Załącznik do zarządzenia Nr 33/2022
Wójta Gminy Tarnówka
z dnia 12 kwietnia 2022 r.

Polityka Bezpieczeństwa Informacji w zakresie bezpieczeństwa informacji i ochrony danych osobowych podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej

Administrator Danych Osobowych – Jacek Mościcki – WÓJT GMINY TARNÓWKA

Zgodnie z art. 32 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 (dalej RODO) oraz zgodnie z USTAWĄ z dnia 10 maja 2018 r. o ochronie danych osobowych Dz. U. 2018 poz. 1000 Administrator Danych Osobowych wdraża dokument o nazwie ***„Polityka Bezpieczeństwa Informacji w zakresie bezpieczeństwa informacji i ochrony danych osobowych podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej".***

➢ Cel i przeznaczenie dokumentu

Celem niniejszej dokumentacji jest przedstawienie zasad oraz procedur w zakresie budowania i stosowania systemu bezpiecznego przetwarzania danych osobowych. Dokumentacja ma zastosowanie zarówno, gdy jest już przetwarzana dokumentacja w postaci elektronicznej, jak również gdy podmiot przygotowuje się lub też wdraża system informatyczny. Dokumentacja zawiera informacje w zakresie rozwiązań technicznych umożliwiających przetwarzanie dokumentacji osobowej. Zostały przedstawione wymagania organizacyjne oraz wskazano odpowiedzialność za przetwarzanie informacji w tym danych osobowych wrażliwych zawartych w dokumentacji osobowej. Celem dokumentacji jest doprecyzowanie zakresu zastosowania przepisów RODO.

Nadrzędnym celem jest:

1. Zapewnienie spełnienia wymagań prawnych.
2. Ochrona systemów przetwarzania informacji przed nieuprawnionym dostępem bądź zniszczeniem.
3. Podnoszenie świadomości pracowników.
4. Zmniejszenie ryzyka utraty informacji.
5. Zaangażowanie wszystkich pracowników w ochronę informacji.
6. Ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji.

7. Właściwy dobór zabezpieczeń (środków bezpieczeństwa) oparty na rezultatach i wnioskach wynikających z procesów szacowania i postępowania z ryzykiem, wymagań prawnych, wymagań nadzoru, zobowiązań kontraktowych oraz pozostałych wymagań dotyczących bezpieczeństwa informacji w **URZĘDZIE GMINY TARNÓWKA**.

➢ **Bezpieczeństwo informacji zapewnione jest poprzez:**

Zarządzanie ryzykiem, na które składa się:
1. Klasyfikacja zasobów i ich zawartości.
2. Identyfikacja stopnia zagrożeń i ich następstw.
3. Określenie i wdrożenie działań zabezpieczających zasoby.

Zarządzanie zmianami na które składa się:
1. Analiza wpływu zmian na poziom bezpieczeństwa.
2. Zapewnienie pełnej koordynacji podczas wprowadzania zmian.
3. Zarządzanie ciągłością działania organizacji poprzez wdrożenie instrukcji awaryjnych.

➢ **Zakres obowiązywania:**

Niniejszy dokument dotyczy wszystkich komórek organizacyjnych oraz wszystkich pracowników, a także innych osób mających dostęp do informacji chronionych (np. pracowników firm zewnętrznych realizujących prace na rzecz podmiotu).
Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej, video lub innej).
Z dokumentem są zobowiązani zapoznać się wszyscy pracownicy mający dostęp do danych osobowych oraz innych chronionych informacji. Niniejsza procedura została opracowana na podstawie rozporządzenia Krajowych Ram Interoperacyjności, w świetle wytycznych standaryzujących obszary zabezpieczeń według Polskiej Normy PN-ISO/IEC 27001, oraz PN-ISO/IEC 27002 w odniesieniu do ustanawiania zabezpieczeń, PN- SO/IEC 27005 w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.
Gwarantuje to system zapewniający poufność, dostępność i integralność informacji z uwzględnieniem dodatkowo takich atrybutow, jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność, oraz ciągłość działania.

