ZARZĄDZENIE NR 312/23
PREZYDENTA MIASTA SZCZECIN
z dnia 28 czerwca 2023 r.

w sprawie określenia zasad bezpieczeństwa informacji oraz wytycznych dla Polityki Bezpieczeństwa Informacji Urzędu Miasta Szczecin

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2023 r. poz. 40 i 572), art. 13 ust. 1 ustawy 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57), oraz art. 24 ust. 2 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 z 04.05.2016, s. 1, Dz. Urz. UE L 127 z 23.05.2018, s. 2 oraz Dz. Urz. UE. L 74 z 04.03.2021, s. 35) **zarządzam, co następuje:**

§ 1. Ilekroć w Zarządzeniu jest mowa o:

1) ADO - należy przez to rozumieć Administratora danych - osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
2) ASI - należy przez to rozumieć Administratora Systemu Informacyjnego - osoby wyznaczone przez ADO, odpowiedzialne za sprawne działanie systemów informatycznych, reagowanie na zagrożenia oraz administrowanie infrastrukturą informatyczną Urzędu i narzędziami programowania i systemami;
3) ASU – Administratora Systemu Użytkowego - należy przez to rozumieć osobę wyznaczoną przez Dyrektora Wydziału Informatyki do pełnienia takiej funkcji, odpowiedzialną za funkcjonowanie systemów użytkowych, nadawanie, odbieranie uprawnień do poszczególnych modułów lub funkcji systemu użytkowego;
4) aktywach – należy przez to rozumieć wszystko co ma wartość dla Urzędu Miasta Szczecin w szczególności zasoby: osobowe, majątkowe, rzeczowe;
5) aktywach informacyjnych – należy przez to rozumieć wszelkie zasoby oraz systemy, infrastrukturę, urządzenia i oprogramowanie wykorzystywane w celu przetwarzania informacji;
6) bezpieczeństwie informacji – należy przez to rozumieć zapewnienie poufności, integralności i dostępności aktywów informacyjnych;
7) ciągłości działania – należy przez to rozumieć zdolność jednostki do wykonywania zadań publicznych (przywrócenia jej działań) w trakcie zakłócenia przez akceptowalne ramy czasowe (okres reagowania na incydenty);
8) czynności przetwarzania – należy przez to rozumieć zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane;
9) dostępności – należy przez to rozumieć właściwość polegającą na pozostawaniu informacji jako dostępnej, użytecznej na żądanie autoryzowanej osoby lub podmiotu;
10) elektronicznych Nośnikach Informacji (ENI) - należy przez to rozumieć zewnętrzne nośniki danych, w szczególności płyty CD, DVD, Pendrive, pamięci typu FLASH, które muszą zostać zgłoszone i zarejestrowane przez ASI;
11) firewall (zapora sieciowa) – należy przez to rozumieć urządzenie zabezpieczające sieć, które monitoruje przychodzący i wychodzący ruch sieciowy i decyduje o jego przepuszczeniu lub zablokowaniu w oparciu o zestaw określonych zasad;

12) haśle - należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;

13) incydencie bezpieczeństwa – należy przez to rozumieć niepożądane zdarzenie lub serię zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań kluczowych i mogą mieć negatywny wpływ na bezpieczeństwo aktywów informacyjnych;

14) identyfikatorze - należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący użytkownika upoważnionego do przetwarzania danych osobowych w systemie informatycznym;

15) integralności – należy przez to rozumieć właściwość polegająca na zapewnieniu dokładności i kompletności informacji;

16) intranecie - należy przez to rozumieć sieć komputerową, ograniczającą się do komputerów w Urzędzie, umożliwiającą korzystanie przez użytkowników usług stron www czy poczty elektronicznej;

17) jednostce – należy przez to rozumieć jednostkę organizacyjną Urzędu (wydział, biuro, samodzielne stanowisko);

18) kierowniku - należy przez to rozumieć Kierownika jednostki organizacyjnej Urzędu;

19) LAN - należy przez to rozumieć lokalną sieć łączącą komputery na określonym obszarze np. w Urzędzie;

20) osobie upoważnionej do przetwarzania danych osobowych – należy przez to rozumieć osobę, która upoważniona została do przetwarzania danych osobowych poprzez upoważnienie na piśmie przez ADO lub upoważnioną przez niego osobę;

21) podatności - należy przez to rozumieć pewnego rodzaju słabość, odnosi się do braku odporności jednostki na wskutek wrogiego środowiska. Zjawisko podatności wykorzystywane jest przez zagrożenia i prowadzi do strat;

22) podmiocie zewnętrznym - należy przez to rozumieć inną organizację, instytucję, inny Urząd;

23) PBI – należy przez to rozumieć politykę bezpieczeństwa informacji – dokument o znaczeniu strategicznym dającym możliwość efektywnego zarządzania bezpieczeństwem informacji w Urzędzie;

24) poufności – należy przez to rozumieć właściwość polegającą na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom lub podmiotom;

25) privacy by design - należy przez to rozumieć wdrażanie odpowiednich środków technicznych i organizacyjnych przez Administratora danych osobowych zarówno przed przystąpieniem do przetwarzania (tj. w fazie planowania / projektowania sposobów przetwarzania) danych osobowych, jak i w czasie samego przetwarzania, mająca na celu zapewnienie zgodności z RODO;

26) publicznej sieci telekomunikacyjnej - należy przez to rozumieć sieć w rozumieniu ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648, 1933 i 2581);

27) raporcie - należy przez to rozumieć przygotowane przez system informatyczny zestawienie zakresu i treści przetwarzanych danych;

28) rozliczalności - należy przez to rozumieć właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

29) RODO – należy przez to rozumieć 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. Urz. UE L 119 z 04.05.2016, s. 1, Dz. Urz. UE L 127 z 23.05.2018, s. 2 oraz Dz. Urz. UE. L 74 z 04.03.2021, s. 35);

30) serwisancie – należy przez to rozumieć pracownika Referatu Wsparcia Użytkowników WInf, firmę lub pracownika firmy zajmującej się instalacją, naprawą, konserwacją sprzętu komputerowego lub systemu/ programu komputerowego;

31) sieci lokalnej VPN - należy przez to rozumieć połączenie jednostek komputerowych pracujących w Urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych, realizowane przez sieć prywatną lub sieć publiczną, taką jak Internet. Połączenie jest ustanowione logicznie (wirtualnie) pomiędzy dwoma lub wieloma węzłami sieci komputerowej umożliwiające bezpieczną łączność pomiędzy uczestnikami tej sieci;

32) słownikach systemowych - należy przez to rozumieć składniki programu (systemu) jako obiekty i procedury służące do gromadzenia stale powtarzających się informacji np. słowniki kodów pocztowych, nazw, ulic miejscowości, organizacji oraz ich udostępniania;

33) systemie informatycznym – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

34) systemie pocztowym - należy przez to rozumieć oprogramowanie zgodne ze standardami poczty elektronicznej w Internecie służące do wymiany informacji oraz zarządzania kalendarzami współdzielonymi;

35) SZBI – należy przez to rozumieć System Zarządzania Bezpieczeństwem Informacji - zbiór procedur, wytycznych oraz przydzielonych zasobów oraz aktywności, zarządzanych wspólnie przez Urząd w celu ochrony swoich zasobów informacyjnych;

36) środkach technicznych i organizacyjnych – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;

37) umowie powierzenia - należy przez to rozumieć umowę zawartą na piśmie przez ADO z podmiotem zewnętrznym, któremu zostało powierzone przetwarzanie danych w rozumieniu art. 28 RODO;

38) Urzędzie – należy przez to rozumieć Urząd Miasta Szczecin;

39) urządzeniach mobilnych – należy przez to rozumieć (przenośne) urządzenia elektroniczne pozwalające na przetwarzanie, odbieranie oraz wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią, w szczególności laptop, tablet, smartfon;

40) uwierzytelnianiu – należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

41) usłudze – należy przez to rozumieć czynności niematerialne (np. porada techniczna, audyt, szkolenie) lub materialne (produkcja, wykonawstwo, dostarczanie);

42) użytkowniku - należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych zarówno w systemach tradycyjnych, w tym systemie informatycznym (m.in. pracownik, praktykant, stażysta, osoba wykonująca pracę na podstawie umowy cywilnoprawnej);

43) WInf – należy przez to rozumieć Wydział Informatyki Urzędu;

44) właścicielu aktywa (zasobu) – należy przez to rozumieć osobę w strukturze organizacyjnej, odpowiedzialną za nadzorowanie, rozwój, utrzymanie, korzystanie i bezpieczeństwo aktywów;

45) zabezpieczeniu danych w systemie informatycznym – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

46) zdarzeniu związanym z bezpieczeństwem informacji – należy przez to rozumieć określony stan, który wskazuje na możliwe naruszenie bezpieczeństwa danych osobowych, błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z bezpieczeństwem danych osobowych.

§ 2. 1. W Urzędzie wprowadza się zasady bezpieczeństwa informacji oraz wytyczne dla Polityki Bezpieczeństwa Informacji.

2. Bezpieczeństwo informacji oraz systemów, w których są one przetwarzane jest jednym z kluczowych elementów zapewniających realizację zadań Urzędu.

§ 3. System Zarządzania Bezpieczeństwem Informacji.

1. Urząd deklaruje, że SZBI, w tym PBI, został opracowany na podstawie rozporządzenia 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 (Dz. U. z 2017 r. poz. 2247, oraz z 2019 r. poz. 848) oraz polskimi normami stanowiącymi wytyczne:

1) PN-EN ISO/IEC 27001:2017 (Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji - Wymagania);
2) PN-EN ISO/IEC 27002:2017 (Technika Informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji) – w odniesieniu do ustanawiania zabezpieczeń;
3) PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-EN ISO/IEC 27001:2017);
4) PN-ISO/IEC 24762:2010 Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.

2. Celem wdrożonego w Urzędzie SZBI jest osiągnięcie właściwego poziomu organizacyjnego i technicznego, który:

1) maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, wynikających z celowej bądź przypadkowej działalności człowieka oraz ich ewentualnego wykorzystania na szkodę Urzędu;
2) zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów informatycznych przetwarzających informacje;
3) zapewni dokładność i kompletność informacji oraz metod jej przetwarzania (zasada integralności informacji);
4) zapewni, że informacja będzie udostępniana jedynie osobom upoważnionym (zasada poufności informacji);
5) zapewni, że osoby upoważnione będą miały dostęp do informacji i związanych z nią aktywów zawsze wtedy, gdy istnieje taka potrzeba (zasada dostępności informacji);
6) zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa działania Urzędu, jego interesów, posiadanych i powierzonych jemu informacji oraz będzie gwarantem właściwej ochrony informacji oraz ciągłości procesu ich przetwarzania.

§ 4. Zakres SZBI.

1. Zakres ustanowionego SZBI obejmuje:

1) odpowiedzialność ADO, IOD, ASI oraz użytkowników;
2) zarządzanie pracą użytkownika w systemach teleinformatycznych tj. nadawanie, modyfikacja i cofanie uprawnień oraz rozpoczęcie, zawieszenie/odwieszenie i zakończenie pracy użytkownika w systemie teleinformatycznym;
3) zarządzanie bezpieczeństwem w systemach teleinformatycznych;
4) zabezpieczenia kryptograficzne;
5) zarządzanie bezpieczeństwem i komunikacją w sieciach teleinformatycznych;
6) ochrona przed szkodliwym oprogramowaniem;

7) postępowanie z urządzeniami mobilnymi;

8) nadzór nad oprogramowaniem oraz zarządzanie zmianami i konfiguracją;

9) inwentaryzację sprzętu;

10) postępowanie z nośnikami;

11) projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych;

12) informacje - obejmujące dane osobowe, które Urząd przetwarza w związku z prowadzoną działalnością; informacje niezbędne do ociągnięcia celów Urzędu,

13) operacje przetwarzania: czynności w procesie przetwarzania danych osobowych, które Urząd jest zobowiązany podejmować/utrzymywać, by osiągać cele strategiczne Urzędu przy jednoczesnym zapewnieniu bezpieczeństwa przetwarzanych informacji w Urzędzie.

2. Cele i dobór zabezpieczeń w SZBI prowadzony jest w oparciu o aktualne wymogi prawa powszechnie obowiązującego, zalecenia polskich norm z rodziny ISO 27000 oraz wyniki monitorowania Systemu, w szczególności wyniki szacowania ryzyka w bezpieczeństwie informacji.

3. Stosowane zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie, zapewniając wymagany poziom bezpieczeństwa informacji.

4. Informacje przetwarzane w Urzędzie objęte zakresem ustanowionego SZBI klasyfikowane są w grupach:

1) informacje chronione na podstawie powszechnie obowiązujących aktów prawa, takie jak: dane osobowe, kadrowe, finansowo-księgowe, informacje zawarte w aktach spraw uzyskane w trakcie i dla potrzeb postępowań, opinie biegłych, oferty przetargowe przed ich otwarciem, polityki bezpieczeństwa, wewnętrzne procedury dotyczące bezpieczeństwa, strategiczne projekty, informacje zastrzeżone do wyłącznej wiadomości ADO oraz inne tajemnice ustawowo chronione (tajemnice powołane na mocy ustaw, których obowiązek ochrony wynika z tychże ustaw) – chronione ze względu na poufność, integralność i dostępność;

2) pozostałe informacje przetwarzane w Urzędzie, w szczególności informacje, których zakres i tryb udostępniania określa ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej.

5. SZBI nie obejmuje w szczególności:

1) przetwarzania przez Urząd poza systemami teleinformatycznymi, za wyjątkiem prowadzenia dokumentacji systemów teleinformatycznych oraz dokumentacji związanej z administracją i eksploatacją systemów teleinformatycznych;

2) bezpieczeństwa informacji w ramach procesów zarządzania personelem w zakresie innym niż eksploatacja systemów teleinformatycznych;

3) przetwarzania informacji niejawnych w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;

4) aktywów służących do przetwarzania informacji niejawnych, w szczególności systemów teleinformatycznych, sprzętu oraz pomieszczeń, w których przetwarzane są informacje niejawne.

6. SZBI podlega przeglądowi w przypadku poważnego naruszenia systemów zabezpieczeń, pojawienia się nowych i istotnych rodzajów ryzyka, zmian regulacji prawnych mających zastosowanie lub wprowadzenie nowych systemów informatycznych lub zmian infrastruktury technicznej. Ponadto SZBI jest przeglądany w cyklu rocznym, tak by zapewnić jego skuteczność w funkcji zachodzących zmian.

7. Co najmniej raz w roku dokonuje się przeglądu zarządzania, wynikiem przeglądu są udokumentowane decyzje najwyższego kierownictwa w zakresie możliwości doskonalenia SZBI i potrzeb jego zmiany.

§ 5. Role i odpowiedzialność w SZBI.

1. W ramach ustanowionego SZBI, role i odpowiedzialność w zakresie bezpieczeństwa informacji zostały zidentyfikowane i przypisane.

2. ADO wytycza kierunek działania systemu ochrony danych oraz podejmuje decyzje w kluczowych sprawach związanych z bezpieczeństwem informacji.

3. ADO odpowiedzialny jest za:

1) zapewnienie zasobów niezbędnych do bieżącego funkcjonowania, utrzymania i ciągłego monitorowania oraz doskonalenia SZBI;
2) zapewnienie, że PBI oraz cele bezpieczeństwa informacji są ustanowione i zgodne z kierunkiem strategicznym Urzędu;
3) zapewnienie, że SZBI osiąga zamierzone wyniki;
4) promowanie ciągłego doskonalenia SZBI;
5) komunikowanie znaczenia skutecznego zarządzania bezpieczeństwem informacji i zgodności z wymaganiami SZBI,
6) kierowanie i wspieranie osób przyczyniających się do osiągnięcia skuteczności SZBI;
7) wspieranie innych członków Urzędu w wykazywaniu przywództwa odpowiednio do obszarów ich odpowiedzialności;
8) definiowanie ról, przypisanie odpowiedzialności i uprawnień w Urzędzie;
9) udział w przeglądach zarządzania i doskonaleniu SZBI;
10) zapewnienie warunków aktualizacji wobec regulacji wewnętrznych w stosunku do zmieniającego się otoczenia;
11) zapewnienie aktualności inwentaryzacji sprzętu i oprogramowania co do rodzaju i konfiguracji;
12) umożliwienie/wykonanie okresowej analizy ryzyka wraz z adekwatnymi do wyniku działaniami minimalizującymi ryzyko;
13) podejmowanie działań zapewniających weryfikację stosownych uprawnień wobec osób uczestniczących w procesie przetwarzania danych;
14) zapewnienie warunków technicznych, organizacyjnych i fizycznych ze szczególnym naciskiem na:
    a) szkolenia obejmujące tematykę zagrożeń, skutków naruszenia bezpieczeństwa informacji oraz zapewnienie bezpieczeństwa wraz z minimalizacją ryzyka błędów ludzkich,
    b) ochrona przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
15) zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z zasadami przetwarzania danych osobowych określonymi w RODO,
16) wytyczanie przez polityki kierunków działania Urzędu w kontekście ochrony informacji;
17) wdrożenie procedur ochrony danych osobowych;
18) prawidłową realizację praw osób, których dane dotyczą;
19) zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich;
20) współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań;
21) stosowanie umów powierzenia;
22) nadawanie upoważnień do przetwarzania danych osobowych;
23) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

24) zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultacje z organem nadzorczym;

25) dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych;

26) zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą.

4. Odpowiedzialność za bezpieczeństwo informacji ponoszą wszyscy pracownicy Urzędu, praktykanci, stażyści, wolontariusze i podmioty objęte zakresem ustanowionego SZBI.

