Polityka Bezpieczeństwa Informacji

Historia zmian dokumentu:

Data	Wersja	Opis zmiany	Autor zmian
01.03.2024	01	Opracowanie i przyjęcie dokumentu	IODO

WPROWADZENIE

1. Polityka bezpieczeństwa informacji jest strategicznym elementem systemu zarządzania bezpieczeństwem informacji.

ROZDZIAŁ I

CZĘŚĆ OGÓLNA

PRZEDMIOT I CELE

1. Polityka Bezpieczeństwa Informacji wprowadza w jednostce System Zarządzania Bezpieczeństwem Informacji, którego ustanowienie, wdrożenie, utrzymanie i doskonalenie opiera się na wymaganiach normy ISO 27001.
2. Polityka jest dokumentem nadrzędnym w stosunku do wszystkich regulacji powiązanych, funkcjonujących w jednostce w zakresie szeroko pojętego bezpieczeństwa informacji.
3. Główną rolą Systemu Zarządzania Bezpieczeństwem Informacji ma być zapewnienie poufności, integralności i dostępności przetwarzanych informacji oraz dbanie o prywatność naszych klientów, a także spełnienie wymogów prawnych związanych z ochroną danych osobowych.
4. Niniejsza polityka ma spełniać następujące cele bezpieczeństwa informacji:
   a. Zabezpieczenie informacji przed udostępnieniem lub ujawnieniem ich nieupoważnionym osobom, podmiotom lub procesom (poufność);
   b. Zabezpieczenie informacji przed nieuprawnionymi zmianami i manipulacjami (integralność);
   c. Zapewnienie dostępu uprawnionym osobom, podmiotom i procesom do wszelkich informacji, gdy jest to wymagane i konieczne (dostępność);
   d. Zapewnienie, że działania osoby/podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie/podmiotowi (rozliczalność);
   e. Udowodnienie wystąpienia deklarowanych zdarzeń lub działań oraz, że zostały one wywołane przez dany podmiot (niezaprzeczalność);
   f. Zapewnienie, że osoba/podmiot jest tym, za kogo się podaje (autentyczność);
   g. Zapewnienie spójnych, zamierzonych zachowań i skutków (niezawodność).
5. Cele bezpieczeństwa informacji są osiągane poprzez:
   a. Zapewnienie integracji bezpieczeństwa informacji z działalnością operacyjną Organizacji;
   b. Zapewnienie zgodności z właściwymi wymaganiami prawa i zarządzanie oczekiwaniami interesantów;
   c. Przyjęcie podejścia opartego na ocenie ryzyka, zapewniającego spójne i efektywne postępowanie wobec ryzyka;
   d. Promowanie odpowiedzialnego postępowania w zakresie bezpieczeństwa informacji.

MATERIALNY I TERYTORIALNY ZAKRES ZASTOSOWANIA

6. Niniejsza polityka ma zastosowanie do przetwarzania każdej informacji bez względu czy jej przetwarzanie odbywa się w sposób całkowicie lub częściowo zautomatyzowany.
7. Niniejsza polityka ma zastosowanie do wszystkich informacji przetwarzanych w związku z działalnością prowadzoną przez organizację bez względu, gdzie aktualnie one się znajdują.
8. W przypadkach, kiedy informacje przetwarzane są poza granicami Polski należy stosować również obowiązujące przepisy międzynarodowe i krajowe.

9. Zasady określone w Polityce Bezpieczeństwa Informacji mają zastosowanie do wszystkich procesów biznesowych, procesów wsparcia, działalności operacyjnej i projektowej wraz ze wspierającymi je systemami informatycznymi i innymi zasobami technicznymi w tym do wszelkich aktywów informacyjnych, do których należą:
    a. wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy (informatyczne oraz tradycyjne - papierowe), w których przetwarzane są informacje podlegające ochronie,
    b. informacje będące własnością Organizacji,
    c. informacje będące własnością klientów Organizacji, uzyskane na podstawie zawartych umów,
    d. wszystkie lokalizacje Organizacji, czyli budynki i pomieszczenia, w których są lub będą przetwarzane informacje podlegające ochronie,
    e. wszyscy pracownicy i współpracownicy Organizacji niezależnie od form zatrudnienia, jak również podmioty zewnętrzne realizujące zadania na rzecz Organizacji lub współpracujące z Organizacją, mające dostęp do informacji podlegających ochronie na podstawie stosownych umów i porozumień.

