Załącznik do Zasad Bezpieczeństwa
Informacji w organizacji o nazwie:
Starostwo Powiatowe w Kutnie

Definicje i skróty użyte w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji

Ilekroć w SZBI mówi się o:

1) **Organizacji** – rozumie się przez to osobę prawną, organ publiczny, jednostkę lub inny podmiot. Do celów niniejszych Zasad Bezpieczeństwa Informacji wprowadza się nazwę własną organizacji: Starostwo Powiatowe w Kutnie (dalej: Starostwo);

2) **Administratorze danych** (AD) – rozumie się przez to osobę fizyczną lub organizację, która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

3) **Inspektorze Ochrony Danych** (IOD) – rozumie się przez to osobę, której Administrator powierzył pełnienie obowiązków określonych w art. 39 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016.

4) **Administratorze Systemu Informatycznego** (ASI) – rozumie się przez to osobę, której Administrator powierzył pełnienie obowiązków nadzoru nad przestrzeganiem zasad ochrony danych osobowych pod kątem zabezpieczeń teleinformatycznych;

5) **Bezpieczeństwie informacji (**BI**)** – działania, których celem jest zapewnienie m.in. dostępności, integralności oraz poufności danych;

6) **Danych osobowych** – rozumie się przez to dane oznaczające informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. 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;

7) **Dostępności** – atrybut informacji, który daje pewność, że dla osób upoważnionych będą one dostępne. W przypadku systemów teleinformatycznych oznacza dodatkowo właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;

8) **Incydent bezpieczeństwa informacji** (w dokumentacji SZBI zwane incydentem) – pojedyncze zdarzenie lub seria niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji;

9) **Incydent cyberbezpieczeństwa** – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbepieczeństwo;
10) **Incydent krytyczny** – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy:

    - CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;

    - CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;

- CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;

11) **Incydent cyberbezpieczeństwa w podmiocie publicznym** – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez Starostwo z zastosowaniem systemu teleinformatycznego. Jako incydent cyberbezpieczeństwa w Starostwie rozumie się przerwanie realizacji zadania publicznego lub brak możliwości skorzystania z usług Starostwa w czasie dłuższym niż czas, w jakim Starostwo zobowiązane jest do ich zrealizowania lub niedostępność usługi świadczonej drogą elektroniczną w dni pracujące w czasie dłuższym niż 48 godzin zegarowych;

    W dokumentacji SZBI używa się pojęcia „Incydent" w znaczeniu wszystkich wyżej wymienionych definicji: Incydentu bezpieczeństwa informacji, incydentu cyberbezpieczeństwa, Incydentu krytycznego, Incydentu cyberbezpieczeństwa w podmiocie publicznym, Incydentu – w rozumieniu RODO.

12) **Integralność** – właściwość informacji, która zapewnia jej dokładność i kompletność. W przypadku systemów teleinformatycznych, oznacza dodatkowo właściwość polegającą na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
13) **Kanał informacyjny** – droga, sposób wysyłania i odbierania danych, np. wiadomość SMS, wykonany telefon, wiadomość mailowa;
14) **Naruszenie ochrony danych osobowych** – sytuacja, w której nastąpiło utracenie, zniszczenie, ujawnienie, zmodyfikowanie, bądź nieuprawniony dostęp do danych osobowych;
15) **Niezaprzeczalność** – w przypadku systemów teleinformatycznych oznacza brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymienia.
    Brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.
16) **Niezgodność** – niespełnienie wymagania;
17) **Nośnik danych** – przedmiot, na którym została zapisana informacja. Nośnik może być elektroniczny, bądź papierowy, np.: dysk przenośny, pendrive, kartka papieru;
18) **Osoba upoważniona** – osoba posiadająca odpowiedni poziom upoważnień, aby mieć dostęp do danej informacji (w tym zawierającej dane osobowe);
19) **Personel** – pracownicy, osoby wykonujące zadania na podstawie umów zlecenia, o dzieło, praktyki staże jak również wolontariusze, a także osoby będące pracownikami innych organizacji wykonujące w sposób stały powierzone zadania;
20) **Podatność** - słabość systemu/ aplikacji/ narzędzia. W przypadku systemów teleinformatycznych oznacza dodatkowo właściwość systemu teleinformatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie;
21) **Poufność** – właściwość informacji, która zapewnia, iż jest ona chroniona przed nieuprawnionym dostępem. W przypadku systemów teleinformatycznych oznacza dodatkowo właściwość zapewniającą, że informacja nie jest udostępniania lub wyjawiana nieupoważnionym osobom fizycznym;
22) **Praca zdalna** – wykonywanie zadań poza siedzibą Starostwa;
23) **Przetwarzanie informacji** – każde działanie, każda czynność, która wykonywana jest na informacjach;
24) **Przetwarzaniu danych osobowych** – rozumie się przez to operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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;
25) **RODO** – Rozporządzenie o ochronie danych osobowych;
26) **Rozliczalność** – w przypadku systemów teleinformatycznych oznacza właściwość systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie;
27) **Rozliczalność RODO** - rozumianą jako właściwość zapewniającą, że administrator jest odpowiedzialny za przestrzeganie przepisów oraz dokłada wszelkich starań aby być w stanie wykazać ich przestrzeganie.