5. Przedmiotowa odpowiedzialność polega na przestrzeganiu wymagań prawa powszechnie obowiązującego, zapisów niniejszego dokumentu oraz pozostałych wymogów wskazanych w dokumentacji bezpieczeństwa, w szczególności na:

1) realizacji przypisanych zadań w obszarze bezpieczeństwa informacji;

2) ochronie powierzonych informacji i zabezpieczeniu aktywów wspierających ich przetwarzanie;

3) nieudostępnianiu informacji osobom nieuprawnionym;

4) zachowaniu w tajemnicy chronionych informacji oraz sposobów ich zabezpieczenia;

5) informowaniu o podejrzeniu/wszelkich zauważonych nieprawidłowościach, które mogą mieć wpływ na bezpieczeństwo informacji.

6. W celu realizacji działań, o których mowa w ust. 5, kluczowe role i odpowiedzialność w zakresie bezpieczeństwa informacji została przypisana do obowiązków osób pełniących funkcje w Urzędzie, w szczególności do:

1) **ASI** – który odpowiada za:

a) definiowanie i wdrażanie zabezpieczeń technicznych w Urzędzie,

b) uczestnictwo w procesie analizy ryzyka w roli eksperta,

c) utrzymywanie zasobów i infrastruktury teleinformatycznej,

d) nadzór nad dostępami do zasobów w Urzędzie,

e) monitorowanie i utrzymanie zasobów i sieci teleinformatycznych Urzędu,

f) zarządzanie dostępnością, potencjałem wykonawczym oraz zdarzeniami,

g) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego,

h) reakcję na zagrożenie i incydenty bezpieczeństwa w Urzędzie,

i) wsparcie i wykonanie elementów składających się na plany ciągłości działania w Urzędzie,

j) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,

k) ścisłą współpracę z IOD w zakresie przestrzegania bezpieczeństwa informacji i zasad przetwarzania danych osobowych w systemach informatycznych,

l) opracowywanie oraz aktualizację ogólnego opisu technicznych środków bezpieczeństwa wdrożonych w strukturze ADO,

m) identyfikację i analizę zagrożeń oraz ocenę ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych;

n) sprawowanie nadzoru nad kopiami zapasowymi;

o) inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,

p) podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych,

q) dokonywanie cyklicznych przeglądów aktualności i stosowania procedur z zakresu przetwarzania danych w systemach informatycznych, na podstawie opracowanego planu przeglądów.

2) **IOD**, który odpowiada za:

a) nadzór nad stosowaniem środków bezpieczeństwa w systemach teleinformatycznych,

b) nadzór nad przestrzeganiem procedur bezpieczeństwa przez ADO oraz użytkowników,

c) proponowanie i uzgadnianie procedur w systemach teleinformatycznych z ADO oraz ASI,

d) informowanie kierownictwa Urzędu oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i doradzanie im w tej sprawie,

e) monitorowanie przestrzegania RODO, innych przepisów branżowych o ochronie danych oraz wewnętrznych polityk w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,

f) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,

g) podejmowanie działań zwiększających świadomość pracowników ADO w zakresie obowiązków wynikających z RODO lub przyjętych procedur,

h) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,

i) udział w procesie realizacji praw osób, których dane dotyczą,

j) udział w procesach związanych z naruszeniami ochrony danych osobowych (koordynacja);

3) **ASU** – który odpowiada za:

a) nadawanie, aktualizację i odbieranie uprawnień do poszczególnych modułów lub funkcji systemu,

b) testowanie nowych wersji systemu,

c) sprawowanie nadzoru nad prawidłowym działaniem systemu,

d) zgłaszanie dostawcy systemu uwag użytkowników oraz nowych funkcjonalności;

4) **Właścicieli zasobów (aktywów) informacyjnych** – kierownicy, którzy odpowiadają za:

a) decyzję o przydzielaniu zasobów informacyjnych użytkownikom,

b) wyznaczenie właścicieli procesów informacyjnych,

c) pełnienie nadzoru właścicielskiego (w imieniu Urzędu) nad danymi osobowymi, niezależnie od ich formy przetwarzania,

d) przeprowadzanie oceny skutków przetwarzania danych osobowych w podległych im procesach zgodnie z procedurą domyślnej ochrony danych osobowych (privacy by default) oraz ochrony danych osobowych na etapie projektowania produktu lub usługi (privacy by design),

e) aktualizowanie rejestru czynności przetwarzania danych osobowych w podległych im procesach,

f) inicjowanie zawarcia umów powierzenia z podmiotami, którym dane mają zostać powierzone do dalszego przetwarzania przez Urząd,

g) zgłaszanie naruszeń ochrony danych osobowych, zgodnie z procedurą zarządzania incydentami bezpieczeństwa informacji,

h) koordynowanie działań w zakresie bezpieczeństwa systemów informacyjnych, w szczególności za opracowanie i akceptację wyników analizy ryzyka aktywów informacyjnych, za które odpowiada właściciel procesu - zgodnie z procesem analizy ryzyka,

i) akceptowanie warunków eksploatacji systemów proponowanych przez ASI,

j) współtworzenie regulacji szczegółowych SZBI w zakresie systemu, którego jest właścicielem, w tym zatwierdzanie procedury i zasad obsługi praw dostępu (wszelkie regulacje muszą być zgodne z zasadami polityki bezpieczeństwa oraz SZBI),

k) realizację praw osób, których dane są przetwarzane, w podległych im procesach zgodnie z zaleceniami IOD,

l) wnioskowanie o udzielenie i odbieranie praw dostępu do systemów użytkownikom, zgodnie z Procedurą zarządzania uprawnieniami do zasobów/systemów informatycznych Urzędu stanowiącą **Załącznik Nr 24 do Zarządzenia;**

5) **Właścicieli procesów informacyjnych** – użytkownicy, którzy odpowiedzialni są za poszczególne procesy przetwarzania danych osobowych w jednostce.

7. W zakresie wykonywanych obowiązków i zadań niezależnie od siebie ASI i IOD mogą:

1) wydawać wytyczne, rekomendacje, opinie;

2) żądać udzielenia wyjaśnień od wszystkich pracowników jednostek Urzędu w zakresie zdarzeń związanych z bezpieczeństwem informacji i ochroną danych osobowych.

8. ADO może wyznaczyć Pełnomocnika ds. SZBI, który odpowiadać będzie za ogólny nadzór nad działaniem i efektywnością SZBI, w szczególności za:

1) definiowanie, ciągłe doskonalenie i nadzór nad SZBI;

2) koordynowanie wszystkich działań składających się na SZBI;

3) komunikowanie SZBI w Urzędzie;

4) kontakt z organami władzy i grupami zainteresowań z obszaru SZBI;

5) koordynowanie procesu zarządzania ryzykiem w bezpieczeństwie informacji.

§ 6. Polityka Bezpieczeństwa Informacji.

1. Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego orazpostanowienia RODO, w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się w Urzędzie Politykę Bezpieczeństwa Informacji, stanowiącą **Załącznik Nr 1** do zarządzenia.

2. Nadrzędnym celem PBI i innych instrukcji oraz regulaminów określonych w Zarządzeniu jest zagwarantowanie, że w Urzędzie:

1) stosuje się ogólne zasady przetwarzania wynikające z RODO;

2) zapewnia się, aby dane przetwarzane były zgodnie z prawem;

3) zapewnia się, aby przestrzegane były prawa osób, których dane są przetwarzane;

4) wypełnia się ogólne obowiązki w zakresie przetwarzania danych ciążących na ADO i podmiocie przetwarzającym;

5) zapewnia się bezpieczeństwo przetwarzania danych uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób;

6) stosuje się 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;

7) zapewnia się kontrolę nad przetwarzaniem danych w postaci monitorowania przestrzegania przepisów i przyjętych procedur przetwarzania;

8) testuje, mierzy i ocenia się skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych (audyty, sprawdzenia, kontrole itd.).

3. Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej lub innej).

4. Z dokumentem są zobowiązani zapoznać się wszyscy pracownicy Urzędu, posiadający dostęp do danych osobowych i informacji ustawowo chronionych.

§ 7. Cele bezpieczeństwa informacji.

1. Do głównych celów bezpieczeństwa informacji w Urzędzie należy:

1) zapewnienie bezpieczeństwa aktywów informacyjnych Urzędu (w tym ochrona wizerunku i relacji z podmiotami zewnętrznymi), zgodnie z wymogami obowiązującego prawa oraz adekwatnie do wyników szacowania ryzyka w bezpieczeństwie informacji;

2) usprawnienie funkcjonowania Urzędu poprzez uporządkowanie zasad przetwarzania informacji oraz zarządzanie aktywami informacyjnymi w zorganizowany sposób, tak aby ułatwić ciągłe doskonalenie i dostosowanie do bieżących celów Urzędu;

3) minimalizowanie ryzyka i ograniczanie skutków utraty bezpieczeństwa informacji;

4) maksymalne ograniczenie występowania zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich wykorzystania na szkodę Urzędu;

5) zapewnienie poprawnego i bezpiecznego funkcjonowania wszystkich systemów informatycznych przetwarzających informacje;

6) stałe podnoszenie świadomości pracowników w zakresie bezpieczeństwa informacji.

2. W ramach realizacji celów, o których mowa w ust. 1, adekwatnie do poziomu zidentyfikowanych zagrożeń podejmowane są działania w kierunku osiągnięcia poziomu organizacyjnego i technicznego Urzędu, który w szczególności zapewni:

1) zachowanie poufności przetwarzanych informacji;

2) integralność informacji oraz ich dostępność;

3) uwzględnienie dodatkowych atrybutów bezpieczeństwa zgodnie z wymaganiami i decyzjami;

4) bezpieczne przetwarzanie informacji, w tym zdolność do podejmowania działań w sytuacjach kryzysowych;

5) przypisanie kompetencji i odpowiedzialności w zakresie bezpieczeństwa informacji;

6) szkolenia oraz otrzymanie odpowiedniego poziomu kompetencji i świadomości pracowników Urzędu;

7) zarządzanie poziomem bezpieczeństwa przetwarzanych informacji;

8) analizę i minimalizację zagrożeń oraz właściwe reakcje w sytuacjach zagrożeń;

9) zarządzanie podatnościami;

10) poprawne i bezpieczne funkcjonowanie systemów przetwarzania informacji;

11) zarządzanie ciągłością działania;

12) zarządzanie incydentami bezpieczeństwa;

13) monitorowanie, podejmowanie działań zapobiegawczych i usprawniających skuteczność przyjętych zasad;

14) zgodność jako unikanie przekroczeń jakichkolwiek przepisów prawa, przyjętych zobowiązań czy posiadanych regulacji wewnętrznych ze szczególnym uwzględnieniem:

a) ochrony własności intelektualnej,

b) ochrony danych osobowych i prywatności osób fizycznych,

c) regulacji dotyczących zabezpieczeń kryptograficznych,

d) zgodność z politykami bezpieczeństwa i standardami ISO.

§ 8. Podstawowe zasady bezpieczeństwa informacji.

1. Dążąc do zabezpieczenia informacji i aktywów wspierających ich przetwarzanie wprowadza się do stosowania podstawowe zasady bezpieczeństwa informacji:

1) zasada asekuracji zabezpieczeń – należy przez to rozumieć, że ochrona zasobów nie może opierać się wyłącznie na jednym mechanizmie zabezpieczenia;

2) zasada indywidualnej odpowiedzialności – należy przez to rozumieć, że Urząd dąży do zapewnienia jednoznacznej odpowiedzialności osób za zasoby im powierzone; wszyscy użytkownicy muszą być świadomi swej odpowiedzialności i konsekwencji, które poniosą, jeżeli zaniedbają swoje obowiązki bądź przekażą swoje uprawnienia innym osobom;

3) zasada adekwatności zabezpieczeń – należy przez to rozumieć, że stosowane zabezpieczenia muszą być adekwatne do zidentyfikowanych zagrożeń;

4) zasada bezpiecznej współpracy z podmiotami zewnętrznymi - należy przez to rozumieć, że dokumenty regulujące współpracę z podmiotami zewnętrznymi (m.in. treść umów i porozumień) zawierające zapisy dotyczące bezpieczeństwa informacji, w tym m.in. klauzule bezpieczeństwa o zachowaniu poufności;

5) zasada czystego biurka – należy przez to rozumieć, że w celu wyeliminowania ryzyka przypadkowego lub celowego odczytania informacji, ich skopiowania, zniszczenia lub zmodyfikowania przez osoby nieuprawnione, opuszczając stanowisko pracy należy usunąć dokumenty zawierające informacje inne niż informacje o charakterze jawnym, umieszczając je w przeznaczonych do tego celu zabezpieczonych meblach biurowych;

6) zasada czystego ekranu - należy przez to rozumieć, że na czas nieobecności dostęp do komputera należy skutecznie blokować, a po zakończeniu pracy komputer wyłączyć, chyba że musi on pracować w trybie ciągłym;

7) zasada najsłabszego ogniwa – należy przez to rozumieć, że poziom bezpieczeństwa informacji wyznacza najsłabsze ogniwo (najsłabiej zabezpieczony element) SZBI;

8) zasada podziału obowiązków i zadań - należy przez to rozumieć, że obowiązki i uprawnienia powinny być tak rozdzielone, aby pojedyncza osoba nie dysponowała pełnią uprawnień do wykonywania zadań w całości;

9) zasada uprawnionego dostępu – należy przez to rozumieć, że korzystanie z aktywów informacyjnych Urzędu odbywać się może tylko w oparciu o formalne uprawnienia do korzystania z wybranych aktywów;

10) zasada wiedzy koniecznej – należy przez to rozumieć, że poszczególne osoby posiadają wiedzę o zasobach Urzędu ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych im zadań;

11) zasada uprawnień koniecznych – należy przez to rozumieć, że każda osoba posiada prawa dostępu do zasobów Urzędu ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych jej obowiązków;

12) zasada doskonalenia SZBI - należy przez to rozumieć, że SZBI jest dostosowywany do zmieniających się warunków w oparciu o wyniki okresowo prowadzonego monitorowania i nadzoru.

2. Dodatkowe zasady bezpieczeństwa mogą zostać określone w pozostałych dokumentach wchodzących w skład dokumentacji bezpieczeństwa.

§ 9. Instrukcja określająca sposób zarządzania systemem teleinformatycznym, służącym do przetwarzania danych.

1. W celu określenia zasad przetwarzania danych osobowych oraz korzystania z Internetu w sieci teleinformatycznej Urzędu, wraz zapewnieniem identyfikacji użytkowników, określeniem obowiązków zabezpieczenia posiadanych zasobów teleinformatycznych wprowadza się Instrukcję Zarządzania Systemem Informatycznym Urzędu służącym do przetwarzania danych osobowych, określoną w **Załączniku Nr 2** do Zarządzenia.

2. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w Urzędzie jest określony w **Załączniku Nr 3** do Zarządzenia.

§ 10. Zarządzanie ryzykiem w bezpieczeństwie informacji.

1. Ocenę ryzyka można przeprowadzić w oparciu o:

1) wszystkie zidentyfikowane zasoby zaangażowane w przetwarzanie danych – podejście rekomendowane lub

2) zidentyfikowane zasoby bezpośrednio powiązane z czynnościami przetwarzania dla których ryzyko jest wysokie.

2. Strategicznym elementem zarządzania aktywami związanymi z przetwarzaniem informacji i bezpieczeństwem informacji w Urzędzie jest przeprowadzanie okresowej analizy ryzyka i opracowanie planu postępowania z ryzykiem.

3. Szczegółowe zasady oceny ryzyka w bezpieczeństwie informacji zostały uregulowane w Procedurze oceny ryzyka z obszaru bezpieczeństwa informacji, stanowiącej **Załącznik Nr 18** do Zarządzenia.

§ 11. Podejście oparte na ryzyku.

1. Zasada podejścia opartego na ryzyku zobowiązuje ADO do:

1) respektowania tego, że RODO szczególny nacisk kładzie na ochronę praw i wolności osób, których dane są przetwarzane;

2) dostosowania środków ochrony przetwarzania danych osobowych do skali ryzyka. Ocenia się je pod kątem utraty poufności, integralności i dostępności danych, biorąc pod uwagę:

   a) zakres, charakter (wrażliwość) danych,

   b) kontekst i cele przetwarzania,

   c) kwestie zapewniania bezpieczeństwa usług przetwarzania (niezawodność, integralność i dostępność systemu przetwarzania),

   d) zapewnianie autentyczności i rozliczalności danych i podmiotów uczestniczących w przetwarzaniu,

3) koncentrowania się na poszukiwaniu środków redukujących prawdopodobieństwo wystąpienia zagrożeń najbardziej dotkliwych oraz środków redukujących skutki ich wystąpienia.

2. W strukturze Urzędu podejście oparte na ryzyku następuje poprzez:

1) przeprowadzanie oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych – uwzględnia się ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

2) dokonywanie kwalifikacji procesów przetwarzania danych osobowych pod kątem konieczności poddania ich ocenie skutków dla ochrony danych osobowych;

3) przeprowadzanie oceny skutków dla ochrony danych osobowych;

4) stosowanie tzw. zasad privacy by design i privacy by default;

5) przeprowadzanie testów równowagi prawnie uzasadnionego interesu ADO;

6) analizę ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze przy uwzględnieniu charakteru, kontekstu, zakresu i celu przetwarzania danych;

7) stały monitoring otoczenia prawnego mającego wpływ na przetwarzanie danych osobowych przez ADO (monitoring zewnętrzny);

8) stały monitoring realizacji wypracowanych założeń w zakresie ochrony danych osobowych w ramach struktury ADO (monitoring wewnętrzny).

3. Skuteczność wdrożonych środków ochrony danych osobowych jest stale monitorowana i udoskonalana, w szczególności w ramach audytów zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze ADO.

