……………………………………

pieczęć Jednostki

**System zarządzania bezpieczeństwem informacji**

......……..…………........., dnia,...............................

(miejsce)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| OPRACOWAŁ |  |  |  |  |
| SPRAWDZIŁ |  |  |  |  |
| ZATWIERDZIŁ |  |  |  |  |
|  | Imię i Nazwisko | Komórka organizacyjna | Data | Podpis |

**SPIS TREŚCI**

[WYKAZ ZMIAN 3](#_Toc1736223)

[1. System zarządzania bezpieczeństwem informacji 4](#_Toc1736224)

[1.1. CEL 4](#_Toc1736225)

[1.2. ZAKRES 4](#_Toc1736226)

[1.3. TERMINOLOGIA 5](#_Toc1736227)

[1.4. OPIS DZIAŁANIA 11](#_Toc1736293)

[1.4.1. Polityka bezpieczeństwa ochrony danych 11](#_Toc1736294)

[1.4.2. Instrukcja zarządzania systemem informatycznym. 11](#_Toc1736306)

[1.4.3. Krajowe Ramy Interoperacyjności. 11](#_Toc1736307)

[1.5. ODPOWIEDZIALNOŚĆ I UPRAWNIENIA 11](#_Toc1736308)

[1.6. DOKUMENTY ZWIĄZANE 12](#_Toc1736309)

[1.7. ZAŁĄCZNIKI 12](#_Toc1736310)

# WYKAZ ZMIAN

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wprowadzona zmiana | Data | Imię i Nazwisko, podpis |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# System zarządzania bezpieczeństwem informacji

SPIS TREŚCI

* CEL
* ZAKRES
* TERMINOLOGIA
* OPIS DZIAŁANIA
* ODPOWIEDZIALNOŚĆ I UPRAWNIENIA
* DOKUMENTY ZWIĄZANE
* ZAŁĄCZNIKI

## CEL

Celem Systemu zarządzania bezpieczeństwem informacji jest zapewnienie pełnej poufności chronionych danych osobowych przez brak (w całym roku) incydentów związanych z umyślnym lub nieumyślnym ujawnieniem danych osobowych osobom nieupoważnionym, rozliczalności oraz integralności danych osobowych.

Lista celów, o których mowa wyżej, może być modyfikowana podczas przeglądów zarządzania systemem. Wtedy także powinno się ocenić realizację celów ustalonych lub potwierdzonych na poprzednim przeglądzie.

## ZAKRES

Niniejszy dokument jest zbiorem zasad, procedur i odniesień do rozproszonych wewnątrz organizacji procedur i instrukcji.

Niniejszy dokument spełnia wymogi 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. Urz. UE L 119, s.1) – zwanego dalej RODO.

Opisane w niniejszym dokumencie procedury i zabezpieczenia mają zapewnić:

* poufność informacji – rozumianą jako właściwość zapewniającą, że informacja nie jest udostępniana nieupoważnionym osobom,
* integralność informacji – rozumianą jako właściwość zapewniającą, że informacja nie jest zmieniana lub niszczona w sposób nieautoryzowany,
* dostępność informacji – rozumianą jako właściwość zapewniającą, że dla upoważnionych osób informacja jest dostępna, gdy jest potrzebna,
* rozliczalność – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
* integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

## TERMINOLOGIA

### **Administrator danych (ADO) -** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania (art. 4 pkt 7 RODO);

### **Administrator Systemu Informatycznego (ASI)–** oznacza osobę lub osoby, upoważnione przez ADO do administrowania i zarządzania systemami informatycznymi;

### **Aktywa –** jest to wszystko co stanowi jakąś wartość dla jednostki i pomaga w osiągnięciu jej celów (np. wiedza know-how, pracownicy, lokalizacja, dane, licencje, infrastruktura);

### **Audyt** – systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny, w celu określenia stopnia spełnienia kryteriów audytu. Audyt jest efektywnym i wiarygodnym narzędziem wspierającym politykę i funkcję nadzorowania zarządzania, dostarcza informacji na podstawie, których organizacja może doskonalić swoje wyniki działania;

### **Audytor** – osoba mająca kompetencje do przeprowadzania audytów;

### **Audytowany** – organizacja, która jest audytowana;

### **Bezpieczeństwo danych osobowych -** zachowanie poufności, integralności i dostępności danych osobowych (art. 32 ust. 1 RODO);

### **Dane osobowe -** informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); 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 (art. 4 pkt 11 RODO);

### **Dokument** – informacja i jej nośnik;

### **Dowód z audytu** – zapisy, stwierdzenia faktu lub inne informacje, które są istotne dla kryteriów audytu i możliwe do zweryfikowania;