28) **SI** – system teleinformatyczny;
29) **Sieci lokalnej** – rozumie się przez to sieć LAN (ang. Local Area Network) – sieć komputerową łączącą komputery na określonym obszarze (urząd, szkoła, laboratorium, biuro). Sieć LAN może być wydzielona zarówno fizycznie, jak i logicznie w ramach innej sieci. Główne różnice LAN, w porównaniu z WAN, to wyższy wskaźnik transferu danych i mniejszy obszar geograficzny;

30) **Sieci rozległej** – rozumie się przez to sieć WAN (ang. Wide Area Network) – sieć komputerową znajdującą się na obszarze wykraczającym poza miasto, kraj, kontynent;

31) **Sieci publicznej** – rozumie się przez to sieć telekomunikacyjną wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych w rozumieniu przepisów ustawy z dnia 16 lipca 2004r. - Prawo telekomunikacyjne (t.j. Dz.U.2022r., poz..1648);

32) **System Zarządzania Bezpieczeństwem Informacji (SZBI)** – zbiór zasad, wytycznych, procedur, których stosowanie gwarantuje spójne podejście do bezpieczeństwa informacji;

33) **Udokumentowana informacja** – informacja wraz z nośnikiem, na którym jest zapisana, wymagająca kontroli, przeglądów;

34) **UDW** – Ukryte do wiadomości – funkcja w poczcie mailowej, umożliwiająca wysłanie kopii wiadomości do adresata, bez wiedzy pozostałych;

35) **Urządzenia mobilne** – inaczej urządzenia przenośne, takie jak tablety, laptopy, telefony;

36) **Uwierzytelnienie, autentykacja** – działanie potwierdzające tożsamość;

37) **Zdarzenie dotyczące bezpieczeństwa informacji (w dokumentacji SZBI zwane zdarzeniem)** – stwierdzenie wystąpienia stanu systemu, usługi lub sieci, która wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji.

38) **Zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

39) **Identyfikatorze użytkownika** – rozumie się przez to nazwę przypisaną określonemu użytkownikowi. Używany jest podczas logowania, umożliwia uprawniony dostęp do danego komputera, systemu bądź sieci. Identyfikator jest ciągiem znaków o ograniczonej długości, wybranych z określonego zestawu znaków. Do identyfikatora przypisane jest konto użytkownika oraz ściśle określone uprawnienia, jakie ma dany użytkownik. Główną cechą identyfikatora jest jego unikalność w ramach danego systemu informatycznego;

40) **Użytkowniku systemu** - rozumie się przez to osobę fizyczną posiadającą formalne upoważnienie do przetwarzania danych osobowych wydane przez Administratora, oraz nadane uprawnienia do przetwarzania w systemie teleinformatycznym;

41) **Systemie teleinformatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz.U.2022r., poz..1648);

42) **Kryptografii** – rozumie się przez to gałąź wiedzy o utajnianiu wiadomości z dziedziny kryptologii - dziedziny wiedzy o przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem. Istotnym elementem technik kryptograficznych jest proces zamiany tekstu jawnego w szyfrogram (inaczej kryptogram); proces ten nazywany jest szyfrowaniem, a proces odwrotny, czyli zamiany tekstu zaszyfrowanego na powrót w możliwy do odczytania, deszyfrowaniem.

43) **Polityce Bezpieczeństwa Informacji, w tym danych osobowych (PBI ODO)** – rozumie się przez to zestaw formalnych zasad, procedur oraz kodeksów dobrych praktyk odnoszących się do bezpieczeństwa przepływu informacji zbieżnych z celami istnienia organizacji;

44) **Polityce Bezpieczeństwa Teleinformatycznego (PBT)** – rozumie się przez to zestaw formalnych zasad i procedur odnoszących się do bezpieczeństwa przepływu informacji w systemie teleinformatycznym;

45) **Polityce zarządzania incydentami związanymi z bezpieczeństwem informacji (PZI)** – rozumie się przez to zestaw formalnych procedur odnoszących się do postępowania z incydentami/ naruszeniami w zakresie bezpieczeństwa informacji, w tym danych osobowych;