§ 12. Ocena skutków dla ochrony danych - proces oceny ewentualnych skutków zagrożeń dla planowanych operacji przetwarzania. Ocena ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych przeprowadzana jest w sytuacjach, gdy istnieje uzasadnione podejrzenie, że dany proces lub sposób organizacji przetwarzania danych osobowych może nieść za sobą ryzyko naruszenia praw lub wolności osób, których dane dotyczą (ze względu na ich charakter, zakres lub cel).

§ 13. Szczegółowe zasady oceny ryzyka oraz oceny skutków dla ochrony danych zostały uregulowane w Procedurze oceny ryzyka dla czynności przetwarzania danych osobowych, stanowiącej **Załącznik Nr 19** do Zarządzenia.

§ 14. Ochrona danych w fazie projektowania oraz domyślna ochrona danych.

1. ADO wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu:

1) skutecznej realizacji zasad ochrony danych osobowych;

2) nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.

2. Wdrażając środki, o których mowa w ust. 1 ADO uwzględnia:

1) stan wiedzy technicznej;

2) koszt wdrażania;

3) charakter, zakres, kontekst i cele przetwarzania danych;

4) ryzyko naruszenia praw lub wolności osób fizycznych wynikające z przetwarzania danych osobowych.

3. ADO wdraża takie środki, o których mowa w ust. 1, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę:

1) ilość zbieranych danych osobowych;

2) zakres danych osobowych;

3) okres przechowywania danych osobowych;

4) dostępność danych osobowych dla innych osób.

4. ADO zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - wdraża odpowiednie środki, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

5. W pierwszej kolejności, ADO rozważa, czy cel jakiemu ma służyć projektowane rozwiązane jest możliwy do osiągnięcia bez konieczności przetwarzania danych osobowych. Jeśli tak, należy wybrać takie rozwiązanie.

6. ADO zapewnia, aby spełnienie warunków wskazanych w ust. 1-5 było odpowiednio udokumentowane np. w formie notatki, maila, raportu z przeprowadzonych testów systemu informatycznego, wydruku z ekranu systemu itd.

§ 15. Za procesy, o których mowa w § 14 odpowiadają Kierownicy.

§ 16. Test równowagi prawnie uzasadnionego interesu ADO.

1. W przypadkach, kiedy ADO przetwarza lub planuje przetwarzać dane osobowe na podstawie art. 6 ust. 1 lit. f RODO, tj. do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią, jest on zobowiązany do przeprowadzenia tzw. testu równowagi.

2. Prawnie uzasadnione interesy ADO lub strony trzeciej, mogą być podstawą przetwarzania danych wyłącznie wtedy, o ile w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z ADO nie są nadrzędne interesy lub podstawowe prawa i wolności osoby, której dane dotyczą.

3. Procedura testu równowagi prawnie uzasadnionego interesu ADO stanowi **Załącznik nr 25** do Zarządzenia.

§ 17. Bezpieczeństwo zasobów ludzkich w zakresie przetwarzania informacji.

1. Celem ograniczenia ryzyka błędu ludzkiego, kradzieży lub nadużycia oraz zapewnienia, że pracownicy Urzędu, praktykanci, stażyści, wolontariusze, zleceniobiorcy oraz inne osoby i podmioty wykonujące czynności w imieniu i na rzecz Urzędu i/lub mające dostęp do aktywów informacyjnych Urzędu są świadomi odpowiedzialności i swoich obowiązków dotyczących bezpieczeństwa informacji oraz, że wypełniają je w odpowiedni sposób i z uwzględnieniem interesów Urzędu, podejmowane są określone działania w obszarze bezpieczeństwa zasobów ludzkich, w szczególności:

1) zapewnienie wykwalifikowanych pracowników i/lub innych osób oraz podmiotów zewnętrznych do realizacji zadań;

2) uwzględnienie odpowiednich zapisów dot. odpowiedzialności w zakresie bezpieczeństwa informacji w umowach zawieranych z ww. osobami i podmiotami;

3) szkolenie ww. osób w zakresie bezpieczeństwa informacji oraz regularne informowanie o aktualizacji polityk i procedur związanych z ich stanowiskiem pracy.

2. Pracownicy Urzędu są zobowiązani do świadomego i odpowiedzialnego przestrzegania bezpieczeństwa informacji i podlegają obowiązkowym szkoleniom z zakresu ochrony informacji w szczególności:

1) przed dopuszczeniem do przetwarzania danych osobowych;

2) podczas zatrudnienia.

3. Zapewnia się szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

1) zagrożenia bezpieczeństwa informacji;

2) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna;

3) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

§ 18. Bezpieczeństwo teleinformatyczne, komunikacji.

1. W ramach zarządzania bezpieczeństwem teleinformatycznym podejmowane są działania w zakresie szacowania i kontroli ryzyka utraty poufności, integralności, dostępności informacji w związku z korzystaniem z systemu informatycznego Urzędu oraz aplikacji, komputerów i urządzeń mobilnych, sieci komputerowych i transmisji danych.

2. Przedmiotowe działania podejmowane są w szczególności w zakresie rozwoju, monitorowania i doskonalenia infrastruktury teleinformatycznej.

3. Skuteczna realizacja postawionego celu możliwa jest dzięki:

1) kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi firmami wspomagającymi Urząd;

2) zasadzie, że wszystkie systemy Urzędu przed dopuszczeniem do eksploatacji muszą spełniać minimalne wymagania bezpieczeństwa i być zgodne z obowiązującymi standardami;

3) obowiązującym zasadom konserwacji i redundancji urządzeń sieciowych w celu zapewnienia ich nieprzerwanej pracy;

4) kontrolowaniu wprowadzania zmian do infrastruktury technicznej;

5) zapewnieniu bezpieczeństwa systemów produkcyjnych, poprzez prowadzenie prac rozwojowych i testowych na oddzielnych urządzeniach lub środowiskach;

6) nadzorowaniu usług dostarczanych przez strony trzecie, a w szczególności wszelkim wprowadzanym do nich zmianom. Po zakupie, lub wprowadzeniu zmiany do systemu jest on odbierany i akceptowany w sposób świadomy, uwzględniający jego wpływ na istniejący system bezpieczeństwa;

7) wdrożonym zabezpieczeniom, chroniącym przed złośliwym oprogramowaniem i złośliwym kodem;

8) usystematyzowanemu tworzeniu, przechowywaniu i testowaniu kopii bezpieczeństwa;

9) przestrzeganiu opracowanych zasad zarządzania bezpieczeństwem usług sieciowych;

10) przestrzeganiu opracowanych zasad korzystania z urządzeń i narzędzi komunikacyjnych;

11) przestrzeganiu opracowanych zasad postępowania z nośnikami;

12) bieżącemu monitorowaniu aktywów informacyjnych, w tym informatycznych, pod kątem wcześniejszego wykrycia wszelkich niebezpieczeństw mogących zagrozić bezpieczeństwu systemów;

13) wykrywaniu incydentów w systemach teleinformatycznych i mechanizmom reagowania w przypadkach ich wystąpienia;

14) systematycznym testom penetracyjnym;

15) ograniczonemu dostępowi do niektórych usług internetowych,

16) monitorowaniu poziomu bezpieczeństwa informacji i posiadaniu mechanizmów reagowania w przypadkach wystąpienia incydentów.

§ 19. Bezpieczeństwo fizyczne, środowiskowe.

1. W celu zapobieżenia nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w przetwarzaniu informacji i środkach przetwarzania informacji oraz utracie, zniszczeniu, uszkodzeniu, kradzieży aktywów informacyjnych Urzędu stosowane są mechanizmy ochrony w obszarze bezpieczeństwa fizycznego i środowiskowego.

2. W ramach ochrony fizycznej, która dotyczy bezpieczeństwa fizycznego i środowiskowego należy uwzględnić zagrożenia zewnętrzne i środowiskowe (pożar, zalanie, wybuch itd.).

3. Zapewnienie ochrony fizycznej przed nieuprawnionym dostępem, uszkodzeniem lub zakłóceniem obejmuje:

1) ochronę przed nieuprawnionym dostępem;

2) zapewnienie ochrony dla przetwarzania informacji krytycznych;

3) zapewnienie ochrony dla eksploatowanego sprzętu teleinformatycznego z uwzględnieniem instalacji wspomagających;

4) zapewnienie ochrony sprzętu używanego poza siedzibą Urzędu.

4. Ochronie podlega sprzęt (łącznie ze sprzętem wykorzystywanym poza siedzibą Urzędu), ze szczególnym uwzględnieniem warunków zabezpieczenia przed utratą, uszkodzeniem lub kradzieżą.

5. Zbywanie, likwidacja lub zmiana użytkownika składnika majątkowego sprzętu informatycznego lub nośnika, wymaga skutecznego usunięcia danych ze szczególnym uwzględnieniem zawartości dysków twardych komputerów. Podstawowym zaleceniem jest skuteczne niszczenie takich nośników.

6. Do ochrony sprzętu stosuje się środki i systemy wspomagające i zabezpieczające przed awariami lub zakłóceniami infrastruktury innego rodzaju: zasilanie, klimatyzacja.

7. Zapewnienie prawidłowej i bezpiecznej eksploatacji posiadanych środków przetwarzania informacji następuje poprzez:

1) określenie procedur w zakresie przetwarzania i administrowania;

2) przypisanie odpowiedzialności w zakresie przetwarzania i administrowania;

3) rozdzielenie odpowiedzialności;

4) prognozowanie wydajności zasobów;

5) zapewnienie integralności i dostępności informacji Urzędu;

6) zapewnienie bezpieczeństwa informacji wymienianej z innymi podmiotami;

7) monitorowanie i wykrywanie działań nieautoryzowanych;

8) monitorowanie i rejestrowanie zdarzeń związanych z bezpieczeństwem informacyjnym z zachowaniem warunku o nie przekraczaniu uprawnień;

9) zarządzanie incydentami związanymi z bezpieczeństwem informacji, w tym gromadzenie materiałów dowodowych;

8. Do zapewnienia ciągłej dostępności i integralności sprzętu zaleca się jego okresową konserwację.

§ 20. Zarządzanie systemami i sieciami.

1. Środki w zakresie rozwiązań teleinformatycznych stosowane na terenie i na rzecz Urzędu podlegają analizie i są adekwatne do wymagań ochrony przetwarzanej informacji wynikającej z przeprowadzonej w Urzędzie analizy ryzyka.

2. Zmiany w środowiskach przetwarzania informacji wymagają zarządzania i nadzoru.

3. Środowisko przetwarzania informacji podlega zarządzaniu i obejmuje:

1) zbiory i pliki z danymi, licencje i dokumentacje systemów;

2) sprzęt komputerowy: serwery, komputery, urządzenia mobilne, macierze, przełączniki, routery itd.;

3) usługi obliczeniowe, przesyłania i przechowywania danych, udostępniania internetu i poczty elektronicznej;

4) inne usługi infrastruktury: zasilanie i klimatyzacja;

5) kwalifikacje zawodowe i informatyczne pracowników i ich doświadczenie;

6) aplikacje.

4. Dla obszaru systemów teleinformatycznych i zarządzanych sieci komputerowych stosuje się następujące wymagania:

1) rozdzielenie obowiązków i odpowiedzialności za środki przetwarzania informacji (systemy), aby uniknąć nieuprawnionej lub nieumyślnej modyfikacji lub niewłaściwego użycia aktywów;

2) oddzielenie aktywów przeznaczonych do działań rozwojowych, testowych i eksploatacyjnych;

3) właściwego zdefiniowania poziomów dostępności usług oraz zapewnienia monitorowania dostarczanych usług. W przypadku świadczenia tych usług przez podmiot zewnętrzny wymagane jest definiowanie usług oraz poziom dostaw w umowach serwisowych;

4) szkolenia dla użytkowników;

5) wycofywanie z eksploatacji nieużywanych usług i infrastruktury i ich likwidowanie po usunięciu informacji;

6) zapewnienie wykonywania kopii bezpieczeństwa zasobów informacyjnych;

7) właściwe wdrażanie procedur obsługi nośników danych oraz ich zastosowania przy wymianie informacji;

8) monitorowanie właściwego zabezpieczenia systemów informatycznych i sieci komputerowych oraz rejestrowanie zdarzeń, błędów oraz informacji w systemie informatycznym.

§ 21. Kontrola dostępu do informacji.

1. Procedury kontroli dostępu do informacji i środków przetwarzania informacji są ustanowione, udokumentowane i monitorowane w zgodzie z potrzebami Urzędu i wymaganiami bezpieczeństwa określonymi w PBI.

2. Zarządzanie dostępem do informacji odbywa się w ramach procesu opartego na systemie obiegu wniosków.

3. W szczególności dostęp do wszystkich systemów informatycznych wymaga uregulowania w zakresie rejestrowania użytkowników, obowiązku stosowania haseł dostępu, zarządzania uprawnieniami i hasłami, izolowania systemów wrażliwych.

4. Wymagane jest wykonywanie regularnych przeglądów praw dostępu.

5. Uregulowania te powinny obejmować wszystkich użytkowników, ASI i ASU.

6. Użytkownicy, ASI, ASU są odpowiedzialni za ochronę haseł do systemów, prawidłową eksploatację systemów informatycznych i użytkowanego sprzętu, zgodnie z uregulowaniami poszczególnych systemów.

7. Usługi sieciowe są chronione przed nieautoryzowanym dostępem poprzez określenie zasad korzystania z tych usług, zasad konfiguracji i kontroli zdarzeń w sieci, tj. identyfikację urządzeń, kontrolę połączeń ich ruchu w sieciach Urzędu.

8. Przetwarzanie na urządzeniach mobilnych i praca na odległość są uregulowane poprzez określenie zasad korzystania z tych usług oraz wdrożenie odpowiednich zabezpieczeń.

9. Nadzór, kontrola nadawania i odbierania uprawnień do systemów informatycznych jest prowadzona w ramach dedykowanego systemu przez Winf.

§ 22. Zarządzanie ciągłością działania.

1. W Urzędzie podejmowane są działania w zakresie planowania, weryfikowania, zapewnienia, przeglądu i oceny ciągłości działania i postępowania w przypadku wystąpienia sytuacji kryzysowych.

2. Urząd posiada procedury zarządzania i nadzoru, które zapewniają ciągłość działania kluczowych funkcji, określonych, jako plany awaryjne zarówno w znaczeniu procesów biznesowych jak i organizacyjnych w przypadkach sytuacji kryzysowych, katastrof, awarii zabezpieczeń, utraty informacji i innych.

3. Strategia zapewnienia ciągłości działania przetwarzania informacji Urzędu została określona w **Załączniku Nr 21** do Zarządzenia.

4. Bazowy plan ciągłości działania do dokumentacji zarządzania ciągłością działania Urzędu ostał określony w **Załączniku Nr 22** do Zarządzenia.

§ 23. Relacje z dostawcami.

1. Z uwagi na realizowane zadania, kompetencje w obszarze kontaktów z dostawcami leżą w gestii właściciela obszaru.

2. Precyzując zasady kontaktów z dostawcami w ramach poszczególnych rodzajów dostaw powinny zostać uwzględnione w miarę możliwości następujące aspekty:

1) umowy o zachowaniu poufności;

2) zasady uświadamiania i szkolenia pracowników dostawców oraz podpisywanie stosownych oświadczeń i upoważnień (dane osobowe);

3) procedury przesyłania informacji, w tym przekazywania informacji innym podmiotom;

4) umowy powierzenia i związane z nimi ankiety bezpieczeństwa;

5) wymagania bezpieczeństwa informacji, w tym dotyczące klasyfikacji informacji;

6) zarządzanie usługami i zmianami w usługach, w tym:

a) precyzyjne zdefiniowanie zakresu usługi,

b) zakres odpowiedzialności poszczególnych stron umowy,

c) wykaz poddostawców,

d) wymagania i uprawnienia dotyczące monitorowania realizacji usług,

e) zarządzanie ryzykiem związanym ze zgłoszoną zmianą;

7) wykaz zawartych umów z dostawcami wraz z ich statusem;

8) tryb zakończenia realizacji umowy, z uwzględnieniem zwrócenia powierzonych wzajemnie aktywów.

3. Zaleca się wypracowanie wspólnych wzorów umów, zawierających między innymi zapisy dotyczące zachowania poufności lub powierzenia przetwarzania danych osobowych, dla ułatwienia procesu ich zawierania.

4. Kierownicy w zakresie zadań realizowanych zgodnie z Regulaminem Organizacyjnym prowadzą bieżący nadzór w swoich jednostkach w zakresie zgodności z przepisami prawa i zapisami umownymi.

§ 24. Zarządzanie incydentami związanymi z bezpieczeństwa informacji.

1. Incydenty naruszenia bezpieczeństwa informacji są bezzwłocznie zgłaszane w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

2. Do przypadków mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania lub słabości systemu teleinformatycznego zalicza się w szczególności:

1) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach (np. wyłamane lub zacinające się zamki, naruszone plomby, niedomykające się bądź wybite okna etc.);

2) utratę usługi, urządzenia lub funkcjonalności;

3) nieautoryzowaną modyfikację lub zniszczenie danych;

4) udostępnienie danych osobom nieupoważnionym;

5) pozyskiwanie oprogramowania z nielegalnych źródeł;

6) pojawianie się nietypowych komunikatów na ekranie komputera;

7) niemożność zalogowania się do systemu teleinformatycznego;

8) spowolnienie pracy oprogramowania;

9) niestabilną pracę zasobu teleinformatycznego;

10) brak reakcji zasobu na działania użytkownika;

11) ponowny start lub zawieszanie się komputera;

12) ograniczenie funkcjonalności oprogramowania.