DEFINICJE

10. Ilekroć w Polityce Bezpieczeństwa Informacji jest mowa o:
    a. **„Polityce”** - należy przez to rozumieć Politykę Bezpieczeństwa Informacji ;
    b. **„GPGK Poniatowa” lub „Organizacja”** – należy przez to rozumieć Gminne Przedsiębiorstwo Gospodarki Komunalnej Sp. z o.o. ul. Młodzieżowa 4 24-320 Poniatowa;
    c. **„Najwyższym kierownictwie**” - należy przez to rozumieć zarząd GPGK Poniatowa;
    d. **„SZBI” -** należy przez to rozumieć System Zarządzania Bezpieczeństwem Informacji;
    e. **„IOD” -** należy przez to rozumieć Inspektora Ochrony Danych Osobowych Organizacji;
11. Na użytek niniejszej polityki należy następująco interpretować użyte sformułowania:
    a. **Informacje** są strategicznym zasobem organizacji niezbędnym do jej funkcjonowania. Informacje są przechowywane w różnych formach:
        - cyfrowej (np. pliki, bazy danych systemów),
        - materialnej (np. na papierze),
        - niematerialnej (np. wiedza pracowników).

       Mogą być one przesyłane za pomocą różnych środków, w tym: komunikacji za pośrednictwem kuriera, komunikacji elektronicznej lub werbalnej.
       Niezależnie od tego, jaką formę posiadają informacje i tego, jaki jest środek ich przesyłania, zawsze wymagają właściwej ochrony.
    b. **Bezpieczeństwo informacji** jest sposobem zapewniania poufności, dostępności, integralności a także autentyczności, rozliczalności, niezaprzeczalności i niezawodności informacji poprzez zastosowanie i zarządzanie właściwymi zabezpieczeniami, co z kolei jest wynikiem rozpatrzenia szerokiej gamy zagrożeń w procesie zarządzania ryzykiem;
    c. **Poufność** jest właściwością polegającą na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
    d. **Integralność** jest właściwością polegającą na zapewnieniu dokładności i kompletności;
    e. **Dostępność** jest właściwością bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu;
    f. **Autentyczność** jest właściwością polegającą na tym, że podmiot jest tym za kogo się podaje;
    g. **Rozliczalność** jest właściwością systemu pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie;

h. **System** jest rozumiany jako zespół wzajemnie powiązanych elementów realizujących jako całość założonych celów;
i. **Niezaprzeczalność** jest zdolnością udowodnienia, że wystąpiły deklarowane zdarzenia lub działania oraz że wywołał je dany podmiot;
j. **Niezawodność** jest właściwością oznaczającą spójne, zamierzone zachowanie i skutki;
k. **Dane osobowe** to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania żyjącej osobie fizycznej.
l. **Incydent związany z bezpieczeństwem informacji** to pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
m. **Zdarzenie związane z bezpieczeństwem informacji** to 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.
n. **Zabezpieczenie** to środek, który modyfikuje ryzyko**.** Zabezpieczenia obejmują procesy, politykę, urządzenia, praktyki lub inne działania modyfikujące ryzyko;
o. **Ryzyko** to wpływ niepewności na cele bezpieczeństwa informacji;
p. **Niepewność** to stan, również częściowy, niedoboru informacji związanej ze zrozumieniem lub wiedzą na temat zdarzenia;
q. **Zdarzenie** to wystąpienie lub zmiana konkretnego zestawu okoliczności;
r. **Przetwarzanie danych** to czynności związane z użytkowaniem tych danych, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie itp.

WYMAGANIA PRAWNE

12. GPGK Poniatowa przy określaniu swoich wymagań związanych z bezpieczeństwem, bierze pod uwagę trzy źródła:
    a. Szacowanie ryzyka dotyczącego bezpieczeństwa informacji, z uwzględnieniem strategii i celów Organizacji;
    b. Przepisy prawne, zobowiązania wynikające z zawartych umów, regulacje oraz środowisko społeczno- kulturowe;
    c. Zbiór dobrych praktyk jakie Organizacja dotychczas wypracowała dla wsparcia swojej działalności.