Kierownictwo i podmioty współpracujące, są proporcjonalnie zaangażowani w działaniach wspierania osób funkcyjnych i przestrzegania procedur zmierzających do zapewnienia bezpieczeństwa informacyjnego, na założonym poziomie. Wdrożona procedura, może podlegać ciągłemu doskonaleniu, zgodnie z wymaganiami normy PN-ISO/IEC 27001.
Celem wdrożonego planu działań jest osiągnięcie właściwego poziomu organizacyjnego i technicznego, który:

1. Maksymalnie ograniczy występowanie zagrożeń dla bezpieczenstwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ewentualnego ich wykorzystania.
2. Zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych (niepublicznych) oraz jawnych (publicznych).
3. Zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów informatycznych przetwarzających informacje.

4. Zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa podmiotu, jego interesów, posiadanych i powierzonych jemu informacji oraz będzie gwarantem właściwej ochrony informacji oraz ciągłości procesu ich przetwarzania.

Administrator Danych Osobowych odpowiada za:

1. Przeszkolenie instruktażowe pracowników w zakresie związanym z bezpieczeństwem informacji na stanowiskach pracy.
2. Przestrzeganie zasad bezpieczeństwa informacji przez podległych mu pracowników.
3. Identyfikowanie i dokumentowanie zagrożeń istotnych dla bezpieczeństwa informacji.
4. Przeprowadzanie audytów zgodności systemu zarządzania bezpieczeństwem informacji.
5. Zatwierdzenie warunków technicznych i organizacyjnych służących bezpieczeństwu informacji, w tym ochronę danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem obowiązujących regulacji prawnych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
6. Cele, zakres oraz metody przetwarzania i ochrony informacji, w tym danych osobowych.
7. Właściwą realizację praw osób, których dane przetwarza.
8. Realizację obowiązku informacyjnego.

Kompetencje i odpowiedzialność w obszarze zarządzania bezpieczeństwem informacji

Obowiązki Administratora Danych:

1. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów, merytorycznie poprawne i adekwatne w stosunku do celów.
2. Wyznacza osobę, odpowiedzialną za bezpieczeństwo danych osobowych.
3. Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.
4. Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego zestawu komputerowego.
5. Opracowuje instrukcję określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
6. Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych oraz uprawnionych do dostępu w poszczególnych systemach.
7. Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
8. Odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem danych, nielegalnym ujawnieniem danych w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

9. Zobowiązuje pracowników sporządzających projekty umów do zawierania w nich projektów umów powierzenia danych zgodnie z wymaganiami ochrony danych osobowych oraz bezpieczeństwa informacji w stopniu właściwym do zakresu umowy oraz ewidencjonowanie ich w stosownym rejestrze umów powierzenia danych.
10. Zgłasza Inspektora Ochrony Danych Osobowych.

Obowiązki Administora Systemu Informatycznego:

1. Zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa.
2. Doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem.
3. Przydziela identyfikatory (loginy) użytkownikom systemu Informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu.
4. Nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu.
5. Zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych.
6. Prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

Obowiązki Kierowników Komórek Organizacyjnych:

1. Zarządzają zasobem danych osobowych w ramach zadań realizowanych przez swoją komórkę.
2. Występują z wnioskiem do ADO o nadawanie upoważnień do przetwarzania danych osobowych podległym pracownikom.
3. Zgłaszają do ADO zamiar utworzenia procesu przetwarzania danych osobowych oraz informacji dotyczących zmian w zakresie i sposobach przetwarzania tego zbioru.
4. Realizują proces udostępniania danych osobowych innemu podmiotowi lub osobie, której dane dotyczą.
5. Wypełniają obowiązki dotyczące obszaru przetwarzania, wykazu osób upoważnionych do przetwarzania danych osobowych, zastosowania zabezpieczeń zbiorów.
6. Prowadzą ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w podległej komórce organizacyjnej, z uwzględnieniem zakresu odpowiedzialności za ochronę tych danych w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.
7. Prowadzą w podległej komórce organizacyjnej nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe generowane przez system informatyczny,
8. Dopilnowują, aby monitory stanowisk dostępu do danych osobowych w podległej komórce organizacyjnej były tak ustawione, aby uniemożliwić postronnym osobom wgląd w dane oraz dopilnowanie stosowania zasady „czystego monitora" na tych stanowiskach,
9. Zapoznają pracowników mających dostęp do danych osobowych z przepisami dotyczącymi ochrony danych osobowych.