4. Kierownicy w sytuacjach związanych ze stwierdzeniem incydentów bezpieczeństwa, naruszeń ochrony danych czy sytuacji kryzysowych obowiązani są do:

1) wyjaśnienia wszelkich aspektów naruszenia bezpieczeństwa informacji;

2) przedsięwzięcia środków zapobiegawczych;

3) wdrożenia postępowania dyscyplinarnego;

4) współpracy z IOD i ASI.

5. W przypadku wystąpienia klęski żywiołowej lub aktu terroru w pierwszej kolejności powiadamiane są właściwe służby, a następnie ochrona budynku oraz Sekretarz Miasta.

6. W przypadku wystąpienia próby włamania, kradzieży dokumentów, sprzętu oraz wszelkich innych prób niszczenia mienia powiadamiana jest ochrona budynku.

7. Ustanawia się instrukcję postępowania z incydentami bezpieczeństwa i naruszeniami ochrony danych osobowych, zasady ich identyfikacji, zasady zgłaszania i postępowania, które określa **Załącznik Nr 15** do Zarządzenia.

8. Klasyfikacja incydentów bezpieczeństwa teleinformatycznego w Urzędzie stanowi **Załącznik Nr 8** do Zarządzenia.

9. Klasyfikacja incydentów i zdarzeń dotyczących bezpieczeństwa fizycznego w związku z bezpieczeństwem systemów i urządzeń teleinformatycznych w Urzędzie stanowi **Załącznik Nr 9** do Zarządzenia.

§ 25. Pozyskiwanie, rozwój, utrzymanie i inwentaryzacja oprogramowania informatycznego.

1. Urząd zapewnia, że wszystkie procesy związane z pozyskaniem, rozwojem bądź utrzymaniem systemów informacyjnych, w tym systemów i aplikacji teleinformatycznych, realizowanych zarówno we własnym zakresie, jak i przy wsparciu podwykonawców, wykorzystywanych wewnętrznie lub oferowanych obywatelom, realizowane są w sposób nadzorowany, gwarantujący utrzymanie odpowiedniego poziomu bezpieczeństwa.

2. Pozyskiwanie, rozwój, utrzymanie i inwentaryzacja systemów teleinformatycznych obejmuje:

1) uwzględnienie wymogów bezpieczeństwa podczas zakupu lub budowy nowych systemów teleinformatycznych;

2) dopuszczenie nowego systemu do eksploatacji poprzedzone jest zawsze fazą testów funkcjonalnych, wydajnościowych i testów bezpieczeństwa na środowisku testowym;

3) nadzorowanie dostępu do kodów źródłowych oprogramowania;

4) wdrożenie mechanizmów aktualizacji oprogramowania;

5) wdrożenie procedur kontroli zmian oprogramowania.

3. Utrzymywana jest aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

4. Dokumentacja zarządzania sprzętem i oprogramowaniem obejmuje:

1) rejestr zasobów informatycznych;

2) procedury prowadzenia rejestru zasobów informatycznych;

3) procedury przydzielenia, zwrotu sprzętu i oprogramowania;

4) procedury korzystania z zasobów informatycznych przez użytkowników;

5) dokumentację wykonywania ww. procedur.

5. Za zapewnienie właściwego przebiegu procesu pozyskiwania, rozwoju, utrzymania i inwentaryzacji systemów teleinformatycznych odpowiedzialny jest Dyrektor WInf.

6. Procedurę pozyskiwania, rozwoju, utrzymania i inwentaryzacji oprogramowania określa Regulamin zarządzania oprogramowaniem w Urzędzie stanowiący **Załącznik Nr 4** do Zarządzenia.

§ 26. Zarządzanie aktywami.

1. Urząd zarządza swoimi aktywami (zasobami) w celu zapewnienia im wymaganego poziomu bezpieczeństwa.

2. Wszystkim zasobom z wyjątkiem zasobów ludzkich przypisuje się poziom ważności:

1) ważność wysoka przyznawana jest, gdy utrata lub naruszenie bezpieczeństwa zasobów powoduje przerwanie procesu. Należą do nich m.in.:

   a) informacje nadzorowane, wrażliwe pod względem poufności w szczególności: informacje niejawne dodatkowo podlegające ochronie w stopniu zgodnym z postanowieniami ustawy o ochronie informacji niejawnych,

   b) dane osobowe dodatkowo podlegające ochronie w stopniu zgodnym z postanowieniami RODO,

   c) dane finansowo – księgowe,

   d) inne informacje, których poufność określają ustawy,

   e) zasoby materialne kluczowe niezbędne do realizowania statutowych celów ADO.

2) ważność średnia przyznawana jest, gdy utrata lub naruszenie bezpieczeństwa zasobów może mieć wpływ na prawidłową realizację procesu. Należą do nich m.in.:

   a) pozostałe informacje nadzorowane, niewrażliwe (np. korespondencja wewnętrzna ADO),

   b) zasoby fizyczne wartościowe, które są drogie lub trudno zastępowalne, ale od których nie zależy bezpośrednio funkcjonowanie ADO,

3) ważność niska przyznawana jest, gdy utrata lub naruszenie bezpieczeństwa zasobu ma znikomy wpływ na funkcjonowanie procesu. Należą do nich m.in.:

   a) informacje nienadzorowane i inne informacje publiczne,

   b) zasoby fizyczne zwykłe, które są łatwo odtwarzalne lub zastępowalne i od których nie zależy bezpośrednio funkcjonowanie ADO.

3. Aktywa chronione są ze względu na przepisy prawa oraz wartość materialną i intelektualną. Aktywa mogą być chronione na mocy:

1) przepisów prawa (np. dane osobowe, informacje niejawne, prawo autorskie);

2) warunków licencji;

3) zapisów umów pomiędzy jednostką organizacyjną a podmiotami zewnętrznymi.

4. Rodzaje aktywów, o których mowa ust 3 określa **Załącznik Nr 20** do Zarządzenia.

§ 27. Audyt i przegląd SZBI.

1. Audyty i przeglądy SZBI podlegają wdrożeniu, jako okresowe procedury kontroli jednostek organizacyjnych w Urzędzie.

2. Audyty i przeglądy SZBI mogą być realizowane przez podmiot zewnętrzny zgodnie z wytycznymi dotyczącymi audytu bezpieczeństwa informacji wykonywanymi przez podmiot zewnętrzny, które określa **Załącznik Nr 23** do Zarządzenia.

3. Na podstawie audytu SZBI dokonuje się oceny, czy cele, zastosowane zabezpieczenia, procedury i procesy realizowane w Urzędzie są skuteczne i zgodnie z wymaganiami PBI.

4. Na podstawie przeglądu SZBI dokonuje się ocenę możliwości doskonalenia i potrzeb zmian w zarządzaniu bezpieczeństwem informacji.

5. Wyniki audytów i wnioski pokontrolne są przekazane ADO i Kierownikom w celu podjęcia i wdrożenia stosownych działań doskonalących.

§ 28. Doskonalenie SZBI.

1. SZBI jest doskonalony poprzez podejmowanie następujących działań:

1) przeprowadzanie działań korygujących oraz ocena ich skuteczności;

2) przeprowadzanie działań zapobiegawczych oraz ocena ich skuteczności;

3) informowanie zainteresowanych stron o działaniach i udoskonaleniach.

§ 29. Zakończenie zatrudnienia w Urzędzie.

1. Wszystkie mechanizmy identyfikacji i autoryzacji uprawniające użytkownika do dostępu do zasobów, kończącego zatrudnienie lub zmieniającego stanowisko pracy, winny być odebrane i wyłączone przed zakończeniem zatrudnienia użytkownika.

2. Użytkownik kończący zatrudnienie w Urzędzie lub zmieniający stanowisko pracy jest zobowiązany do przekazania wszystkich posiadanych zasobów informacyjnych użytkownikowi wskazanemu przez jego Kierownika, z zachowaniem wszystkich aspektów bezpieczeństwa informacji.

§ 30. Sankcje za naruszenie zasad bezpieczeństwa informacji i ochrony danych osobowych. Pracownik, który nie przestrzega przepisów dotyczących bezpieczeństwa informacji i ochrony danych osobowych, w zależności od sytuacji może ponieść:

1) odpowiedzialność dyscyplinarną (możliwe jest rozwiązanie z nim umowy o pracę za wypowiedzeniem lub bez wypowiedzenia z winy pracownika);

2) odpowiedzialność odszkodowawczą;

3) w niektórych sytuacjach odpowiedzialność karną.

§ 31. Minimalne wymagania bezpieczeństwa systemów informatycznych.

1. Każdy system informatyczny wykorzystywany w Urzędzie musi spełniać następujące wymagania lub posiadać następujące funkcjonalności:

1) możliwość przyznawania indywidualnych identyfikatorów użytkownikom;

2) możliwość gradacji uprawnień na minimum dwóch poziomach administrator – użytkownik;

3) możliwość konfiguracji kontroli dostępu do systemu (złożoność haseł, częstotliwość zmiany haseł);

4) możliwość odnotowania daty oraz identyfikatora użytkownika pierwszego i każdej kolejnej modyfikacji wprowadzenia danych (rekordów) do systemu;

5) każdy system informatyczny przetwarzający dane osobowe wykorzystywany w organizacji musi spełniać następujące wymagania lub posiadać następujące funkcjonalności:

a) możliwość odnotowania sprzeciwu i odwołania zgody wobec przetwarzania danych osobowych,

b) możliwość sporządzania wydruków dotyczących konkretnej osoby lub generowania plików do powszechnie używanych formatów,

c) możliwość poprawiania wprowadzonych danych,

d) możliwość trwałego usunięcia lub zanonimizowania danych w systemie,

e) możliwość wprowadzenia ograniczenia przetwarzania poszczególnych pól informacyjnych tylko do wglądu (bez możliwości edycji).

2. Administrator systemu informatycznego (na wniosek osoby zainteresowanej) oraz każda osoba umocowana do podejmowania wiążących decyzji w zakresie korzystania z zewnętrznego oprogramowania weryfikują ww. zasady wobec każdego nowego systemu informatycznego.

§ 32. W celu zapewnienia ochrony przetwarzanych informacji oraz zabezpieczenia prawidłowego przetwarzania danych osobowych w Urzędzie wprowadza się następujące dokumenty:

1) Polityka Bezpieczeństwa Informacji w Urzędzie stanowiąca **Załącznik Nr 1 do Zarządzenia;**

2) Instrukcja Zarządzania Systemem Informatycznym Urzędu stanowiąca **Załącznik Nr 2 do Zarządzenia;**

3) Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w Urzędzie stanowiący **Załącznik Nr** 3 do Zarządzenia;

4) Regulamin zarządzania oprogramowaniem w Urzędzie stanowiący **Załącznik Nr 4 do Zarządzenia;**

5) Zasady korzystania z internetu oraz poczty elektronicznej Urzędu stanowiące **Załącznik Nr 5 do Zarządzenia;**

6) Kategorie uprawnień do systemów teleinformatycznych Urzędu stanowiące **Załącznik Nr 6 do Zarządzenia;**

7) Regulamin użytkowania urządzeń mobilnych w Urzędzie stanowiący **Załącznik Nr 7 do Zarządzenia;**

8) Klasyfikację incydentów bezpieczeństwa teleinformatycznego w Urzędzie stanowiącą **Załącznik Nr 8 do Zarządzenia;**

9) Klasyfikacja incydentów i zdarzeń dotyczących bezpieczeństwa fizycznego w związku z bezpieczeństwem systemów i urządzeń teleinformatycznych w Urzędzie stanowiącą **Załącznik Nr 9 do Zarządzenia;**

10) Zasady stosowania pamięci komputerowych i pomocniczych w Urzędzie ze wskazaniem poziomu ich bezpieczeństwa stanowiące **Załącznik Nr 10 do Zarządzenia;**

11) Zgłoszenie użytkownika systemów informatycznych w Urzędzie stanowiące **Załącznik Nr 11 do Zarządzenia;**

12) Regulamin korzystania z zasobów teleinformatycznych Urzędu stanowiący **Załącznik Nr 12 do Zarządzenia;**

13) Zasady wydawania upoważnień do przetwarzania danych osobowych stanowiące **Załącznik Nr 13 do Zarządzenia;**

14) Oświadczenie o zapoznaniu się z zarządzeniem stanowiące **Załącznik Nr 14 do Zarządzenia;**

15) Instrukcja postępowania z incydentami bezpieczeństwa i naruszeniami ochrony danych osobowych w Urzędzie stanowiąca **Załącznik Nr 15 do Zarządzenia;**

16) Procedura administrowania identyfikatorami i hasłami dostępu w Urzędzie stanowiąca **Załącznik Nr 16 do Zarządzenia;**

17) Procedura tworzenia i przechowywania kopii bezpieczeństwa oraz archiwum danych w Urzędzie stanowiąca **Załącznik Nr 17 do Zarządzenia;**

18) Procedura oceny ryzyka z obszaru bezpieczeństwa informacji stanowiąca **Załącznik Nr 18 do Zarządzenia;**

19) Procedura oceny ryzyka dla czynności przetwarzania danych osobowych stanowiąca Załącznik **Nr 19 do Zarządzenia**;

20) Aktywa Urzędu stanowiące **Załącznik Nr 20 do Zarządzenia;**

21) Strategia zapewnienia ciągłości działania przetwarzania informacji w Urzędzie stanowiąca **Załącznik Nr 21 do Zarządzenia**;

22) Bazowy Plan dokumentacji zarządzania ciągłością działania w Urzędzie stanowiący **Załącznik Nr 22 do Zarządzenia;**

23) Wytyczne dotyczące audytu bezpieczeństwa informacji wykonywane przez podmiot zewnętrznej stanowiące **Załącznik Nr 23 do Zarządzenia;**

24) Procedura zarządzania uprawnieniami do zasobów/systemów informatycznych Urzędu, stanowiąca **Załącznik Nr 24 do Zarządzenia**;

25) Procedura testu równowagi prawnie uzasadnionego interesu ADO stanowi **Załącznik Nr 25 do Zarządzenia;**

26) Procedura kontroli podmiotów przetwarzających dane osobowe w imieniu ADO stanowi **Załącznik Nr 26 do Zarządzenia;**

27) Plan wewnętrznego audytu zgodności przetwarzania danych u ADO stanowi **Załącznik Nr 27 do Zarządzenia;**

28) Procedura obsługi żądań podmiotów danych stanowi **Załącznik Nr 28** do Zarządzenia.

§ 33. Wykonanie zarządzenia powierzam dyrektorom wydziałów, kierownikom biur oraz samodzielnym stanowiskom działającym poza strukturą wydziałów i biur Urzędu Miasta Szczecin.

§ 34. Nadzór nad realizacją zarządzenia powierzam Sekretarzowi Miasta.

§ 35. 1. Załączniki, o których mowa w § 32 od pkt. 1-4; 6; 8-9; 15-22 nie podlegają publikacji w Biuletynie Informacji Publicznej Urzędu.

2. Załącznik, o którym mowa w § 32 pkt 3, nie podlega udostępnieniu użytkownikom.

§ 36. Traci moc Zarządzenie Nr 150/18 Prezydenta Miasta Szczecin z dnia 6 kwietnia 2018 roku w sprawie określenia zasad bezpieczeństwa informacji oraz wytycznych dla Polityki Bezpieczeństwa Informacji Urzędu Miasta Szczecin (zm. Zarządzenie Nr 327/19 Prezydenta Miasta Szczecin z dnia 26 lipca 2019 r.).

§ 37. Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta

Piotr Krzystek

Załącznik Nr 5 do zarządzenia Nr 312/23
Prezydenta Miasta Szczecin
z dnia 28 czerwca 2023 r.

Zasady korzystania z Internetu oraz z poczty elektronicznej Urzędu

§ 1. 1. Użytkownicy będący pracownikami Urzędu, uzyskują dostęp do Internetu i poczty elektronicznej za pomocą sieci teleinformatycznej LAN Urzędu i w sposób określony w niniejszych zasadach.

2. Użytkownicy, nie będący pracownikami Urzędu, określeni także, jako podmiot zewnętrzny, mogą uzyskać dostęp do sieci teleinformatycznej LAN Urzędu jedynie na podstawie:

1) polecenia ADO lub Sekretarza Miasta;
2) polecenia Dyrektora WInf;
3) umowy zawartej pomiędzy Urzędem, a podmiotem zewnętrznym, w której określono warunki takiego dostępu.

3.Użytkownicy podmiotu zewnętrznego, w przypadku stwierdzenia naruszeń zapisów PBI podlegają natychmiastowemu odłączeniu od sieci LAN Urzędu. Powyższą decyzję podejmuje Dyrektor WInf lub ASI.

4. Użytkownicy są zobowiązani do wykorzystywania poczty elektronicznej Urzędu i serwisów internetowych zgodnie z zakresem swoich obowiązków, tj. w celu realizacji zadań służbowych oraz zadań związanych z podnoszeniem kwalifikacji zawodowych.

5. Dostęp do Internetu dostarczanego za pomocą sieci teleinformatycznej LAN Urzędu może być realizowany wyłącznie po prawidłowo przeprowadzonej procedurze logowania do tej sieci.

6. Procedury logowania są administrowane przez WInf i zapewniają odpowiedni poziom bezpieczeństwa sieci teleinformatycznej LAN Urzędu.

7. Użytkownicy, jeżeli wykonują pracę poza siecią teleinformatyczną LAN Urzędu mogą uzyskiwać dostęp do Internetu przy pomocy urządzeń i technologii mobilnych.

8. Użytkownicy zobowiązani są do korzystania wyłącznie ze sprzętu komputerowego będącego własnością Urzędu i wyłącznie przy użyciu legalnego oprogramowania, do którego Urząd posiada odpowiednie licencje lub inne uprawnienia.

9. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie przez niego zainstalowane.

10. Procedury przywrócenia właściwego stanu komputera, na którym stwierdzono oprogramowanie niezgodne z zasadami określonym w Zarządzeniu wykonywane są przez WInf.