### **Europejski Obszar Gospodarczy (EOG)** – strefa wolnego handlu i wspólny rynek, obejmujące państwa Unii Europejskiej i Europejskiego Stowarzyszenia Wolnego Handlu, z wyjątkiem Szwajcarii. EOG opiera się na czterech fundamentalnych wolnościach: swobodzie przepływu ludzi, kapitału, towarów i usług;

### **Funkcja** – zbiór zadań zawodowych, czynności do wykonywania;

### **Hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

### **Identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

### **Incydent -** zdarzenie lub seria powiązanych ze sobą zdarzeń, które skutkują lub mogą skutkować naruszeniem ochrony danych osobowych;

### **Informacja** – znaczące dane;

### **Inspektor Ochrony Danych (IOD)** – osoba, którą może wyznaczyć ADO na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO;

### **Instrukcja** – dokument szczegółowo opisujący sposób działania lub procesu opisanego w procedurze.

### **Integralność** - właściwość polegająca na zapewnieniu dokładności i kompletności;

### **Kontrola dostępu** - środki mające na celu zapewnienie, że dostęp do aktywów jest autoryzowany i ograniczony w oparciu o wymagania biznesowe i wymagania bezpieczeństwa;

### **Kryteria audytu** – zestaw polityk, procedur lub wymagań stosowanych jako odniesienie;

### **Kształcenie** – przekazywanie wiedzy, umiejętności, wiadomości w jakiejś dziedzinie;

### **Motywacja wewnętrzna** – motywacja pochodząca z subiektywnych odczuć pracownika, nie zaś oparta na tradycyjnym systemie wynagradzania płacą i świadczeniami dodatkowymi;

### **Motywacja zewnętrzna** – motywacja wywoływana udzielanymi pracownikowi nagrodami obiektywnymi, takimi jak płaca i świadczenia;

### **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;

### **Nazwa dokumentu** – krótki tekst opisujący typ dokumentu (procedura itp.);

### **Numer dokumentu** – unikalny ciąg cyfr i znaków, który wraz z symbolem w sposób jednoznaczny pozwala zidentyfikować dokument;

### **Niezgodność** - niespełnienie wymagania;

### **Obowiązki** – czynności związane z zajmowanym stanowiskiem;

### **Odbiorca –** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;

### **Odpowiedzialność** – konieczność odpowiadania przez pracownika za naruszenie obowiązków służbowych;

### **Organ nadzorczy** – niezależny organ publiczny, ustanowiony przez państwo członkowskie Unii Europejskiej w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii Europejskiej;

### **Organizacja międzynarodowa** - organizacja i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy;

### **Państwo trzecie** – Państwo, które znajduje się poza Europejskim Obszarem Gospodarczym;

### **Plan audytu** – opis działań prowadzonych w miejscu ich występowania oraz ustaleń związanych z audytem;

### **Podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu ADO;

### **Poufność** - właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom (PN-EN ISO 27000:2014, pkt 2.12);

### **Proces** - zbiór działań wzajemnie powiązanych oraz wzajemnie oddziałujących, które przekształcają wejścia w wyjścia. W przypadku danych osobowych, przez proces rozumie się wszystkie działania mające na celu osiągnięcie celu przetwarzania, od momentu zebrania danych osobowych, poprzez ich wykorzystanie, aż do usunięcia (np. rekrutacja, zatrudnienie);

### **Procedura** – ustalony sposób przeprowadzenia działania lub procesu;

### **Program audytu** – zestaw audytów zaplanowanych w określonych ramach czasowych i mających określony cel;

### **Przetwarzanie** - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych 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;

### **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 (ogólne rozporządzenie o ochronie danych);

### **Ryzyko** - wpływ niepewności na cele. W przypadku danych osobowych o ryzyku mówi się w kontekście możliwości naruszenia praw lub wolności osób, których dane dotyczą;

### **Stanowisko** – pozycja w hierarchii zawodowej, służbowej;

### **Specyfikacja** – dokument, w którym podano wymagania;

### **Strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe.

### **System informatyczny –** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

### **System tradycyjny** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze;

### **Szkolenie** – kurs, cykl wykładów zorganizowanych w celu uzupełnienia wykształcenia, wiadomości i umiejętności z jakiejś dziedziny;