ROZDZIAŁ II

UREGULOWANIA SZCZEGÓŁOWE

DEKLARACJA NAJWYŻSZEGO KIEROWNICTWA

13. Najwyższe kierwnictwo zobowiązuje się do podejmowania wszelkich niezbędnych działań zmierzających do realizacji celów bezpieczeństwa, a w szczególności:
    a. zapewnia wsparcie dla inicjatyw z zakresu bezpieczeństwa informacji,
    b. zapewnia środki potrzebne do zapewnienia bezpieczeństwa informacji,
    c. wyznacza zakresy odpowiedzialności związane z bezpieczeństwem informacji,

d. podejmuje działania utrzymujące świadomość w zakresie bezpieczeństwa informacji,
e. reaguje na wszelkie incydenty i gwarantuje bieżącą ich obsługę,
f. zapewnia zgodność stosowanych w Organizacji zasad bezpieczeństwa z regulacją w Polsce i Unii Europejskiej,
g. ocenia i doskonali System Zarządzania Bezpieczeństwem Informacji.

14. Realizacja powyższego zobowiązania będzie badana na podstawie „**Deklaracji stosowania**".

ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI

15. Za organizację i nadzorowanie bezpieczeństwa informacji odpowiadają w szczególności:
    a. Najwyższe kierownictwo;
    b. administratorzy systemów informatycznych;
    c. inspektor ochrony danych i jego zastępcy;
    d. osoba zapewniająca obsługę w obszarze IT;
    e. osoby odpowiedzialne za sprawy kadrowe;
    f. osoby odpowiedzialna za obsługę sekretariatu, archiwizację i czynności kancelaryjne.
16. Odpowiedzialność za organizację i nadzorowanie bezpieczeństwa informacji ponosi również każdy kto w zakresie własnych uprawnień, upoważnień, zakresu obowiązków lub innych umocowań prawnych uczestniczy w czynnościach choćby tylko wpływających na bezpieczeństwo informacji.

KLASYFIKACJA INFORMACJI

17. Klasyfikacja informacji została wprowadzona w celu uporządkowania postępowania z różnymi rodzajami informacji, które są głównym zasobem organizacji.
18. Struktura klasyfikacji informacji w Organizacji opiera się na założeniu istnienia trzech poziomów postrzegania informacji:
    a. **informacje jawne**- informacje publicznie dostępne, których obowiązek udostępniania wynika z przepisów prawa, w szczególności informacje publiczne w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej lub których publiczna dostępność i jawność wynika z wewnętrznych uregulowań;
    b. **informacje wewnętrzne**- informacje, przetwarzane w ramach i na potrzeby wewnętrzne Organizacji, których przetwarzanie i udostępnianie podlega uregulowaniom wewnętrznym z uwagi na szczególne znaczenie dla Organizacji (właściciela informacji). Wyszczególniamy trzy kategorie informacji wewnętrznych:
        - **informacje wewnętrzne dostępne**- informacje dostępne dla wszystkich pracowników Organizacji, np.: książka adresowa z listą pracowników i danymi kontaktowymi;
        - **informacje wewnętrzne wrażliwe**- informacje dostępne dla pracowników upoważnionych z uwagi na realizowane zadania, np. informacje o urlopach, informacje o zastosowanych zabezpieczeniach budynku;
        - **informacje stanowiące tajemnicę pracodawcy** - informacje, których przetwarzanie i udostępnianie mogą narazić Organizację na szkodę i których dostępność ograniczona jest do absolutnego minimum;
    c. **Informacje poufne** - tajemnice określone w odrębnych przepisach, np.:
        - w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;

- w Rozporządzeniu 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).

19. Wprowadzenie klasyfikacji informacji, o której mowa powyżej, nie wprowadza konieczności specjalnego fizycznego oznaczania informacji udokumentowanych, chyba, że inaczej wynika z przepisów.
20. Klasyfikacje informacji należy przeprowadzać zawsze, kiedy:
    - ustala się środki bezpieczeństwa informacji;
    - ustala się zasady udostępniania, przechowywania, usuwania czy w inny sposób przetwarzania informacji;
    - przeprowadzania analizy ryzyka naruszenia bezpieczeństwa informacji;
    - organizowana jest nowa czynność lub zmiana w aktualnie wykonywanej czynności;
    - oraz w każdym innym przypadku, kiedy będzie to niezbędne ze względu na podejmowane działania lub zaniechania.
21. Nadawanie symboli spraw bądź przydzielanie do właściwej klasy zgodnie z Jednolitym Rzeczowym Wykazem Akt oraz Instrukcją Kancelaryjną nie jest przeprowadzaniem klasyfikacji informacji na potrzeby bezpieczeństwa informacji.

DOKUMENTACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

22. Dokumentacja systemu zarządzania bezpieczeństwem informacji w szczególności składa się z:
    a. Polityki bezpieczeństwa ochrony danych osobowych
    b. Instrukcji zarządzania systemami informatycznymi
    c. Polityki ochrony danych osobowych
    d. innych dokumentów organizacyjnych częściowo obejmujący obszar bezpieczeństwa informacji (np. instrukcje archiwalne czy kancelaryjne;
    e. regulacji prawnych dotyczących obszarów bezpieczeństwa informacji;
    f. Procedur bezpieczeństwa regulujące pojedyncze obszary bezpieczeństwa informacji.

ŚRODKI (PROCEDURY) BEZPIECZEŃSTWA

23. W celu zapewnienia najwyższego poziomu bezpieczeństwa informacji oraz w celu sformalizowania, ujednolicenia i udokumentowania różnych obszarów bezpieczeństwa informacji najwyższe kierownictwo wdraża odpowiednie środki techniczne i organizacyjne (zwane dalej „**środki bezpieczeństwa**").
24. Ustalając odpowiednie środki bezpieczeństwa informacji uwzględnia się:
    a. charakter, zakres, kontekst i cele przetwarzania informacji
    b. ryzyko naruszenia bezpieczeństwa informacji o różnym prawdopodobieństwie i wadze zagrożenia
    c. stan wiedzy technicznej
    d. koszty wdrożenia
    e. obowiązki wynikające z regulacji prawnych i wewnętrznych.
25. Ustalanie odpowiednich środków bezpieczeństwa odbywa się przed rozpoczęciem przetwarzania informacji oraz -w razie potrzeby- w trakcie przetwarzania.
26. Środki bezpieczeństwa ustalane są w odrębnych procedurach (zwane dalej „**procedury bezpieczeństwa**"), które w razie potrzeby są poddawane przeglądom i uaktualnienia.

27. Procedury bezpieczeństwa są dokumentacją poufną, dostępną tylko dla osób uprawnionych, chyba, że inaczej stanowią poszczególne procedury.
28. Procedury bezpieczeństwa mogą być dokumentacją regulującą wyłącznie elementy bezpieczeństwa informacji, ale również mogą stanowić część dokumentacji regulującej inne obszary prowadzonej działalności.

PRAWO DO WGLĄDU

29. Prawo wglądu do informacji sklasyfikowanych jako publiczne przysługuje każdemu kto takiej informacji zażąda.
30. Prawo wglądu do informacji sklasyfikowanej jako wewnętrzna przysługuje każdemu zgodnie ze schematem organizacyjnym i zakresem uprawnień.
31. Prawo wglądu do informacji sklasyfikowanej jako poufna przysługuje tylko odbiorcom, których uprawnienie wynika z przepisów prawa, prawomocnych wyroków, oświadczeń, umów, porozumień lub innych wiążących prawnie czynności.

ZACHOWANIE POUFNOŚCI

32. Zobowiązany do zachowania jest każdy pracownik, niezależnie od formy zatrudnienia.
33. Obowiązek zachowania poufności trwa również po ustaniu stosunku pracy lub innego stosunku prawnego, na podstawie którego była wykonywana praca na rzecz Organizacji.
34. Zobowiązanie do zachowania poufności potwierdzone jest podpisaniem przez każdą ww. osobę stosownego oświadczenia.
35. W przypadku realizacji zadań przez podmioty zewnętrzne zachowanie poufności każdorazowo regulowane jest w ramach zawartych z nimi umów.

POLITYKA KONTROLI DOSTĘPU

36. Dostęp do informacji przetwarzanych w Organizacji jest poddany kontroli wynikającej z obowiązujących przepisów prawa oraz wymagań bezpieczeństwa informacji wskazanych w normie ISO 27001.
37. Kontrola dostępu polega w szczególności na:
    a. wydzieleniu obszarów przeznaczonych do przetwarzania poszczególnych zbiorów danych/informacji i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi;
    b. zarządzaniu uprawnieniami poszczególnych użytkowników w sposób zapewniający dostęp wyłącznie do informacji wymaganych do wykonywania obowiązków służbowych, jeśli informacje te podlegają ochronie z jakiejkolwiek przyczyny;
    c. stosowaniu bezpiecznych systemów przetwarzania informacji;
    d. nadzorowaniu działalności stron trzecich, mogących wpłynąć na bezpieczeństwo informacji;
    e. bieżącym informowaniu pracowników o wszelkich zmianach w zakresie regulacji dotyczących przetwarzania i udostępniania informacji.
38. Adekwatność i skuteczność stosowanych w Organizacji środków kontroli dostępu do informacji podlega weryfikacji:
    a. systematycznej – w trakcie wykorzystywania środków kontroli dostępu;
    b. cyklicznej – w ustalonych i zaplanowanych odstępach czasu;
    c. doraźnej – w efekcie istotnych zmian w organizacji.