§ 2. Uprawnienia dostępu do sieci LAN Urzędu.

1. Zabrania się podłączania do sieci LAN Urzędu jakichkolwiek urządzeń, w tym komputerów przenośnych, urządzeń sieciowych czy jakichkolwiek urządzeń pracujących z zastosowaniem technologii komputerowych. Powyższy zakaz nie dotyczy pracowników WInf, którzy realizują zadania służbowe.

2. Zabrania się instalowania i uruchamiania oprogramowania niedopuszczonego do użycia przez Urząd. Działania powyższe, po ich potwierdzeniu, traktowane będą, jako celowe i świadome, zmierzające do zwiększenia zagrożeń zasobów teleinformatycznych, a w szczególności rażąco łamiące postanowienia PBI Urzędu.

§ 3. 1. Wprowadza się następujące postanowienia związane z realizacją dostępu do Internetu oraz korzystania z poczty elektronicznej Urzędu:

1) podczas łączenia się ze skrzynką pocztową należy zachować szczególne warunki bezpieczeństwa i poufności w zakresie korespondencji służbowej, w tym ochrony danych osobowych;
2) korzystanie z poczty elektronicznej Urzędu odbywa się:
a) jedynie przy pomocy konta pocztowego przydzielonego Użytkownikowi przez WInf lub przekierowanego na podstawie decyzji kierownika,
b) za pośrednictwem programu przeglądarki internetowej lub programu klienta pocztowego.

2.W przypadku zainstalowania i uruchomienia oprogramowania niedopuszczonego do użycia przez Urząd - WInf:

1) zastosuje blokadę konta Użytkownika w sieci LAN Urzędu oraz redukcję dostępu do Internetu lub zastosuje całkowite odłączenie komputera pracownika od sieci LAN Urzędu;
2) sporządzi raport potwierdzający stan komputera oraz aktywność sieciową Użytkownika i przekaże ten raport jego Kierownikowi.

3.Postanowienia ust. 2 mają zastosowanie dla Użytkowników będących pracownikami Urzędu.

4.W celu zapewnienia bezpieczeństwa zasobom sieci LAN Urzędu oraz jej Użytkownikom zabrania się dokonywania na niej, działań o charakterze nielegalnym, a w szczególności:

1) umieszczania lub uruchamiania programów i innych obiektów niebezpiecznych realizujących działania niepożądane lub wrogie;
2) skanowania sieci teleinformatycznej LAN Urzędu;
3) łączenia urządzeń mobilnych podłączonych już do sieci LAN Urzędu do kolejnych sieci komputerowych w tym bezprzewodowych (Wi-Fi);
4) prowadzenia ataków, skanowania sieci oraz innych czynności związanych z ingerencją w działanie urządzeń w sieci LAN Urzędu, a także w stosunku do osób trzecich, ich komputerów i urządzeń w Internecie;
5) naruszania w jakikolwiek sposób bezpieczeństwa serwerów Urzędu, zakłócania ich bezawaryjnej pracy;
6) anonimowego wysyłania przesyłek poczty elektronicznej;
7) gromadzenia (w dowolnej formie) na stanowisku pracy, tj. stacji roboczej lub na zasobie dyskowym dostępnym w sieci LAN, materiałów lub treści niezgodnych z obowiązującym prawem lub naruszających dobre obyczaje;
8) uruchamiania programów z komputerowych nośników zewnętrznych, tj. z płyt CD lub nośników typu pendrive, kart SD, itp. oraz z Internetu;
9) rozpowszechniania plików w Internecie tj. przesyłania zdjęć, filmów, tekstów czy innych formatów plików.

5. Postanowienia ust. 4. pkt: 2, 8 i 9 nie dotyczą:

1) podmiotów zewnętrznych, które realizują zadania na rzecz Urzędu, na podstawie umów, a użyte technologie powinny zostać ustalone z ADO i zaakceptowane przez ASI;

2) pracowników Urzędu, których zadania polegają na komunikowaniu się i udostępnianiu danych i materiałów poprzez Internet;
3) pracowników WInf, upoważnionych przez Dyrektora WInf, których zadania wymagają zwiększonych uprawnień.

6. Zakazuje się umożliwiania osobom nieupoważnionym dostępu do sieci LAN Urzędu przy wykorzystaniu infrastruktury technicznej Urzędu, w szczególności umożliwienia pracy na stacjach roboczych Urzędu przy pomocy identyfikatora i hasła pracownika Urzędu.

§ 4. Zabrania się pracownikom Urzędu wykonywania następujących czynności:

1) używania służbowej poczty elektronicznej Urzędu do celów innych niż służbowe;
2) używania prywatnej poczty elektronicznej w celach służbowych;
3) wysyłania wiadomości pocztowych (e-mail), zawierających reklamy, „łańcuszki szczęścia", materiały pornograficzne, czy inne materiały uważane powszechnie za niedozwolone;
4) logowania się w celach prywatnych lub komercyjnych na stronach www czy uczestniczenia w portalach o charakterze społecznościowym, zwłaszcza towarzyskim, rozrywkowym, komercyjnym, itp.;
5) używania w celach prywatnych lub komercyjnych komunikatorów internetowych oraz mediów społecznościowych;
6) korzystania z serwisów internetowych niezwiązanych z obowiązkami pracownika;
7) przetwarzania na komputerach, kopiowania i wysyłania plików, do których Urząd nie posiada praw autorskich z określonymi polami eksploatacji;
8) korzystania z serwisów internetowych zawierających treści o charakterze przestępczym, hakerskim, pornograficznym, erotycznym, niecenzuralnym, rasistowskim lub w jakikolwiek sposób łamiące prawo.

§ 5. 1. Służbowa poczta elektroniczna Urzędu stanowi pomocnicze narzędzie pracy dla pracowników Urzędu.

2. Przesyłanie informacji poza Urząd może odbywać się tylko w sytuacji wynikającej z zakresu obowiązków lub prowadzonych postępowań.

3. W przypadku przesyłania informacji wrażliwych wewnątrz Urzędu, bądź wszelkich danych osobowych poza Urząd należy wykorzystywać mechanizmy kryptograficzne (pakowanie i wykorzystanie silnych haseł podczas wysyłania plików, podpis elektroniczny).

4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy wiadomości (dokumentu).

5. Nie należy otwierać załączników w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę, jak również nie należy uruchamiać odnośników (linków, hiperłączy) z treści takich wiadomości.

6. Pojemność standardowego zasobu na serwerze poczty elektronicznej, przydzielanego użytkownikowi poczty elektronicznej jest limitowana. Limit ten może zwiększyć Dyrektor WInf na pisemny, umotywowany wniosek Kierownika jednostki.

7. Korzystanie z poczty elektronicznej powinno odbywać się na bieżąco, w sposób racjonalny, zwłaszcza poprzez regularne przeglądanie zawartości skrzynki pocztowej z uwzględnieniem, że użytkownik jest zobowiązany:

1) zwrócić szczególną uwagę na wiadomości z nieznanych źródeł (adresów), zawierających jakiekolwiek anonse czy załączniki, w szczególności takie, które wymagają od Użytkownika poczty wpisania danych jego konta lub jego danych osobowych - tych danych nie wolno podawać;
2) reagować w przypadku otrzymywania wiadomości mających charakter przesyłek niechcianych, tj. „spam-u";
3) w przypadku stwierdzenia, że przesyłka wcześniej zakwalifikowana, jako spam nie jest uprawniona, przenieść ją do folderu „Skrzynka odbiorcza";
4) zgłosić pracownikom WInf potrzebę blokowania nieuprawnionych nadawców;
5) okresowo porządkować zawartość skrzynki pocztowej.

8. Użytkownik obsługuje konto pocztowe przy użyciu przeglądarki internetowej lub programu klienta pocztowego.

9. W przypadku planowanej nieobecności w pracy, użytkownik powinien uaktywnić funkcję informującą o nieobecności.

10. W uzasadnionych przypadkach Kierownik podejmuje decyzję o przekierowaniu wiadomości pocztowych na adres innego użytkownika poczty.

11. Użytkownik po powrocie do pracy podejmuje obsługę poczty elektronicznej i przywraca ustawienia osobiste programu pocztowego.

12. Kierowanie wiadomości pocztowych do grup użytkowników winno odbywać się z zastosowaniem polecenia UDW (ukryty do wiadomości), które powoduje, że użytkownicy wzajemnie nie mogą widzieć swych adresów pocztowych, w szczególności do użytkowników zewnętrznych.

13. Hasło użytkownika poczty elektronicznej do konta pocztowego musi spełniać cechy określone dla haseł dostępu wymaganych przy obsłudze danych osobowych, w szczególności nie może być udostępniane innym osobom, a w przypadku ujawnienia winno być niezwłocznie zmienione.

14. Awaryjna procedura resetu hasła jest prowadzona przez upoważnionego pracownika Winf.

§ 6. Zasady tworzenia konta poczty elektronicznej Urzędu.

1. Wszystkie konta (adresy) poczty elektronicznej Urzędu, które przydzielono Użytkownikom, stanowią własność Urzędu.

2. Dla sprawnej i nieprzerwanej obsługi poczty elektronicznej Urzędu ustanawia się skrzynki pocztowe (adresy poczty elektronicznej) podstawowe oraz pomocnicze z zastrzeżeniem, że wszystkie zostały ustanowione i przeznaczone wyłącznie do obsługi korespondencji służbowej Urzędu:

1) konto poczty elektronicznej dla wydziału lub biura Urzędu tworzone jest po ustaleniu zapisu, np.: winf@um.szczecin.pl co jest tożsame z nazwą jednostki w tym przypadku WInf;
2) konto użytkownika poczty elektronicznej tworzone jest na ogólnych zasadach, np.: login@um.szczecin.pl;

3) w przypadku wystąpienia konfliktu nazwy konta (powielenie nazwy) ASI wspólnie z pracownikiem ustalą nowy zapis nazwy konta.

3. Przesyłki poczty elektronicznej wychodzącej z Urzędu, winny być opatrywane stopką zgodną z:

a) standardami identyfikacji wizualnej Miasta Szczecin,

b) zadaniami informacyjnymi lub promocyjnymi ustalanymi z Dyrektorem WInf.

4. Obowiązują procedury dotyczące podłączenia stanowiska pracy do sieci teleinformatycznej (LAN Urzędu) i utworzenia konta poczty elektronicznej:

1) komputer - stanowisko pracy podłącza do sieci LAN Urzędu tylko pracownik WInf, niezwłocznie po wydaniu i ustawieniu we wskazanej lokalizacji;

2) konto domenowe dla nowego użytkownika tworzone jest tylko i wyłącznie na podstawie zgłoszenia przez kierownika. Dla czasowo zatrudnionego użytkownika wymagane jest określenie daty zakończenia umowy;

3) użytkownicy, nie będący pracownikami Urzędu, mogą otrzymać konto poczty elektronicznej Urzędu na podstawie zapisów umowy pomiędzy Urzędem i podmiotem zewnętrznym lub na podstawie polecenia Dyrektora WInf, gdzie wykonanie nastąpi za pośrednictwem procedur realizowanych poprzez WInf.

§ 7. Zasady likwidacji konta/adresu poczty elektronicznej.

1. Uprawnienia do konta poczty elektronicznej Użytkownika są blokowane i likwidowane po ustaniu zatrudnienia pracownika.

2. WInf blokuje konto użytkownika po otrzymaniu informacji od Kierownika.

3. W związku z likwidacją konta poczty elektronicznej (przykładowo: z powodu ustania zatrudnienia pracownika), ASI może podjąć procedurę zabezpieczenia dostępu do zawartości skrzynki pocztowej, którą inicjuje Kierownik, podlegającą na:

1) eksporcie skrzynki pocztowej i przekazaniu Kierownikowi pracownika, lub

2) przypisaniu skrzynki pocztowej innemu użytkownikowi w Urzędzie.

§ 8. Dla zapewnienia bezpieczeństwa poczty elektronicznej w sieci LAN Urzędu stosuje się obowiązkowo mechanizmy ochronne i procedury:

1) ochrona przed spamem (niepożądane przesyłki w poczcie elektronicznej) realizowana jest za pomocą dedykowanych narzędzi do ochrony poczty elektronicznej;

2) ochrona antywirusowa realizowana jest na wszystkich komputerach przez mechanizmy programu antywirusowego z serwerami realizujących dystrybucję wzorców i raportowanie;

3) ochrona brzegowa sieci LAN Urzędu realizowana jest automatycznie przez urządzenia o funkcjach filtrujących, blokujących, szyfrujących i raportujących. Urządzenia te zapewniają funkcje administracyjne siecią LAN i zapewniają wysoką dostępność wszystkich funkcji;

4) pracownicy Urzędu, zobowiązani są do reagowania na wszelkie nieprawidłowości, jakie zaobserwują w otrzymywanych przesyłkach pocztowych i zgłaszania do WInf.

§ 9. Procedury kontrolne dotyczące komputerowego stanowiska pracy w Urzędzie.

1. Winf dokonuje okresowych przeglądów zawartości komputerów stanowiących własność Urzędu za pomocą dedykowanych narzędzi. Okresowemu sprawdzaniu podlegają wszystkie komputery. Kontrola sprawowana jest poprzez automatyczne procedury oraz aplikacje skanujące komputery Urzędu. Wyniki skanowania komputerów zapisywane są w bazie danych. Procedury kontrolne nadzorują ASI. Obowiązek ten wprowadza się dla zapewnienia:

1) ochrony zasobów teleinformatycznych i danych Urzędu;

2) zgodności wykorzystywanych zasobów z posiadanymi uprawnieniami i licencjami.

2. Procedury sprawdzające realizowane są przy pomocy specjalistycznego oprogramowania, którego raporty stanowią podstawę dla działań naprawczych podejmowanych przez ASI oraz działań organizacyjnych podejmowanych przez Dyrektora WInf.

3. Przepływ informacji w sieci LAN Urzędu, generowany przez pracownika, podlega automatycznemu zapisowi dostępu do stron internetowych. Informacje statystyczne potwierdzające adresy sieciowe, czas dostępu do najczęściej odwiedzanych serwisów internetowych, gromadzonych plików oraz uruchamianych aplikacji podlegają automatycznej analizie w celu:

1) zbierania materiału dowodowego dla dalszych kroków podejmowanych na drodze służbowej;
2) generowania statystyk i ostrzeżeń dla użytkowników próbujących dostępów do stron WWW podlegających filtrowaniu i blokowaniu, gdzie ostrzeżenia dla użytkowników realizowane są w formie komunikatu ostrzegawczego, którego formę zatwierdza Dyrektor WInf.

Załącznik Nr 7 do zarządzenia Nr 312/23
Prezydenta Miasta Szczecin
z dnia 28 czerwca 2023 r.

Regulamin użytkowania urządzeń mobilnych w Urzędzie

§ 1. 1. Urząd występuje, jako właściciel urządzeń mobilnych oraz jako administrator urządzeń mobilnych, o których mowa w § 2 ust. 2.

2. Zapisy Regulaminu określają sposoby użytkowania urządzeń mobilnych, jako ponad standardowego wyposażenia stanowiska pracy w Urzędzie.

3. Użytkownik urządzenia mobilnego zwany jest dalej Użytkownikiem, to pracownik Urzędu, Radny Miasta Szczecin lub osoba upoważniona przez Prezydenta Miasta.

4. Jako urządzenia mobilne określa się przenośne urządzenie wyposażone w technologię komputerową i połączenie do sieci bezprzewodowych, komórkowych czy komputerowych, w szczególności tablety i smartfony.

§ 2. 1. Dopuszcza się zastosowanie urządzeń mobilnych w środowisku informatycznym Urzędu, przy wykorzystywaniu sieci komputerowej LAN Urzędu z uwzględnieniem wskazanych w Regulaminie ograniczeń.

2. Dopuszczenie, określone w ust.1 obejmuje urządzenia mobilne stanowiące własność prywatną Użytkowników.

§ 3. Obowiązki i odpowiedzialność.

1. WInf, zapewni obsługę urządzeń mobilnych w zakresie użytkowania technologii szyfrowania dla wskazanych urządzeń mobilnych, wg dostępności technologii zapotrzebowania użytkowników.

2. Użytkownicy urządzeń mobilnych zobowiązani są do:

1) fizycznej ochrony urządzenia mobilnego, w szczególności do bezpiecznego przechowywania i zabezpieczania przed kradzieżą, a w przypadku jego utraty do niezwłocznego powiadomienia WInf;

2) używania hasła lub kodu PIN do zabezpieczania urządzenia mobilnego, które to hasło winno być zgodne z polityką haseł określoną w niniejszym Zarządzeniu;

3) aktywowania funkcji „znajdź mój tablet” (lub smartfon) poprzez konto na portalu producenta lub dostawcy rozwiązań antykradzieżowych;

4) stosowania transmisji szyfrowanej, zgodnie z wytycznymi WInf;

5) użytkowania konta pocztowego poczty elektronicznej Urzędu zarządzanej przez WInf.

3. Odpowiedzialność Użytkowników urządzeń mobilnych dotyczy:

1) udostępniania oraz pobierania z sieci Internet materiałów chronionych prawami autorskimi (oprogramowanie, filmy, muzyka, itp.) lub zawierających materiały lub treści zakazane wprost odpowiednimi przepisami;

2) przesyłania i udostępniania treści mogących naruszyć prawa osób trzecich;

3) rozpowszechniania programów mogących uszkodzić oprogramowanie lub dane innych użytkowników Internetu;

4) uzyskiwania nieuprawnionego dostęp do zasobów systemów informatycznych będących w posiadaniu innych użytkowników sieci Internet;

5) realizacji zadań o charakterze komercyjnym.

§ 4. Katalog działań zarządczych sprawowanych przez Urząd.

