych przez Prezesa Urzędu Ochrony Danych Osobowych;

3.4. Możliwe jest przeprowadzenie pojedynczej oceny skutków dla podobnych procesów przetwarzania danych wiążących się z podobnym wysokim ryzykiem.

3.5. Za podobne procesy przetwarzania można uznać procesy, w których:

a) dane są przetwarzane przy wykorzystaniu podobnych aktywów, tj. systemów informatycznych, komputerów lub nośników;

b) dane są przetwarzane w tej samej formie, tj. elektronicznej lub tradycyjnej;

c) przetwarzane są podobne kategorie danych, np. dane kontaktowe, dane finansowe, dane wrażliwe;

d) dane są przekazywane do podobnych odbiorców danych;

e) dane nie różnią się w stopniu ochrony narzucanej przepisami prawa, w zakresie bezpieczeństwa informacji;

3.6. Ocena skutków zawiera co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania;

b) ocenę czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;

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

d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Załącznik nr 1 do Procedury przeprowadzania szacowania ryzyka i oceny s

Data przeprowadzenia pełnego szacowania ryzyka:		
Rodzaj	Przykłady podatności	Prawdopodobieństwo
Oprogramowanie	Błędne przypisanie praw dostępu	
Oprogramowanie	Brak wylogowania przy opuszczaniu stacji roboczej	
Oprogramowanie	Brak śladu audytowego lub brak jego przeglądów	
Oprogramowanie	Niekontrolowane ściąganie i użytkowanie oprogramowania	
Organizacja	Brak odpowiedzialności związanej z bezpieczeństwem informacji	
Organizacja	Brak lub niewystarczająca polityka czystego biurka i czystego ekranu	
Organizacja	Brak regularnych audytów (nadzór)	
Organizacja	Brak formalnej procedury rejestrowania i wyrejestrowywania użytkownika	
Organizacja	Brak lub niewystarczające zapisy (odnoszące się do bezpieczeństwa) w umowach z klientami i/lub stronami trzecimi	
Organizacja	Pozbywanie się lub ponowne używanie nośników bez właściwego wykasowania informacji	
Organizacja	Brak lub niewystarczające zapisy, odnoszące się do bezpieczeństwa informacji, z pracownikami	
Organizacja	Brak procedur zapewniających zgodność z prawem własności intelektualnej	
Organizacja	Brak formalnej procedury nadzoru nad dokumentacją SZBI	
Personel	Brak świadomości w zakresie bezpieczeństwa	
Personel	Praca personelu zewnętrznego lub sprzątającego bez nadzoru	
Personel	Brak polityk w zakresie poprawnego użytkowania środków telekomunikacyjnych	
Sieć	Błędna konfiguracja urządzeń sieciowych	
Sieć	Niezabezpieczone połączenia z siecią publiczną	
Siedziba	Brak fizycznej ochrony budynków, drzwi i okien	
Siedziba	Nieodpowiednie lub niestaranne użytkowanie fizycznej kontroli dostępu do budynków i pomieszczeń	

Sprzęt	Niezabezpieczone urządzenia mobilne poza siedzibą	
Sprzęt	Niekontrolowane kopiowanie	
Sprzęt	Niezabezpieczone urządzenia do przechowywania danych	
Organizacja	Niedostateczne środki ochrony środowiskowej	
Sieć	Brak szyfrowanej komunikacji i wymiany danych	
Sprzęt	Wrażliwość na zmiany napięcia zasilania	
Sprzęt	Brak planów okresowej wymiany	

Przegląd wyników szacowania ryzyka		
Wykonał:		Data:

Podsumowanie przeglądu i podjętych działań:

skutków

Przykłady zagrożeń	Skutek	Wynik	Plan postępowania
Nadużycie praw		0	
Nadużycie praw		0	
Nadużycie praw		0	
Sfałszowanie oprogramowania		0	
Błąd użytkowania		0	
Kradzież nośników lub dokumentów		0	
Nadużycie praw		0	
Nadużycie praw		0	
Nadużycie praw		0	
Nieautoryzowane użycie urządzeń		0	
Nielegalne przetwarzanie danych		0	
Użycie fałszywego lub skopiowanego oprogramowania		0	
Zniekształcenie danych		0	
Błąd użytkowania		0	
Kradzież nośników lub dokumentów		0	
Błąd użytkowania		0	
Nieautoryzowany dostęp do danych		0	
Nieautoryzowany dostęp do danych		0	
Kradzież nośników lub dokumentów		0	
Kradzież nośników lub dokumentów		0	

Nieautoryzowany dostęp do danych		0	
Kradzież nośników lub dokumentów		0	
Kradzież nośników lub dokumentów		0	
Wilgoć, pożar		0	
Nieautoryzowany dostęp do danych		0	
Utrata zasilania		0	
Zniszczenie urządzeń lub nośników		0	

Szczegóły planu	Status wykonania planu (data wykonania)	Informacje o zmianach w ramach przeglądu