### **Tytuł dokumentu** – krótki tekst opisujący zawartość dokumentu;

### **Uprawnienia** – prawo nadane komuś do działania, wykonywania określonych czynności i podejmowania decyzji;

### **Ustalenia z audytu** – wyniki oceny zebranych dowodów z audytu w stosunku do kryteriów audytu;

### **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 z późn. zm.);

### **Użytkownik** - pracownik upoważniony do korzystania z systemu informatycznego, a w przypadku przetwarzania danych osobowych - posiadający pisemne upoważnienie wydane przez ADO lub osoby upoważnione przez ADO;

### **Właściciel procesu** - a) w odniesieniu do istniejących czynności przetwarzania - główna osoba odpowiedzialna za organizację, projektowanie, zarządzanie oraz doskonalenie danego procesu, b) w odniesieniu do planowanych operacji przetwarzania - główna osoba, która będzie odpowiedzialna za organizację, projektowanie, zarządzanie zmianami oraz ustawiczne doskonalenie planowanego procesu;

### **Wniosek z audytu** – wynik audytu przedstawiony przez zespół audytujący, po rozważeniu celów audytu i wszystkich ustaleń z audytu;

### **Współadministrator** – podmiot, który wspólnie z organizacją, która przyjęła niniejszą politykę, decyduje o celach i środkach przetwarzania danych osobowych (np. spółka z grupy kapitałowej);

### **Zabezpieczenie** - „środek, który modyfikuje ryzyko” (ISO 27000:2013);

### **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

### **Zasób** – jakikolwiek z aktywów organizacji, uczestniczący w operacjach przetwarzania danych osobowych. Do zasobów należą m.in. infrastruktura teleinformatyczna, sprzęt biurowy, personel oraz dokumenty w wersji papierowej;

### **Zarządzanie** – są to skoordynowane działania dotyczące kierowania i nadzorowania;

### **Zbiór danych –** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany, czy rozproszony funkcjonalnie lub geograficznie;

### **Zespół audytujący** – jeden lub więcej audytorów przeprowadzających audyt, wspomaganych przez ekspertów technicznych, jeżeli jest to wymagane;

### **Zgoda osoby, której dane dotyczą** - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

### **Zgodność** - „spełnienie wymagania” (ISO 27000:2013).

## OPIS DZIAŁANIA

### Polityka bezpieczeństwa ochrony danych:

#### Procedura systemowa „Zarządzanie zasobami ludzkimi” PS1.

#### Procedura systemowa „Nadzór nad dokumentacją i zapisami” PS 2.

#### Procedura systemowa „Zarządzanie danymi osobowymi” PS 3.

#### Procedura systemowa „Zarządzanie ryzykiem” PS 4.

#### Procedura systemowa „Procedura oceny skutków przetwarzania dla ochrony danych” PS 5.

#### Procedura systemowa „Audyty” PS 6.

#### Procedura systemowa „Komunikacja” PS 7.

#### Procedura systemowa „Zabezpieczenia” PS 8.

#### Procedura systemowa „Naruszenia” PS 9.

#### Procedura systemowa „Privacy by design and privacy by default” PS 10.

#### Procedura systemowa „Procedura przekazywania danych poza EOG” PS 11.

### Instrukcja zarządzania systemem informatycznym.

### Krajowe Ramy Interoperacyjności.

## ODPOWIEDZIALNOŚĆ I UPRAWNIENIA

|  |  |
| --- | --- |
| **Czynność** | **Odpowiedzialny** |
| Opracowanie procedur  | Inspektor Ochrony Danych w porozumieniu z Administratorem Danych Osobowych |
| Wdrożenie procedur  | Administrator Danych Osobowych |
| Nadzór nad przestrzeganiem procedur | Inspektor Ochrony Danych oraz Administrator Danych Osobowych |
| Wprowadzanie zmian w procedurach  | Administrator Danych Osobowych w porozumieniu z Inspektor Ochrony Danych  |

## DOKUMENTY ZWIĄZANE

* System zarządzania bezpieczeństwem informacji,
* 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 (ogólne rozporządzenie o ochronie danych),
* przepisy Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 z późn. zm.),
* Norma międzynarodowa PN-EN ISO/IEC 27001:2017-06 wersja polska.

## ZAŁĄCZNIKI

* PS 1 „Zarządzanie zasobami ludzkimi”
* PS 2 „Nadzór nad dokumentacją i zapisami”
* PS 3 „Zarządzanie danymi osobowymi”
* PS 4 „Zarządzanie ryzykiem”
* PS 5 „Procedura oceny skutków przetwarzania dla ochrony danych”
* PS 6 „Audyty”
* PS 7 „Komunikacja”
* PS 8 „Zabezpieczenia”
* PS 9 „Naruszenia”
* PS 10 „Privacy by design and privacy by default”
* PS 11 „Procedura przekazywania danych poza EOG”