1. Urząd, w związku z pracą Użytkownika na urządzeniu mobilnym, wyłącza swoją odpowiedzialność za wszelkie działania oraz za efekty pracy na tym urządzeniu, w szczególności, nie jest w żaden sposób odpowiedzialny za:

1) prywatne dane gromadzone lub przekazywane przez Użytkownika;

2) nieuprawnione użycie oprogramowania lub innych utworów będących przedmiotem ochrony własności intelektualnej, dostępnych w Internecie, czy przeniesionych w jakikolwiek sposób na urządzenie mobilne;

3) szkody potencjalne i faktyczne, jakie może spowodować Użytkownik w związku z korzystaniem z urządzeń mobilnych, a w szczególności za szkody bezpośrednie, pośrednie, przypadkowe czy też polegające na naruszeniu przepisów dotyczących danych osobowych;

4) ujawnienie danych podlegających jakiejkolwiek ochronie.

2. W przypadku korzystania przez Użytkownika z urządzenia mobilnego niezgodnego z przepisami prawa lub nie przestrzegania postanowień niniejszego Regulaminu, administrator sieci komputerowej LAN Urzędu obowiązany jest do zarejestrowania zdarzenia oraz do zablokowania dostępu urządzeniu mobilne.

Załącznik Nr 10 do zarządzenia Nr 312/23

Prezydenta Miasta Szczecin

z dnia 28 czerwca 2023 r.

Zasady stosowania pamięci komputerowych i pomocniczych ze wskazaniem poziomu ich bezpieczeństwa w Urzędzie

§ 1. Wszelkie pamięci komputerowe, eksploatowane poza zasobami pamięci dyskowej, którymi zarządza WInf należy traktować jako pamięci pomocnicze. Zalicza się do nich karty pamięci, pendrive, małe dyski przenośne - podłączane poprzez USB oraz dyski lub zestawy dysków podłączanych poprzez sieć komputerową oraz nośniki z zapisem optycznym (np. płyty CD i DVD).

§2. Wszystkie, powyżej wskazane rodzaje pamięci czy nośników danych nie powinny służyć do przechowywania danych osobowych.

§3. Tabela określająca potencjalne zastosowania oraz poziom bezpieczeństwa zewnętrznych pamięci i nośników danych w systemach komputerowych Urzędu

	Pendrive i karta pamięci	Mały dysk zewnętrzny	Duży dysk zewnętrzny lub zespół dysków (NAS)	CD i DVD
pojemność	Przeciętna pojemność 16 GB, dostępne są także duże pojemności do 512 GB	Łatwo dostępne są pojemności do 512 GB, dostępne są rozwiązania o pojemności 2 TB	Od 1 TB do wielu terabajtów, dostępne są rozwiązania o pojemności rzędu 10 TB	cd – 700 MB dvd - 4,7 GB dvd - 8,5 GB
przenaszalność	Warunkowa	Zakaz wynoszenia	Zakaz wynoszenia	Warunkowa
dane osobowe	Zakaz przetwarzania	Zakaz przetwarzania	Zakaz przetwarzania	Zakaz przetwarzania
zastosowanie	Zazwyczaj służą do przenoszenie danych, także do przechowywania	Kopia zapasowa danych dla lokalnej stacji	Archiwum danych dla lokalnej stacji lub grupy stacji. Możliwość pracy grupowej, tj. wymiany plików i pracy wspólnej	Głównie do zabezpieczenia i do przekazywania danych
wymagania dodatkowe	Należy stosować ochronę przed złamaniem hasła i szyfrowanie z algorytmem, (co najmniej AES-256)	Wymagane jest: zamykanie w szafie po użyciu, czyli zastosowanie zabezpieczenia fizycznego	Wymagane są: • zabezpieczenie przed ingerencją fizyczną • zabezpieczenie przed wynoszeniem • opiekun - administrator sprzętu (dysku), bez którego dane będą. podlegać dezintegracji	Należy opisać płytę (data zapisu, zawartość, itp.)
poziom bezpieczeństwa	Bardzo niski poziom bezpieczeństwa. Pendrive i karty samoistnie się uszkadzają, mogą być łatwo zagubione lub skradzione	Niski poziom bezpieczeństwa, mały dysk nie zapewnia lepszego bezpieczeństwa niż dysk w stacji roboczej, możliwość utraty jak i uszkodzenia	Poziom dobry, (co nie oznacza, że wysoki). Technologia zabezpieczająca przed utratą danych w połączeniu z procesem administrowania oraz zabezpieczeniem fizycznym dają dobry poziom bezpieczeństwa	Poziom dobry, pod warunkiem odpowiedniego przechowywania w zamykanych szafach (zabezpieczanie fizyczne)
uwagi	Bardzo popularne	Popularne	Stosowany przez administratorów WInf	Zastosowanie malejące może służyć, jako archiwum oraz do przekazywania danych

§ 4. Mając na uwadze konieczność użytkowania do celów służbowych pamięci pomocniczych, WInf zaleca:

1)należyte ich umiejscowienie;

2) maksymalne ograniczenie zastosowania pamięci typu pendrive. Pamięci typu pendrive ze względu na ich rozmiary i łatwą przenaszalność są stosowane powszechnie, nie powinny jednak zastępować rozwiązań bardziej bezpiecznych. W Urzędzie dopuszcza się jedynie rozwiązania z

kryptograficzną ochroną sprzętową (minimalny algorytm AES-256) oraz z ochroną przed złamaniem hasła metodą siłową (brute force). Do tej kategorii należą także wszelakie karty pamięci, powszechnie używane w aparatach fotograficznych i smartfonach, karta pamięci w połączeniu z czytnikiem kart posiada funkcjonalność równorzędną jak pendrive;

3) ograniczanie zastosowanie małych (miniaturowych) dysków przenośnych. Wielka pojemność wskazuje na potencjalnie wielkie straty w przypadku jego utraty. Dyski te mogą znaleźć jedynie zastosowanie, jako lokalne kopie zapasowe, a po godzinach pracy powinny być zabezpieczane fizycznie i nie mogą opuszczać pomieszczeń Urzędu;

4) zastosowanie dużego dysku lub zestawu dysków w obudowie, zwłaszcza z zastosowaniem zaawansowanych mechanizmów formatowania i ochrony. Użytkowanie dużych dysków jest uzasadnione, zwłaszcza dla jednostki, która nie ponosi dużych nakładów na utrzymanie takiego zasobu. Dyski te umożliwiają sprawną pracę grupową i zapewniają zabezpieczenia lepsze niż stacja robocza. Nie jest to jednak zasób całkowicie bezpieczny. Zastosowanie ich powoduje powstanie dodatkowych obowiązków administracyjnych dla jednostki. Duży dysk lub zestaw dysków w obudowie nie może być traktowany, jako zasób mobilny, powinien być zabezpieczony fizycznie, bezpiecznie zasilany i nie należy wynosić go poza pomieszczenia Urzędu;

5)płyty CD i DVD mogą pełnić rolę zasobów archiwalnych, a nakłady na utrzymanie takiego zasobu są minimalne. Płyty zapisane, jako archiwalne należy zabezpieczać w zamykanej szafie, nie mogą być wynoszone z Urzędu i powinny być opisane z podaniem czasu zapisu, zawartości i wykonawcy. Należy mieć na uwadze, że żywotność płyt jest ograniczona do około 10 lat.

§ 5. Składniki sprzętu informatycznego (system informatyczny lub nośniki) przed zbyciem lub likwidacją powinny podlegać skutecznemu usunięciu informacji ze szczególnym uwzględnieniem zawartości dysków twardych komputerów. Zaleceniem podstawowym jest procedura polegająca na demagnetyzacji nośnika przy pomocy dedykowanego sprzętu,
w innych przypadkach należy skutecznie niszczyć nośniki danych.

Załącznik Nr 11 do zarządzenia Nr 312/23
Prezydenta Miasta Szczecin
z dnia 28 czerwca 2023 r.

Zgłoszenie użytkownika systemów informatycznych w Urzędzie

WNIOSEK DOTYCZĄCY UPRAWNIEŃ PRACOWNIKA

NADANIE / ZMIANA / PRZEDŁUŻENIE / ODEBRANIE *

Jednostka organizacyjna:

Imię i nazwisko:

Nr ewidencyjny pracownika:

Stanowisko lub rodzaj pracy:

Komórka organizacyjna:

Zasady znakowania akt:

e-mail:

Telefon:

Czy następuje zmiana komórki organizacyjnej**: TAK / NIE

W przypadku zmiany komórki organizacyjnej:

Poprzednia komórka organizacyjna (wydział, referat):

Czy osoba była wcześniej pracownikiem UM i miała założone konto w systemie informatycznym*: TAK/NIE

Identyfikator sieciowy (login)**:

Oprogramowanie*:

- Konto AD + poczta + zasoby wydziałowe
- eDok: wybierz poziom*: dyrektor wydziału, kierownik referatu; sekretariat wydziału; referent; kancelaria, delegatura wydziału
- SIP - System Informacji Przestrzennej >>> >>> uzyskać akceptację od BGM
  wybierz poziom*: poziom I - podstawowy (imię, nazwisko, KW); poziom II - rozszerzony (pełne dane osobowe dot. EGiB);
  poziom III - pełne dane osobowe dot. EGiB + ewidencja ludności na mapie >>> dla poziomu III uzyskać akceptację od WSO
- iEGIB >>> >>> uzyskać akceptację od BGM
- SELWINWEB >>> >>> uzyskać akceptację od WSO
  wybierz poziom*: skrócony (aktualny adres); podstawowy (dane aktualne bez archiwalnych); rozszerzony (dane aktualne + dane archiwalne)
- SELWIN >>> >>> uzyskać akceptację od WSO
- BBD - Wydawanie Poświadczeń
- BBD - Rejestry Wydziału Urbanistyki
- DoKasy
- ICOR UM: wybierz poziom*: BIP; UMINET - Zarządzenia Prezydent; inne: ……
- BIP – Jednostki zewnętrzne
- Lex
- Kostka analityczna wybierz poziom*: budżetowa; hurtowniana; strategiczna
- Środowisko Raportowe (raporty budżetowe, opisowe i inne) - dostępne z przeglądarki
- Q-matic: wybierz oddział*: Lewobrzeże; Prawobrzeże; USC;
  wybierz poziom*: stanowisko; recepcja; statystyki; podgląd; kalendarz; koordynator; kierownik
- ZSI-FK (wymienić moduł, moduły): ……..
- ZSI-FK(test) (wymienić moduł, moduły): …….

- KOMAeHR: wybierz poziom*: KP_Kadry; KP_KZP; KP_Płace; KP_RCP; KP_Sekretariat; KP_Socjalny; KP_PPK; inne: …
- Zdalny dostęp (VPN)
- Inne: skrzynka e-mail ……..

.....

Okres obowiązywania uprawnień OD DO

(*DD-MM-RRRR*) (*DD-MM-RRRR / CZAS NIEOKREŚLONY*)

W przypadku braku określenia dat obowiązywania, uprawnienia nadawane są na okres 1 miesiąca.

Pracownik posiada upoważnienie do przetwarzania danych osobowych: TAK/NIE

Pracownik posiada dostęp do tajemnicy skarbowej*: TAK/NIE

Załącznik Nr 12 do zarządzenia Nr 312/23
Prezydenta Miasta Szczecin
z dnia 28 czerwca 2023 r.

Regulamin korzystania z zasobów teleinformatycznych Urzędu

§1. 1. Zasady korzystania z oprogramowania:

1) na komputerowym stanowisku pracy dozwolona jest eksploatacja oprogramowania przydzielonego przez WInf;
2) nośniki instalacyjne oprogramowania, dokumenty poświadczające posiadanie licencji oraz inne dowody poświadczające prawo korzystania z oprogramowania przechowuje WInf w miejscu niedostępnym dla osób nieupoważnionych;
3) zabrania się instalacji i eksploatacji oprogramowania innego, niż wymienione w pkt. 1;
4) w szczególności zabrania się pobierania i instalacji oprogramowania z Internetu, płyt CD/DVD, innych nośników danych stanowiących załącznik do literatury i czasopism informatycznych lub pochodzących z innych źródeł;
5) instalacji oprogramowania dokonuje pracownik WInf;
6) każda zmiana dotycząca oprogramowania zainstalowanego na stacji roboczej wymaga zgłoszenia wniosku do WInf, zaakceptowanego przez Kierownika;
7) w Urzędzie decyzje o obowiązującym standardzie oprogramowania dla stacji roboczych podejmuje WInf;
8) zabrania się pracy z komputerem bez zainstalowanego i aktywnego oprogramowania antywirusowego;
9) zabrania się rozbudowy i wprowadzania zmian w użytkowanym sprzęcie komputerowym oraz ingerencji w okablowanie strukturalne;
10) zabrania się wykorzystywania sprzętu i wyposażenia innego niż dostarczony przez WInf;
11) zabrania się wykorzystywania gniazd energetycznych infrastruktury informatycznej do celów innych, niż zasilanie stacji roboczych i urządzeń peryferyjnych. W szczególności zabrania się podłączania urządzeń o wysokim poborze mocy – czajniki, wentylatory, grzejniki itp.;
12) zlecenie konfiguracji komputera, wszelkie zmiany w stacjach roboczych, urządzeniach peryferyjnych i okablowaniu strukturalnym wykonują uprawnieni pracownicy WInf;
13) każdy użytkownik ma prawo i obowiązek pracy przy wykorzystaniu wyłącznie własnego, indywidualnego konta w systemach informatycznych. Obowiązuje zakaz pracy z wykorzystaniem cudzego konta. W przypadku zauważenia takiego faktu należy niezwłocznie poinformować o tym WInf lub IOD;
14) u obowiązuje bezwzględny zakaz ujawniania jakichkolwiek haseł własnych lub cudzych komukolwiek i kiedykolwiek;
15) zakładanie i usuwanie kont użytkowników oraz modyfikacja uprawnień uregulowane jest zgodnie z **Załącznikiem Nr 24** do Zarządzenia;

16) stacje robocze, znajdujące się w miejscach dostępnych dla osób nieuprawnionych (w szczególności dla interesantów), muszą być chronione wygaszaczem ekranu zabezpieczonym hasłem, z czasem uaktywnienia wygaszacza nie dłuższym niż 1 minuta. Ustawienie monitora powinno zapobiegać możliwości podglądania danych wyświetlanych na ekranie przez osoby nieuprawnione.

2. Oprogramowanie jest ewidencjonowane w rejestrze oprogramowania, dopuszczonego do stosowania w Urzędzie przez Winf.
3. Zabrania się:
   1) korzystania ze sprzętu niezgodnie z jego przeznaczeniem;
   2) instalowania i używania programów deszyfrujących hasła, skanujących infrastrukturę, łamiących zabezpieczenia oprogramowania;
   3) wykonywania innych działań mogących mieć wpływ na konfigurację komputerów / sieci oraz bezpieczeństwo Urzędu.
4. Pracownicy WInf mają prawo i obowiązek do:
   1) weryfikacji stanu eksploatowanego sprzętu i oprogramowania;
   2) usuwania nieautoryzowanego oprogramowania bez konieczności uzyskania akceptacji użytkowników i ich kierowników;
   3) blokowania konta w przypadku wykrycia naruszenia zasad bezpieczeństwa sieci lub wygaśnięcia konta użytkownika;
   4) stałego monitoringu bezpieczeństwa sieci w tym ruchu internetowego;
   5) stałego monitoringu wydruków na urządzeniach kopiujących i drukujących.
5. Dostęp do Internetu dozwolony jest tylko z wykorzystaniem metod i łącz autoryzowanych przez WInf.
6. Zabrania się stosowania innych metod, w szczególności samodzielnego instalowania modemów i kreowania kanałów dostępu przez telefony komórkowe i inne urządzenia. Powyższe nie dotyczy sprzętu służbowego wykorzystywanego poza lokalizacjami Urzędu.
7. Korzystanie ze stron www dozwolone jest wyłącznie w celach realizacji zadań służbowych.
8. Bezwzględnie zabrania się przeglądania stron www o charakterze erotycznym, pornograficznym, o zasobach dyskryminujących lub mogących urazić inne osoby itp. oraz stron do pobierania oprogramowania.

§ 2. Korzystanie z zasobów.

1. Zabrania się umieszczania na dyskach lokalnych stacji roboczych i dyskach sieciowych jakichkolwiek prywatnych lub publicznych (np. dostępnych w Internecie) plików multimedialnych (zdjęć, filmów, muzyki itp.).
2. W przypadku przechowywania plików multimedialnych przeznaczonych do zadań związanych z zakresem obowiązków pracownika (w tym prezentacji), zaleca się archiwizacje tych plików po ich wykorzystaniu. Pliki multimedialne starsze niż 6 miesięcy mogą być usuwane z dysków sieciowych bez powiadomienia użytkownika.

§ 3. WInf na bieżąco będzie przesyłał informacje pozwalające użytkownikom doskonalić swoją wiedzę, wyjaśnienia i bieżące zalecenia dotyczące bezpieczeństwa sieci. Użytkownicy zobowiązani są te informacje przyswajać i bezwzględnie się do nich stosować. W razie pytań lub wątpliwości mają się zwrócić do pracowników WInf.

§ 4. Winf może dopuścić do użytkowania w Urzędzie oprogramowanie spełniające jeden z warunków:

1) do którego Urząd posiada prawa autorskie;
2) licencjonowane dla Urzędu;
3) przekazane dla Urzędu przez inny podmiot z zastosowaniem cesji;
4) określone przez jego wytwórcę lub właściciela praw autorskich jako publicznie dostępne, w szczególności bezpłatne, bez opłat licencyjnych.