46) **Analizie Ryzyka Ogólnego i Ocenie Skutków dla Przetwarzania danych (DPIA)** – rozumie się przez to dokumentację zawierającą opis metodologii, częstotliwości oraz zakresu przeprowadzanego procesu szacowanie ryzyka;

47) **CRWDE** – rozumie się przez to Centralne Repozytorium Wniosków Dokumentacji Elektronicznej;

48) **ESP** – rozumie się przez to elektroniczną skrzynkę podawczą;

49) **ePUAP** – rozumie się przez to elektroniczną platformę usług administracji publicznej;

50) **SOA** – (ang. Service-Oriented Architecture) rozumie się przez to architekturę zorientowaną na usługi. Koncepcja tworzenia systemów informatycznych, w której główny nacisk stawia się na definiowanie usług, które spełnią wymagania użytkownika. Pojęcie SOA obejmuje zestaw metod organizacyjnych i technicznych mający na celu powiązanie biznesowej strony organizacji z jej zasobami informatycznymi;

51) **SLA** – (ang. Service Level Agreement) rozumie się przez to umowę utrzymania i systematycznego poprawiania ustalonego między organizacją a usługodawcą poziomu jakości usług poprzez stały cykl obejmujący uzgodnienia, monitorowanie usługi, raportowanie oraz przegląd osiąganych wyników.

DEFINICJE PBT:

Ilekroć w „Polityce Bezpieczeństwa Teleinformatycznego" mówi się o:

1) **Organizacji** – rozumie się przez to osobę prawną, organ publiczny, jednostkę lub inny podmiot. Do celów niniejszej Polityki Bezpieczeństwa Teleinformatycznego wprowadza się nazwę własną organizacji: **Starostwo Powiatowe w Kutnie**;

2) **Administratorze** – rozumie się przez to osobę fizyczną lub organizację, która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

3) **Inspektorze Ochrony Danych** – rozumie się przez to osobę, której Administrator powierzył pełnienie obowiązków określonych w art. 39 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016.

4) **Administratorze Systemu Informatycznego** – rozumie się przez to osobę, której Administrator powierzył pełnienie obowiązków nadzoru nad przestrzeganiem zasad ochrony danych osobowych pod kątem zabezpieczeń teleinformatycznych;

5) **Danych osobowych** – rozumie się przez to dane oznaczające informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. 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;

6) **Przetwarzaniu** – rozumie się przez to operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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;

7) **Sieci lokalnej** – rozumie się przez to sieć LAN (ang. Local Area Network) – sieć komputerową łączącą komputery na określonym obszarze (urząd, szkoła, laboratorium, biuro). Sieć LAN może być wydzielona zarówno fizycznie, jak i logicznie w ramach innej sieci. Główne różnice LAN, w porównaniu z WAN, to wyższy wskaźnik transferu danych i mniejszy obszar geograficzny;

8) **Sieci rozległej** – rozumie się przez to sieć WAN (ang. Wide Area Network) – sieć komputerową znajdującą się na obszarze wykraczającym poza miasto, kraj, kontynent;

9) **Sieci publicznej** – rozumie się przez to sieć telekomunikacyjną wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (t.j. Dz.U.2022r., poz..1648);

10) **Zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

11) **Osobie upoważnionej** – rozumie się przez to osobę posiadającą formalne upoważnienie do przetwarzania danych osobowych wydane przez Administratora;

12) **Identyfikatorze użytkownika** – rozumie się przez to nazwę przypisaną określonemu użytkownikowi. Używany jest podczas logowania, umożliwia uprawniony dostęp do danego komputera, systemu bądź sieci. Identyfikator jest ciągiem znaków o ograniczonej długości, wybranych z określonego zestawu znaków. Do identyfikatora przypisane jest konto użytkownika oraz ściśle określone uprawnienia, jakie ma dany użytkownik. Główną cechą identyfikatora jest jego unikalność w ramach danego systemu informatycznego;

13) **Użytkowniku systemu** - rozumie się przez to osobę fizyczną posiadającą formalne upoważnienie do przetwarzania danych osobowych wydane przez Administratora, oraz nadane uprawnienia do przetwarzania w systemie teleinformatycznym;

14) **Systemie teleinformatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz.U.2022r., poz..1648);

15) **Kryptografii** – rozumie się przez to gałąź wiedzy o utajnianiu wiadomości z dziedziny kryptologii - dziedziny wiedzy o przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem. Istotnym elementem technik kryptograficznych jest proces zamiany tekstu jawnego w szyfrogram (inaczej kryptogram); proces ten nazywany jest szyfrowaniem, a proces odwrotny, czyli zamiany tekstu zaszyfrowanego na powrót w możliwy do odczytania, deszyfrowaniem.