Obowiązki użytkownika systemu informacji

1. Użytkownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą Dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji, regulaminami i instrukcjami wewnętrznymi.
2. Ochrona danych przed dostępem osób nieupoważnionych.
3. Ochrona danych przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją.
4. Ochrona nośników magnetycznych i optycznych oraz wydruków komputerowych przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem.
5. Utrzymywanie w tajemnicy powierzonych identyfikatorów, haseł, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia.
6. Archiwizowanie danych zgodnie z instrukcją.
7. Użytkownik obsługujący system informatyczny w obszarze przyznanego mu dostępu do systemu zobowiązany jest do sprawdzania czy nie wprowadzono nieautoryzowanych aplikacji oraz zmian w zainstalowanych aplikacjach.
8. Zabrania się pod rygorem odpowiedzialności służbowej i karnej ujawniania danych, kopiowania baz danych lub ich części poza przewidzianymi kopiami zapasowymi.
9. Zabrania się wykorzystywania sprzętu komputerowego i sieci komputerowej do celów prywatnych.
10. Zabrania się używania prywatnych komunikatorów.
11. Zabrania się ściągania i wysyłania plików (filmów, muzyki itp.) niezwiązanych z obowiązkami zawodowymi.
12. Zabrania się korzystania z nośników nieznanego pochodzenia.
13. Zabrania się instalowania jakiegokolwiek oprogramowania bez wiedzy ASI.
14. Dopuszcza się wykorzystanie zarejestrowanych pamięci pendrive lub innych nośników do przenoszenia informacji wewnątrz siedziby jednostki, a także za zgodą i wcześniejszym sprawdzeniem nośnika przez administratora sieci, poza siedzibę w ściśle określonym celu.
15. W celu zachowania bezpieczeństwa wszelkie dane indywidualne i funkcyjne przechowywane są na dyskach lokalnych komputerów użytkowników, zaś kopie na dyskach sieciowych w lokalnej sieci komputerowej.
16. Zaleca się robienie kopii zapasowych ważnych plików i baz danych, jeśli nie są realizowane centralnie. Kopie należy wykonywać na udziałach sieciowych.
17. Użytkownik jest zobowiązany do zachowania porządku na biurku w trakcie pracy oraz zabezpieczenia wszystkich dokumentów po jej zakończeniu.
18. Użytkownik jest zobowiązany do stosowania zasady „czystego pulpitu" polegającej na blokowaniu stacji poprzez wciśnięcie równocześnie klawisza „Windows" + „l".
19. Wszelkie niepotrzebne dokumenty/brudnopisy należy zniszczyć w niszczarce jeśli zawierają dane osobowe, pieczątki firmowe, podpisy itp.; zabrania się wyrzucania całych dokumentów do śmietnika.

Kontrola dostępu do informacji

Dostęp do informacji podlega ciągłej kontroli, która polega na:

1. Wydzielaniu obszarów przeznaczonych do przechowywania oraz przetwarzania zbiorów danych.
2. Zarządzaniu uprawnieniami poszczególnych użytkowników.
3. Nadzorowaniu działalności stron trzecich, mogących wpłynąć na bezpieczeństwo informacji.
4. Bieżącym informowaniu pracowników o wszelkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji.
5. Wszystkie osoby posiadające dostęp do informacji podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa.

Zarządzanie aktywami i ryzykiem

Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzanie okresowego szacowania ryzyka i opracowanie planów postępowania z ryzykiem. Analiza uzyskanych wyników stanowi podstawę do podejmowania działań w zakresie doskonalenia ochrony aktywów. Identyfikowanie ryzyk polega na możliwym rozpoznaniu zagrożeń, które mogą wpływać na bezpieczeństwo informacji.

Na szacowanie ryzyka składają się: analiza ryzyka (identyfikowanie, estymacja), ocena ryzyka. W szacowaniu ryzyka określa się wartość aktywów informacyjnych, identyfikuje się mające zastosowanie zagrożenia oraz istniejące (lub mogące zaistnieć) podatności, identyfikuje się istniejące zabezpieczenia i ich wpływ na zidentyfikowane ryzyko, określa się możliwe następstwa oraz na końcu wskazuje się priorytety uzyskanych ryzyk i ustala ich kolejność zgodnie z kryteriami oceny ryzyka wyznaczonymi podczas ustanawiania kontekstu.

Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych

ADO zapewnia, że wszystkie procesy związane z pozyskaniem, rozwojem bądź utrzymaniem systemów informacyjnych, w tym systemów i aplikacji informatycznych własnych i/lub wykonawców, wykorzystywanych wewnętrznie w podmiocie prowadzone jest w sposób nadzorowany, gwarantujący utrzymanie odpowiedniego poziomu bezpieczeństwa informacji.

Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych u ADO obejmuje:

1. uwzględnianie wymogów bezpieczeństwa podczas zakupu lub budowy nowych systemów informatycznych,
2. dopuszczenie nowego systemu do eksploatacji poprzedzone jest zawsze fazą testów funkcjonalnych i testów bezpieczeństwa,
3. wdrożenie mechanizmów aktualizacji oprogramowania,
4. wdrożenie procedur kontroli zmian oprogramowania.

Za zapewnienie właściwego przebiegu procesu pozyskiwania, rozwoju i utrzymania systemów informatycznych ADO odpowiedzialny jest administrator system informatycznego.

Deklaracja ochrony własności intelektualnej

W podmiocie zostały wdrożone mechanizmy zapobiegające naruszeniom prawa powszechnego związanego z ochroną własności intelektualnej. Stacje robocze zostały zabezpieczone przed możliwością instalowania oprogramowania z naruszeniem licencji.

Prowadzona jest bieżąca ewidencja sprzętu komputerowego i licencji oprogramowania.

Nadzorowana jest także własność intelektualna powierzona lub przekazana przez osoby trzecie.

Bezpieczeństwo zasobów ludzkich

Podmiot zatrudnia kompetentną kadrę pracowniczą do realizacji wyznaczonych zadań. Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów. Realizacja postawionego celu możliwa jest dzięki wdrożonym zasadom rekrutacji pracowników.

Prowadzone są szkolenia dla pracowników oraz kontrahentów z zakresu wdrożonych zasad i procedur bezpieczeństwa informacji, które zakończone jest złożeniem oświadczenia o zachowaniu poufności podczas współpracy oraz po jej zakończeniu.

Do przetwarzania informacji dopuszczone są tylko osoby posiadające stosowne upoważnienie.

Bezpieczeństwo fizyczne i środowiskowe

Celem bezpieczeństwa fizycznego jest zapewnienie ochrony przed nieautoryzowanym dostępem fizycznym, uszkodzeniami lub zakłóceniami w siedzibie urzędu poprzez wprowadzenie technicznych zabezpieczeń.

Utrzymanie ciągłości działania

Zastosowanie odpowiednich środków organizacyjnych i technicznych umożliwi utrzymanie ciągłości działania, odtworzenie procesów oraz wznowienie działania systemów w sytuacji kryzysowej.

Na utrzymanie ciągłości działania składają się następujące zasady:

1. zastosowanie działań naprawczych,
2. ustalenie reguł współpracy z innymi podmiotami,
3. opracowanie planu awaryjnego,
4. ciągłe doskonalenie opracowanych procedur, planów oraz środków organizacyjnych i technicznych.

Naruszenie bezpieczeństwa informacji

W celu utrzymania wysokiego poziomu bezpieczeństwa informacji w podmiocie podejmuje się odpowiednie działania wobec sytuacji, które są związane z jego naruszeniem. Każdy przypadek naruszenia dostępności, poufności i integralności informacji w podmiocie jest rejestrowany i poddawany odpowiedniej procedurze postępowania. W systemie zarządzania bezpieczeństwem informacji konieczne jest zaangażowanie wszystkich

pracowników, w tym niezwłoczna interwencja na różne niepokojące sygnały i zdarzenia.

Podstawy prawne i organizacyjne

1. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (Dz. U. RPUE.L.2016.194.1),
2. 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) (Dz. U. UE.L.2016.119.1),
3. Norma PN-ISO/IEC 27005:2014-01 Technika informatyczna - Techniki bezpieczeństwa -Zarządzanie ryzykiem w bezpieczeństwie informacji,
4. Norma PN-ISO/IEC 27001:2014-12 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania,
5. Norma PN-ISO/IEC 27002:2014-12 Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji.

Postanowienia końcowe

W sprawach nieuregulowanych niniejszą procedurą odpowiednie zastosowanie mają reguły i procedury zawarte w dokumentach powiązanych podmiotu.

Polityka Bezpieczeństwa Informacji wchodzi w życie z dniem podpisania.

Zapisy tego dokumentu wchodzą w życie z dniem 12.04.2022r.

Sporządził: Marcin Misztal – Inspektor Ochrony Danych Osobowych.

Administrator Danych Osobowych:

WÓJT
12.04.2022 Jacek Mościcki

Data, podpis i pieczątka