§ 5. Postanowienia końcowe:

1. Obowiązkiem każdego użytkownika zasobów informatycznych Urzędu jest ochrona tychże zasobów w sposób odpowiadający jego uprawnieniom, obowiązkom i możliwościom.
2. Urząd ma prawo do bieżącej, zdalnej lub bezpośredniej kontroli zasobów oraz ingerencji w zasoby bez powiadomienia.
3. Zawartość zasobów informatycznych (w tym poczty elektronicznej) jest własnością Urzędu. Jakiekolwiek ich wykorzystywanie niezgodnie z zadaniami wynikającymi z obowiązków służbowych jest zabronione, w szczególności zabrania się udostępniania danych z zasobów Urzędu osobom nieupoważnionym bez pisemnej zgody przełożonych.

Załącznik Nr 13 do zarządzenia Nr 312/23
Prezydenta Miasta Szczecin
z dnia 28 czerwca 2023 r.

Zasady wydawania upoważnień Administratora do przetwarzania danych osobowych

1. Upoważnienia ADO do przetwarzania danych osobowych wydawane jest każdemu pracownikowi, stażyście i praktykantowi mającemu lub mogącemu mieć dostęp do danych osobowych, niezależnie od formy zatrudnienia.
2. Upoważnienia przygotowywane są przez Wydział Organizacyjny Urzędu dla osób zatrudnionych, odbywających staż lub praktykę w Urzędzie na podstawie informacji kadrowych.
3. Upoważnienie jest aktualizowane /zmieniane w przypadku gdy:
    1) pracownik zmienił dane osobowe;
    2) pracownik zmienił stanowisko;
    3) pracownik zmienił jednostkę organizacyjną Urzędu.

4. Odwołanie upoważnienia następuje w przypadku, gdy upoważnienie było wydane na czas określony, a osoba kończy umowę o pracę, staż, praktykę przed tym terminem.

Załącznik Nr 14 do zarządzenia Nr 312/23
Prezydenta Miasta Szczecin
z dnia 28 czerwca 2023 r.

OŚWIADCZENIE

o zapoznaniu się z Zarządzeniem w sprawie określenia zasad bezpieczeństwa informacji oraz wytycznych dla Polityki Bezpieczeństwa Informacji Urzędu Miasta Szczecin

Oświadczam, iż zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych, w szczególności z przepisami 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 (Dz.Urz. UE.L Nr 119, str. 1 ze zm.), obowiązującą w Urzędzie dokumentacją ochrony danych osobowych, w tym z zasadami przetwarzania danych osobowych i bezpieczeństwa informacji.

Zobowiązuję się do:
1) zachowania w tajemnicy danych osobowych do których mam lub będę miał/a dostęp w związku z wykonywaniem obowiązków pracowniczych;
2) niewykorzystywania danych osobowych oraz innych informacji w celach pozasłużbowych, o ile informacje te nie są jawne;
3) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych oraz innych informacji, o ile informacje te nie są jawne;
4) korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków;
5) wykorzystywania jedynie legalnego oprogramowania pochodzącego od ADO;
6) należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją przetwarzania danych osobowych;
7) korzystania z komputerów przenośnych i innych urządzeń mobilnych zgodnie z zasadami przetwarzania danych osobowych przez użytkownika końcowego;
8) nieudostępniania sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.

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, za naruszenie przepisów karnych w zakresie ochrony danych osobowych lub za ciężkie naruszenie obowiązków umownych w przypadku umowy o pracę.
Jednocześnie przyjmuję do wiadomości, że WInf monitoruje wszelkie czynności wykonywane na komputerze takie jak:
1) zmiany w oprogramowaniu, w tym audyt legalności oprogramowania;
2) zmiany sprzętowe, w tym również podłączanie urządzeń zewnętrznych;
3) historia pracy i użytkowane aplikacje;
4) ruch internetowy wraz z historią przeglądanych stron;
5) monitoring wydruków zbierający statystyki wydrukowanych stron;
6) możliwość zdalnej pracy pracownika na komputerze użytkownika.

…….

data i podpis osoby upoważnionej

Załącznik Nr 23 do zarządzenia Nr 312/23
Prezydenta Miasta Szczecin
z dnia 28 czerwca 2023 r.

Wytyczne dotyczące audytu bezpieczeństwa informacji wykonywane przez podmiot zewnętrzny

§ 1. W Urzędzie przeprowadza się audyty SZBI:
1) audyt bezpieczeństwa informacji;
2) audyt zabezpieczeń systemów informatycznych.

§ 2. Audyty SZBI powinny być przeprowadzane co najmniej raz na rok kalendarzowy.

§ 3. 1. Audyt bezpieczeństwa informacji może być wykonywany przez uprawnionego pracownika Wydziału Kontroli i Audytu Wewnętrznego Urzędu.

2. W przypadku podjęcia decyzji o zleceniu usługi podmiotom zewnętrznym decyzję o rozpoczęciu postępowania celem zlecenia audytu zewnętrznego podejmuje ADO.

3. Zakres audytu zewnętrznego określany jest przez ADO po konsultacjach z WInf i IOD.

4. Wybór podmiotu świadczącego usługę audytu zewnętrznego odbywa się na podstawie przepisów dotyczących zamówień publicznych lub wewnętrznym przepisów w przypadku gdy zamówienie nie podlega wymogom ustawy zamówień publicznych.

§ 4. 1. Audyt przeprowadzany jest na podstawie zakresu i harmonogramu prac przygotowanego przez usługodawcę i zatwierdzonego przez ADO lub upoważnionego pracownika.

2. Audyt zewnętrzny nie powinien powodować utrudnień w realizacji zadań Urzędu.

§ 5. 1. W ramach przeprowadzania audytu usługodawca może otrzymać dokumentację w zakresie niezbędnym do realizacji przedmiotowych prac.

2. Dopuszcza się przekazanie kopii dokumentacji usługodawcy do pracy poza siedzibą Urzędu, o ile dokumentacja nie zawiera informacji prawnie chronionych.

3. Dokumentacja przekazywana jest za pokwitowaniem przez upoważnionego pracownika po stronie Urzędu.

4. Po zakończeniu audytu dokumentacja w postaci papierowej jest zwracana za potwierdzeniem.

5. Po zakończeniu audytu usługodawca podpisuje oświadczenie zawierające klauzule:
1) potwierdzające zwrot całości dokumentacji papierowej otrzymanej od Urzędu;
2) potwierdzającej zniszczenie wszelkich wykonanych przez siebie kopii dokumentacji papierowej;
3) potwierdzającej zniszczenie wszelkiej podlegającej audytowi dokumentacji elektronicznej otrzymanej od Urzędu oraz ich kopii.

§ 6. 1. Wywiady z pracownikami Urzędu (jeśli są przewidziane w metodyce audytu) powinny odbywać się w obecności pracownika, o którym mowa w § 4 ust. 1 lub kierownika osoby biorącej udział w wywiadzie.

2. Zakres wywiadu może dotyczyć wyłącznie zagadnień będących przedmiotem audytu i wynikających z umowy z usługodawcą przeprowadzającym audyt.

3. Wywiady podlegają dokumentowaniu przez osoby biorące w nich udział.

§ 7. 1. Wizje lokalne mogą odbywać się wyłącznie w obecności pracownika, o którym mowa w § 4 ust. 1, kierownika w którego gestii znajduje się dane pomieszczenie lub wyznaczonego przez niego pracownika.

2.Wyniki wizji lokalnych są dokumentowane w postaci protokołu i przekazywane ADO.

§ 8. Czynności audytowe dopuszczają możliwość rozdysponowania ankiet wśród pracowników Urzędu, celem zapoznania się ze świadomością pracowników w audytowanym obszarze.

§ 9. 1. Zakres audytu zabezpieczeń systemów informatycznych, metodyka przeprowadzenia audytu, w tym wykorzystywane narzędzia, oraz terminy realizacji prac podlegają zatwierdzeniu przez ADO.

2. Komputery usługodawcy i inne urządzenia informatyczne mogą być podłączone do sieci informatycznej Urzędu wyłącznie za zgodą Dyrektora WInf lub upoważnionego pracownika.

§ 10. 1.Wyniki audytu dokumentowane są w postaci raportu i przekazywane ADO.

2.Dopuszcza się odstąpienie od dokumentowania w postaci protokołów jeżeli audyt zabezpieczeń jest przeprowadzany przy pomocy specjalistycznego oprogramowania generującego raporty zawierające wyniki audytu.

3. Raport z audytu podlega zatwierdzeniu przez ADO.

4. Wnioski z audytu podlegają zatwierdzeniu i wdrożeniu jako działania korygujące i zapobiegawcze.

Załącznik Nr 24 do zarządzenia Nr 312/23
Prezydenta Miasta Szczecin
z dnia 28 czerwca 2023 r.

Procedura zarządzania uprawnieniami do zasobów/systemów informatycznych Urzędu

§1. Cel

Celem niniejszej procedury jest określenie uporządkowanego, skończonego ciągu czynności procesu zarządzania uprawnieniami, który obejmuje nadawanie, zmianę, przedłużenie oraz odebranie uprawnień pracownikom Urzędu* do zasobów i systemów informatycznych Urzędu Miasta Szczecin.

§2. Zakres procedury

Procedura obejmuje wszystkie jednostki Urzędu.

§3. Terminologia

1. **ALGORYTM** - uporządkowany, skończony ciąg czynności do wykonania określonego zadania

2. **ACTiVE DIRECTORY** - umożliwia zarządzanie tożsamościami i relacjami tworzącymi sieć organizacji. Zawiera informacje m. in. o serwerach, komputerach, użytkownikach, grupach i wszelkich innych obiektach występujących w sieci Urzędu.

§4. Przebieg realizacji / opis czynności

1. Rozpoczęcie procesu zarządzania uprawnieniami inicjuje każda zmiana kadrowa występująca w Urzędzie.

Zmiany kadrowe to:

1) nawiązanie stosunku pracy;
2) rozwiązanie stosunku pracy;
3) zmiana warunków umowy o pracę w zakresie zmiany stanowiska pracy, zmiany zakresu czynności.

2. Kierownik wnioskuje o uprawnienia dla pracownika.

3. Wniosek dotyczący uprawnień dla pracownika w zależności od rodzaju zmian kadrowych może dotyczyć:

1) nadania uprawnień - występuje w przypadku potrzeby przydzielenia nowych uprawnień do zasobów/systemów informatycznych, których do tej pory pracownik nie posiadał (dot. §4 ust. 1 pkt 1, 3)
2) odebrania uprawnień - występuje w przypadku potrzeby odebrania dostępu do zasobów/systemów informatycznych, które należy wskazać we wniosku (dot. §4 ust. 1 pkt 2, 3),
3) zmiany uprawnień - występuje w przypadku potrzeby rozszerzenia lub zmniejszenia przydzielonego dostępu do zasobów/systemów informatycznych. (dot. §4 ust. 1 pkt 3),
4) przedłużenia uprawnień - występuje w przypadku przedłużenia stosunku pracy oraz braku potrzeby zmiany zakresu, a także poziomu uprawnień*.

4. Wniosek dotyczący odebrania uprawnień przekazywany jest bezpośrednio do WInf.

5. Wniosek dotyczący nadania, zmiany, przedłużenia uprawnień należy zweryfikować czy dotyczy zasobu/systemu informatycznego, dla którego wymagane jest wyrażenie zgody na przetwarzanie danych przez Właściciela zasobu:

1) jeżeli TAK: wniosek zostaje przekazany do Właściciela zasobu, który w przypadku wyrażenia zgody, załącza do wniosku dokument potwierdzający udzielenie zgody na dostęp do danych wraz ze wskazaniem poziomu dostępu, następnie wniosek jest przekazywany do WInf,
2) jeżeli NIE: wniosek jest przekazywany do WInf.

6. WInf otrzymuje wniosek dotyczący uprawnień dla pracownika.

7. WInf dokonuje weryfikacji wniosku pod względem poprawności:
1) formularza wniosku;
2) osoby wnioskującej;
3) wyrażenia zgód przez Właścicieli zasobu do nadania uprawnień;
4) wypełnienia pozycji obowiązkowych.

8. Wynik przeprowadzonej weryfikacji wniosku decyduje o dalszym postępowaniu:
1) jeżeli wniosek jest poprawny, zostaje zadekretowany;
2) jeżeli wniosek nie jest poprawny, zostaje zwrócony Kierownikowi wraz ze wskazaniem jego nieprawidłowości.

9. Dekretacja wniosku dotyczącego uprawnień następuje poprzez:
1) dekretację wniosku przez Dyrektora WInf,
2) przygotowanie wersji elektronicznej zadekretowanego wniosku.

10. WInf rejestruje wniosek dotyczący uprawnień w systemie informatycznym.

11. Zarejestrowany wniosek jest weryfikowany, analizowany oraz uzupełniany niezbędnymi informacjami przez WInf.

12. Analiza zarejestrowanego wniosku - czy dotyczy działań związanych z Active Directory:
1) jeżeli TAK: wniosek zostaje przekazany do ASI,
2) jeżeli NIE: wniosek zostaje przekazany do ASI z danego systemu dziedzinowego.

13. Analiza zarejestrowanego wniosku - czy dotyczy kilku ASU:
1) jeżeli TAK: wykonywana jest odpowiednia ilości kopii zarejestrowanego wniosku,
2) jeżeli NIE: przekazanie wniosku do właściwego ASU.

14. Zarejestrowany wniosek przekazany jest do właściwego ASU.

15. ASU realizuje zarejestrowany wniosek.

16. ASU informuje bezpośredniego przełożonego pracownika o realizacji wniosku dotyczącego uprawnień.

17. Pracownik, którego dotyczył wniosek, weryfikuje poprawność realizacji wniosku dot. uprawnień (dot. §4 ust. 3. pkt 1, 3, 4).

§5. Procedurę zarządzania uprawnieniami do zasobów/systemów informatycznych Urzędu stosuje się odpowiednio do podmiotu zewnętrznego.

**Zmiana kadrowa dotycząca zmiany jednostki przez pracownika Urzędu generuje dwa wnioski:*
- *wniosek Kierownika, w którym pracownik zakończył pracę, o odebranie uprawnień,*
- *wniosek Kierownika, w którym pracownik rozpoczął pracę, o nadanie uprawnień.*

Załącznik Nr 25 do zarządzenia Nr 312/23
Prezydenta Miasta Szczecin
z dnia 28 czerwca 2023 r.

Procedura testu równowagi prawnie uzasadnionego interesu ADO

§ 1.

1. Test równowagi polega na porównaniu prawnie uzasadnionych interesów realizowanych przez ADO w związku z konkretnymi czynnościami przetwarzania danych osobowych z interesami lub podstawowymi prawami i wolnościami osoby, której dane dotyczą.
2. IOD informuje Kierownika o konieczności przeprowadzenia testu równowagi dla konkretnego procesu przetwarzania danych osobowych.
3. Test równowagi przeprowadzany jest przez Kierownika, przy współpracy z pracownikami uczestniczącymi w procesie przetwarzania danych osobowych, który podlega testowi równowagi.
4. Test równowagi składa się z następujących etapów:
   1) zidentyfikowanie prawnie uzasadnionych interesów ADO lub strony trzeciej, realizowanych w związku z przetwarzaniem danych osobowych w określonym celu;
   2) zidentyfikowanie interesów lub podstawowych praw i wolności osoby, której dane dotyczą, a które mogą być naruszone przez przetwarzanie danych osobowych;
   3) ustalenie, czy przetwarzanie danych osobowych w danych okolicznościach jest konieczne do zrealizowania prawnie uzasadnionego interesu ADO lub strony trzeciej;
   4) dokonanie ważenia interesów ADO lub strony trzeciej i osoby, której dane dotyczą.
5. Ważenie interesów podczas przeprowadzanego testu równowagi, polega na określeniu, czyje interesy mają charakter nadrzędny. Podczas ważenia interesów uwzględnia się, w szczególności:
   1) charakter danych osobowych;
   2) kategorie osób, których dane dotyczą;
   3) relacje zachodzące pomiędzy ADO, a osobą, której dane dotyczą;
   4) uzasadnione oczekiwania osób, których dane dotyczą;
   5) sposób przetwarzania danych;
   6) ewentualne szkody ADO związane z zaniechaniem przetwarzania;
   7) zastosowane środki bezpieczeństwa.
6. Kierownik wykonuje test równowagi poprzez wypełnienie:
   1) wzoru testu równowagi prawnie uzasadnionych interesów ADO – obligatoryjnie;
   2) wzoru załącznika do testu równowagi prawnie uzasadnionego interesu ADO – fakultatywnie, tj. wyłącznie wówczas, gdy IOD uzna, że z uwagi na charakter i sposób przetwarzania danych osobowych w analizowanym procesie, zachodzi potrzeba dodatkowego przeanalizowania stosowanych zabezpieczeń ochrony danych.
7. Wynik testu równowagi może być:
   1) pozytywny dla ADO tj. interesy osoby, której dane dotyczą nie są nadrzędne wobec interesów ADO lub strony trzeciej;
   2) negatywny dla ADO tj. interesy osoby, której dane dotyczą są nadrzędne wobec interesów ADO lub strony trzeciej.

§ 2.

1. Wynik testu równowagi jest negatywny dla ADO, w szczególności wówczas, gdy istnieje możliwość zrealizowania tego samego celu bez konieczności przetwarzania danych osobowych lub ograniczając ich przetwarzanie.