ZARZĄDZANIE PROJEKTAMI

39. W przypadku każdego nowego projektu, bądź zmiany obecnie realizowanego projektu, należy uwzględniać bezpieczeństwo informacji jako jeden z podstawowych celów projektu od samego początku jego planowania a następnie poprzez jego organizację i zakończenie.
40. Uwzględnienie bezpieczeństwa informacji w każdej fazie projektu zapewnić ma odpowiedni poziom bezpieczeństwa informacji poprzez zastosowanie adekwatnych środków bezpieczeństwa.
41. Wybór odpowiednich środków bezpieczeństwa informacji dokonywany jest na podstawie analizy ryzyka.

ANALIZA RYZYKA

42. Najwyższe kierownictwo wykonuję analizę ryzyka naruszenia bezpieczeństw informacji lub powierza jej wykonanie na podstawie formalnych uprawnień.
43. Analizy ryzyka przeprowadzana jest:
    a. systematycznie – w ramach codziennych czynności;
    b. cyklicznie - w ustalonych i zaplanowanych odstępach czasu;
    c. doraźnej – w efekcie istotnych zmian w organizacji.
44. Analiza ryzyka obejmuje wszelkie informacje, aktywa i środki bezpieczeństwa.
45. Analiza ryzyka wykonywana jest zgodnie z ustalonymi i wprowadzonymi procedurami.

REAKCJA NA INCYDENTY

46. Każdy pracownik, współpracownik lub osoba trzecia, w przypadku wykrycia incydentu lub słabości mogącej skutkować lub skutkujące naruszeniem bezpieczeństwa informacji (np. kradzieży lub podejrzenia wycieku danych), zobowiązana jest niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego i postępować zgodnie z jego poleceniem i procedurami dotyczącymi incydentów bezpieczeństwa informacji.
47. W zależności od sklasyfikowania informacji reakcja na incydent może wynikać z różnych procedur np. dotyczących bezpieczeństwa informacji lub naruszenia ochrony danych osobowych lub incydentów cyberbezpieczeństwa lub innych procedur regulujących sytuację wystąpienia bądź ryzyka wystąpienia zagrożenia bezpieczeństwa informacji.
48. Każdy pracownik, wykonawca czy zleceniobiorca zobowiązany jest zapoznać się z procedurami dotyczący incydentów bezpieczeństwa i obowiązany jest ich bezwzględnie przestrzegać.

POSTĘPOWANIE DYSCYPLINARNE, ODSZKODOWAWCZE I KARNE

49. Za złamanie zasad bezpieczeństwa informacji wynikających z ustanowionych procedur i polityk oraz z przepisów prawa pracownikowi grozi odpowiedzialność dyscyplinarna wynikająca z Kodeksu Pracy i regulaminu pracy, odpowiedzialność cywilna w ramach poniesionej szkody oraz odpowiedzialność karna w ramach czynu zabronionego.
50. Odpowiedzialność ponosi w szczególności ten kto umyślnie łamie zasady bezpieczeństwa informacji.

PRZEGLĄDY

51. Dokumentacja dotycząca bezpieczeństwa informacji, środki bezpieczeństwa oraz aktywa należy poddawać przeglądom:

a. systematycznym – w trakcie realizacji różnych czynności związanych z bezpieczeństwem informacji;
b. cyklicznym – w ustalonych i zaplanowanych odstępach czasu;
c. doraźnym – w efekcie istotnych zmian w organizacji.

52. Plan przeglądów cyklicznych ustala najwyższe kierownictwo wraz ze wskazaniem osoby odpowiedzialnej za przegląd.
53. Plan przeglądów cyklicznych ustala się do końca roku na cały rok następny.
54. Bez względu na to kto wykonuje przegląd i jaki rodzaj przeglądu jest wykonywany, każdy przegląd musi zakończyć się sprawozdaniem zatwierdzonym przez najwyższe kierownictwo.
55. W ramach zaplanowanych przeglądów, należy ustalić również wykonanie przeglądów przez osoby niezależne.