16) **Polityce Bezpieczeństwa Informacji, w tym danych osobowych (PBI ODO)** – rozumie się przez to zestaw formalnych zasad, procedur oraz kodeksów dobrych praktyk odnoszących się do bezpieczeństwa przepływu informacji zbieżnych z celami istnienia organizacji;

17) **Polityce Bezpieczeństwa Teleinformatycznego (PBT)** – rozumie się przez to zestaw formalnych zasad i procedur odnoszących się do bezpieczeństwa przepływu informacji w systemie teleinformatycznym;

18) **Polityce zarządzania incydentami związanymi z bezpieczeństwem informacji (PZI)** – rozumie się przez to zestaw formalnych procedur odnoszących się do postępowania z naruszeniami w zakresie bezpieczeństwa informacji, w tym danych osobowych;

19) **Analizie Ryzyka Ogólnego i Ocenie Skutków dla Przetwarzania danych (DPIA)** – rozumie się przez to dokumentację zawierającą opis metodologii, częstotliwości oraz zakresu przeprowadzanego procesu szacowanie ryzyka;

20) **CRWDE** – rozumie się przez to Centralne Repozytorium Wniosków Dokumentacji Elektronicznej;

21) **ESP** – rozumie się przez to elektroniczną skrzynkę podawczą;

22) **ePUAP** – rozumie się przez to elektroniczną platformę usług administracji publicznej;

23) **SOA** – (ang. Service-Oriented Architecture) rozumie się przez to architekturę zorientowaną na usługi. Koncepcja tworzenia systemów informatycznych, w której główny nacisk stawia się na definiowanie usług, które spełnią wymagania użytkownika. Pojęcie SOA obejmuje zestaw metod organizacyjnych i technicznych mający na celu powiązanie biznesowej strony organizacji z jej zasobami informatycznymi;

24) **SLA** – (ang. Service Level Agreement) rozumie się przez to umowę utrzymania i systematycznego poprawiania ustalonego między organizacją a usługodawcą poziomu jakości usług poprzez stały cykl obejmujący uzgodnienia, monitorowanie usługi, raportowanie oraz przegląd osiąganych wyników.

Ilekroć w „Analizie Ryzyka Ogólnego i Ocenie Skutków Dla Przetwarzania Danych (DPIA)" mówi się o:

1) **Szacowaniu ryzyka** – rozumie się przez to proces analizy i oceny ryzyka. W procesie szacowania ryzyka w kontekście danych osobowych szacowanie ryzyka uwzględnia ryzyka związane z naruszeniem praw i wolności osób fizycznych, których przetwarzanie dotyczy;

2) **Analizie ryzyka** – rozumie się przez to proces identyfikacji źródeł ryzyka i oszacowania ryzyka;

3) **Ocenie ryzyka** – proces porównywania oszacowanego ryzyka w celu określenia znaczenia ryzyka;

4) **Ryzyku** – rozumie się przez to kombinację prawdopodobieństwa zdarzenia i jego konsekwencji;

5) **Ryzyku szczątkowym** – rozumie się przez to ryzyko pozostające po procesie postępowania z ryzykiem;

6) **Postępowaniu z ryzykiem** – rozumie się przez to proces zmiany poziomu ryzyka poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych;

7) **Akceptacji ryzyka** – rozumie się przez to decyzję Administratora/ kierownictwa organizacji o tym, aby ryzyko zaakceptować;

8) **Podatności** – rozumie się przez to słabość w strukturze fizycznej, technicznej, organizacyjnej organizacji;

9) **Incydencie** – rozumie się przez to zdarzenie mające lub mogące mieć negatywny wpływ na System Zarządzania Bezpieczeństwem Informacji w organizacji. Incydent może powodować w stosunku do osoby fizycznej, której dane osobowe organizacja przetwarza, szkodę o charakterze majątkowym lub niemajątkowym;

10) **Poufności** – rozumie się przez to właściwość polegająca na tym, że osoba nieupoważniona bądź podmiot nie mają dostępu do danych osobowych, które temu atrybutowi podlegają;

11) **Integralności** – rozumie się przez to właściwość polegająca na tym, że aktywa w postaci informacji/danych osobowych pozostają kompletne;

12) **Dostępności** – rozumie się przez to właściwość polegająca na tym, że aktywa w postaci informacji/ danych osobowych pozostają dostępne dla osób upoważnionych/ uprawnionych do ich przetwarzania;

13) **Bezpieczeństwie informacji** – rozumie się przez to zachowanie wobec przetwarzanych danych osobowych/informacji takich atrybutów jak poufność, integralność oraz dostępność.

Daniel Kowalik

Elektronicznie podpisany przez Daniel Kowalik
Data: 2022.11.22 10:44:27 +01'00'