2. Kierownik przekazuje wynik testu równowagi do IOD.
3. Jeżeli wynik testu równowagi jest negatywny dla ADO, wraz z tym wynikiem IOD przekazuje ADO rekomendacje w zakresie dalszego przetwarzania danych osobowych. Rekomendacje mogą dotyczyć, w szczególności:
   1) wdrożenia odpowiednich środków naprawczych mających wpływ na wzajemne interesy ADO lub stron trzecich i osoby, której dane dotyczą;
   2) zmiany podstawy prawnej przetwarzania danych osobowych w procesie;
   3) zaprzestania przetwarzania danych osobowych w procesie.
4. Na podstawie przedstawionego wyniku testu równowagi ADO podejmuje decyzję odnośnie dalszego przetwarzania danych osobowych w procesie.
5. Jeżeli wynik testu równowagi jest negatywny dla ADO i podjął on decyzję o wdrożeniu rekomendowanych przez IOD odpowiednich środków naprawczych, wówczas za koordynację ich wdrożenia odpowiada Kierownik współpracując przy tym z IOD.
6. Po wdrożeniu środków, o których mowa w ust. 5, Kierownik ponownie przeprowadza test równowagi na zasadach opisanych w procedurze.
7. W przypadkach, kiedy już po przeprowadzeniu testu równowagi, proces przetwarzania uległ znaczącej zmianie w stosunku do jego pierwotnego charakteru i może mieć wpływ na wzajemne interesy ADO lub strony trzeciej i osoby, której dane dotyczą, test równowagi powinien zostać wykonany ponownie, na zasadach opisanych w niniejszej procedurze.

§ 3. Wzór Testu równowagi prawnie uzasadnionego interesu ADO umieszczony jest na UMiNET w zakładce RODO/ Ochrona danych.

Załącznik Nr 26 do zarządzenia Nr 312/23
Prezydenta Miasta Szczecin
z dnia 28 czerwca 2023 r.

Procedura kontroli podmiotów przetwarzających dane osobowe w imieniu ADO

§1. ADO dopuszcza, by dane osobowe, których jest administratorem w rozumieniu art. 4 pkt 7 RODO, były przetwarzane poza jego strukturami organizacyjnymi przez podmioty przetwarzające.
§ 2. Przetwarzanie danych osobowych przez podmioty przetwarzające może się odbywać wyłącznie w określonym celu i zakresie, na mocy umowy powierzenia lub innego instrumentu prawnego.
§3. ADO ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych z punktu widzenia zgodności tego przetwarzania z:
1) przepisami prawa;
2) postanowieniami zawartej umowy powierzenia;
3) wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności.

§4. 1. Kontrola, o której mowa w § 3 prowadzona jest w postaci audytu podmiotu przetwarzającego.
2. Szczegóły dotyczące audytu podmiotu przetwarzającego określa zawarta z tym podmiotem umowa powierzenia.
3. W sytuacji, gdy umowa powierzenia nie określa sposobu i terminu przekazywania podmiotowi przetwarzającemu informacji o terminie i zakresie audytu, kwestie te ustalane są z tym podmiotem w formie porozumienia przed przeprowadzeniem pierwszego audytu, z zastrzeżeniem, że poczynione ustalenia pozostają właściwe dla przyszłych audytów.
4. Audyt podmiotu przetwarzającego może zostać przeprowadzony, w szczególności w następujących przypadkach:
1) powierzenie przetwarzania obejmuje szczególne kategorie danych osobowych i/lub dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa;
2) powierza się przetwarzanie danych osobowych na dużą skalę;
3) ADO otrzymał informację o incydentach z zakresu ochrony danych osobowych występujących u podmiotu przetwarzającego.

5. Decyzję o przeprowadzeniu audytu podmiotu przetwarzającego podejmuje ADO:
1) Samodzielnie;
2) na podstawie złożonego wniosku o przeprowadzenie audytu.

6. Z wnioskiem o przeprowadzenie audytu podmiotu przetwarzającego występuje IOD.
7. Wniosek o przeprowadzenie audytu podmiotu przetwarzającego składany jest do ADO.
8. Na podstawie otrzymanego wniosku, ADO podejmuje ostateczną decyzję o przeprowadzeniu audytu podmiotu przetwarzającego. Gdy jest to zasadne, przed podjęciem decyzji, ADO konsultuje się z IOD.
9. Audyt podmiotu przetwarzającego realizowany jest przez IOD.
10. Jeżeli jest to zasadne, IOD realizuje audyt przy współpracy z innymi osobami upoważnionymi przez ADO, których wiedza może mieć kluczowe znaczenie dla merytorycznej poprawności przeprowadzanego audytu.
11. ADO może zlecić realizację audytu podmiotowi zewnętrznemu.
§5. 1. Audyt podmiotu przetwarzającego realizowany jest:
1) w siedzibie podmiotu przetwarzającego,
2) w głównym miejscu przetwarzania powierzonych danych osobowych, lub

3) zdalnie.

2. IOD oraz osoba odpowiedzialna za bezpośrednią współpracę i utrzymywanie stałych kontaktów z podmiotem przetwarzającym opracowują wspólnie harmonogram przeprowadzania audytu, który wskazuje w szczególności na:
1) termin audytu;
2) miejsce audytu;
3) zakres audytu;
4) osoby biorące udział w audycie.

3. IOD, przy współpracy z osobą odpowiedzialną za bezpośrednią współpracę i utrzymywanie stałych kontaktów z podmiotem przetwarzającym, informuje ten podmiot o terminie, miejscu i zakresie audytu.

4. IOD przeprowadza audyt z wykorzystaniem formularza audytu, którego wzór znajduje się na UMiNET w zakładce RODO/ Ochrona danych.

5. Formularz audytu uzupełniany jest:
1) w przypadku audytu w siedzibie podmiotu przetwarzającego lub w głównym miejscu przetwarzania powierzonych danych osobowych – przez IOD oraz inne osoby realizujące audyt, o których mowa w § 4,
2) w przypadku audytu zdalnego – przez osoby upoważnione do tego przez podmiot przetwarzający.

§ 6. 1. Po przeprowadzonym audycie IOD sporządza protokół poaudytowy, według wzoru znajdującego się na UMiNET w zakładce RODO/ Ochrona danych .

2. IOD przedkłada Protokół poaudytowy:
1) ADO,
2) podmiotowi przetwarzającemu.

3. Podmiot przetwarzający ma 7 dni na ustosunkowanie się do treści przedstawionego mu Protokołu poaudytowego, z zastrzeżeniem, że umowa powierzenia zawarta z tym podmiotem może określać inny termin.

4. Jeżeli w wyniku audytu stwierdzono niezgodność przetwarzania powierzonych danych osobowych z:
1) obowiązującymi przepisami prawa, lub
2) postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych,
3) wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności,

ADO, na podstawie przedłożonego mu Protokołu poaudytowego, podejmuje ostateczną decyzję w zakresie dalszej współpracy z podmiotem przetwarzającym.

Załącznik Nr 27 do zarządzenia Nr 312/23
Prezydenta Miasta Szczecin
z dnia 28 czerwca 2023 r.

Plan wewnętrznego audytu zgodności przetwarzania danych u ADO

§1. 1. Audyt zgodności przetwarzanych danych osobowych, zwany dalej audytem przeprowadza IOD.
2. ADO może wyznaczyć zespół ds. przeprowadzenia audytu.
3. Audyt przeprowadza się w trybie:
1) planowym - według planu audytów zatwierdzonych przez ADO;
2) audytu doraźnego - niezwłocznie w sytuacji powzięcia przez ADO wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia.

3. IOD podlega wyłączeniu z zespołu ds. audytu jeżeli audyt ma obejmować zakres działań IOD.
4. IOD przygotowuje plan audytu zgodności przetwarzania danych osobowych w okresie nie dłuższy niż rok - wskazując jednostki, które będą podlegać ww. audytowi.
5. Plan jest przedstawiany przez IOD do wiadomości ADO i kierownikowi co najmniej 2 tygodnie przez wskazanym w planie dniem rozpoczęcia audytu.
6. W planie audytu uwzględnia się wszystkie czynności przetwarzania podlegające audytowi.
§ 2. 1. Plan określa:
1) termin rozpoczęcia audytu;
2) zagadnienia, które będzie obejmował audyt, w szczególności.:
   a) funkcjonowanie zastosowanych środków organizacyjnych;
   b) funkcjonowanie zabezpieczeń systemowych;
   c) funkcjonowanie zastosowanych zabezpieczeń fizycznych;
   d) legalność przetwarzania danych;
   e) realizowanie obowiązków informacyjnych;
   f) realizowanie praw osób, których dane dotyczą;
   g) powierzanie przetwarzania danych osobowych.
3) czynności lub procesy przetwarzania, które będzie obejmował audyt;
4) sposób przeprowadzenia audytu w szczególności:
   a) oględziny w wybranych obszarach przetwarzania;
   b) przegląd dokumentów;
   c) uzyskanie wyjaśnień od osób przetwarzających dane;
   d) uzyskanie wyjaśnień od osób odpowiedzialnych za bezpieczeństwo danych;
   e) wgląd w dokumenty zawierające dane osobowe;
   f) wgląd do systemów służących do przetwarzania danych.
5) przyjęcie do wiadomości przez ADO informacji o planowanym audycie zgodności przetwarzania danych, w tym o konieczności poinformowania pracowników o audycie i zapewniania IOD środków technicznych i organizacyjnych niezbędnych do przeprowadzania audytu zgodności z przepisami RODO.

§ 3. 1. Wszelkie czynności podjęte w toku audytu należy udokumentować.
2. Dokumentowanie czynności podjętych w toku audytu dotyczącego technicznego i organizacyjnego zabezpieczenia obszarów przetwarzania danych osobowych może polegać, w szczególności, na:
1) sporządzeniu notatki z wizji lokalnej.

2) sporządzeniu notatki z odebrania ustnych wyjaśnień.

3. Dokumentowanie czynności podjętych w toku audytu dotyczącego zbiorów danych i systemów informatycznych służące do przetwarzania danych osobowych może polegać, w szczególności, na:

1) utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych;
2) sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
3) odebraniu wyjaśnień od osoby, której czynności objęto sprawdzeniem;
4) sporządzeniu kopii otrzymanego dokumentu;
5) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
6) sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

§4. 1. Po zakończeniu audytu zgodności przetwarzania danych osobowych IOD przygotowuje protokół pokontrolny.

2. Po podpisaniu przez IOD protokół pokontrolny przedstawia się ADO a następnie po jego zapoznaniu się i zatwierdzeniu przedstawia się Kierownikowi audytowanej jednostki.

§ 5. 1. Realizacja zaleceń pokontrolnych podlega na podjęciu działań zaradczych w przypadku stwierdzonych nieprawidłowości.

2. IOD zobowiązany jest do opracowania harmonogramu realizacji zaleceń pokontrolnych wydanych w trakcie audytu zgodności przetwarzania danych osobowych, który otrzymują:

1) jednostka odpowiedzialna za wykonanie zaleceń;
2) IOD.

3. IOD może przeprowadzać czynności sprawdzające dokonując oceny działań jednostek, odpowiedzialnych za wykonanie zaleceń pokontrolnych.

4. Z wykonania zaleceń pokontrolnych Kierownik audytowanej jednostki przedstawia notatkę z wykonania zaleceń pokontrolnych.

5. IOD sporządza protokół z kontroli sprawdzającej dotyczącej wykonania zaleceń pokontrolnych wynikających z przeprowadzonego audytu.

Załącznik Nr 28 do zarządzenia Nr 312/23
Prezydenta Miasta Szczecin
z dnia 28 czerwca 2023 r.

Procedura obsługi żądań podmiotów danych

§ 1.

1. Procedura określa ogólne ramy postępowania z żądaniami podmiotów danych, kierowanymi do ADO, dotyczącymi praw podmiotu danych.
2. Żądania podmiotów danych polegają na:
   1) prawie do bycia poinformowanym o przetwarzaniu danych przy zbieraniu danych, od osoby, której dane dotyczą;
   2) prawie do bycia poinformowanym o przetwarzaniu danych w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą;
   3) prawie realizowanym na wniosek:
      a) prawie dostępu przysługujące osobie, której dane dotyczą,
      b) prawie do sprostowania danych,
      c) prawie do usunięcia danych („prawo do bycia zapomnianym”),
      d) prawie do ograniczenia przetwarzania,
      e) prawie do powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania,
      f) prawie do przenoszenia danych,
      g) prawie do sprzeciwu,
      h) prawie do wycofania zgody na przetwarzanie danych,
      i) prawie do poinformowania o naruszeniach

3. W każdym przypadku, w którym sposób postępowania nie wynika wprost z procedury, niezbędna jest konsultacja z IOD.
4. Żądanie dotyczące praw podmiotu danych może być złożone w formie elektronicznej.
5. Żądania dotyczące praw podmiotu danych realizuje Kierownik.
6. W razie skierowania żądania do niewłaściwej jednostki pracownik, który otrzymał żądanie, zobowiązany jest niezwłocznie, lecz nie później niż do końca dnia roboczego, w którym żądanie wpłynęło, przekazać je do właściwej jednostki.
7. W przypadku braku możliwości jednoznacznej weryfikacji tożsamości Wnioskodawcy Kierownik może zażądać dodatkowych informacji w celu potwierdzenia tożsamości Wnioskodawcy, zgodnie z postanowieniami § 2 procedury.
8. Rozpoznanie żądania zgłoszonego przez pełnomocnika Wnioskodawcy możliwe jest pod warunkiem, że przedstawia on pełnomocnictwo (upoważnienie), z którego jednoznacznie wynika umocowanie do zgłoszenia żądania i zakres żądania.
9. W przypadku braku możliwości jednoznacznego określenia faktycznej treści żądania Wnioskodawcy Kierownik może żądać od Wnioskodawcy dodatkowych wyjaśnień.
10. Po załatwieniu sprawy Kierownik przekazuje wniosek i odpowiedź w sprawie do IOD.
11. Rejestr wszystkich wniosków prowadzi IOD.

§ 2.

1. Przed udzieleniem odpowiedzi na żądanie Kierownik jest zobowiązany do weryfikacji tożsamości Wnioskodawcy.

2. W przypadku braku możliwości jednoznacznej weryfikacji tożsamości Wnioskodawcy może on żądać dodatkowych informacji w celu potwierdzenia tożsamości Wnioskodawcy.
3. Weryfikacja tożsamości Wnioskodawcy powinna każdorazowo odbywać się zgodnie z poniższymi zasadami:
    1) w przypadku żądania od Wnioskodawcy podania dodatkowych danych w celu jednoznacznego potwierdzenia tożsamości Wnioskodawcy należy pozyskiwać jedynie dane w zakresie niezbędnym dla osiągnięcia zamierzonego celu;
    2) w przypadku żądania od Wnioskodawcy podania dodatkowych danych w celu jednoznacznego potwierdzenia tożsamości Wnioskodawcy należy niezwłocznie, lecz nie później niż w ciągu miesiąca, poinformować Wnioskodawcę, że termin udzielenia odpowiedzi na żądanie będzie liczony od dnia udzielenia informacji umożliwiających jednoznaczną identyfikację;
    3) w przypadku okazania przez Wnioskodawcę dokumentu w celu umożliwienia jednoznacznego potwierdzenia tożsamości dokument powinien być pozyskiwany wyłącznie do wglądu, tzn. nie powinna być wykonywana jego kopia ani skan.

§ 3.

1. Kierownik zobowiązany jest udzielić odpowiedzi na żądanie w terminie miesiąca od dnia jego otrzymania (tzn. od dnia wpłynięcia żądania do ADO). W przypadku zamiaru przesłania odpowiedzi drogą pocztową zapewnia, by odpowiedź została wysłania nie później niż w terminie 3 dni roboczych przed upływem miesiąca od daty otrzymania żądania.
2. Jeżeli koniec terminu przypada na dzień ustawowo wolny od pracy lub sobotę, termin upływa następnego dnia, który nie jest dniem wolnym od pracy ani sobotą.
3. W przypadkach otrzymania żądania, w związku z którym konieczne jest:
    1) ustalenie lub weryfikacja tożsamości Wnioskodawcy lub
    2) ustalenie lub doprecyzowanie przedmiotu żądania– miesięczny termin dotyczy podjęcia czynności w celu uzyskania informacji niezbędnych do ustalenia powyższych okoliczności. W takim przypadku termin na udzielenie odpowiedzi na żądanie wynosi miesiąc od dnia uzyskania przez Kierownika wszystkich informacji niezbędnych do realizacji żądania.
4. Kierownik uprawniony jest do przedłużenia terminu udzielenia odpowiedzi na żądanie jedynie w przypadku, gdy dochowanie miesięcznego terminu nie jest możliwe z uwagi na skomplikowany charakter żądania lub dużą liczbę zgłoszonych żądań. W przypadku przedłużenia terminu rozpatrzenia żądania Kierownik zobowiązany jest poinformować Wnioskodawcę w terminie miesiąca od otrzymania żądania o przedłużeniu terminu udzielenia odpowiedzi, wskazując przyczyny przedłużenia terminu.
5. Jeżeli Kierownik nie podejmuje działań w związku z żądaniem Wnioskodawcy, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje Wnioskodawcę o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego i skorzystania ze środków ochrony prawnej przed sądem.
6. W przypadku, w którym żądanie zostało skierowane do ADO elektronicznie, odpowiedzi udziela się w tej samej formie, chyba że Wnioskodawca zażądał udzielenia odpowiedzi w innej formie. W innych przypadkach odpowiedzi udziela się pisemnie.

7. Odmowa podjęcia działań w związku ze zgłoszonym żądaniem dopuszczalna jest wyłącznie w przypadku, gdy:
   1) żądanie jest ewidentnie nieuzasadnione;
   2) żądania Wnioskodawcy są nadmierne, w szczególności gdy ich zgłaszanie ma charakter ustawiczny.
8. O odmowie podjęcia działań z uwagi na powyższe okoliczności Kierownik informuje Wnioskodawcę w terminie miesiąca od otrzymania żądania.

§ 4. Zobowiązuje się kierowników do ścisłej współpracy z IOD w zakresie przygotowania odpowiedzi na żądanie podmiotu danych.