Załącznik Nr 2 do Zarządzenia Nr 150/18

Prezydenta Miasta Szczecin

z dnia 6 kwietnia 2018 r.

Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Miasta Szczecin

§ 1. Instrukcja zarządzania systemem informatycznym Urzędu określa:

1) sposób zabezpieczenia i zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,

2) zasady ochrony danych osobowych zawartych w systemie informatycznym Urzędu (A.18.1.4*),

3) zasady użytkowania programów komputerowych i baz danych Urzędu,

4) zasady korzystania z zasobów informatycznych Urzędu Miasta Szczecin określono w Załączniku nr 4 do Zarządzenia.

2. Bezpieczeństwo informacji w systemach teleinformatycznych wymaga wdrożenia odpowiednich ról w celu prawidłowego zarządzania bezpieczeństwem informacji w Urzędzie. Zadania wynikające z przewidzianych ról zostają przypisane do obowiązków pracownika. Przetwarzanie informacji musi być wykonywane na urządzeniach zgodnych z minimalnymi wymaganiami w zakresie bezpieczeństwa.

3. Minimalne wymagania definiują standardy bezpieczeństwa informacji w Urzędzie w zakresie: stacji roboczej, serwera, urządzenia sieci teleinformatycznej, systemu operacyjnego oraz aplikacji opartej o przeglądarkę internetową.

4. Autoryzacja środków przetwarzania informacji obejmuje swoim zakresem wszystkie urządzenia teleinformatyczne. W przypadku przetwarzania informacji na urządzeniach, które nie są zdefiniowane przez standardy np. urządzenia mobilne z własnym systemem operacyjnym, ASI dokonuje weryfikacji konfiguracji urządzenia pod kątem naruszenia bezpieczeństwa teleinformatycznego.

§ 2. Celem wprowadzanych Instrukcją regulacji jest ochrona danych, w tym danych osobowych zawartych w systemie informatycznym Urzędu. (pkt 6.2*)

§ 3. Określone niżej sposoby zabezpieczeń dotyczą:

1) zabezpieczenia przed dostępem do danych osób nieupoważnionych na etapie eksploatacji systemów tj. wprowadzania danych, aktualizacji lub usuwania danych, wyświetlania lub drukowania zestawień,

2) ochrony danych zarchiwizowanych na nośnikach zewnętrznych, procedur niszczenia niepotrzebnych wydruków lub nośników danych,

3) systemu zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których eksploatowane są systemy,

4) sposobów dostępu do pomieszczeń , w których eksploatowane są systemy uprawnionych pracowników Urzędu oraz firm zewnętrznych,

5) monitorowania systemu zabezpieczeń,

6) wprowadzenia odpowiednich zapisów do zakresów obowiązków pracowników zatrudnionych przy przetwarzaniu danych osobowych.

§ 4. Dla zapewnienia prawidłowego bezpieczeństwa funkcjonowania systemu informatycznego Urzędu przyjmuje się następujące sposoby zabezpieczeń:

1) podstawowym sposobem zabezpieczenia danych i dostępu do nich w trybie online jest system definiowania użytkowników, grup użytkowników oraz haseł. Są to zabezpieczenia programowe wmontowane w system zarządzania siecią oraz w eksploatowane systemy użytkowe uniemożliwiające dostęp do systemu osobom nieupoważnionym. Zasady obowiązujące przy definiowaniu użytkowników i przydziału haseł określa procedura administrowania identyfikatorami i hasłami dostępu - stanowiąca **Załącznik nr 16** do zarządzenia,

2) fizyczny dostęp do pomieszczeń, w których eksploatowane są systemy chronią odpowiednio do wagi zagrożeń: zamykane drzwi, zakratowane okna pomieszczeń na parterze, alarmy, szafy pancerne i sejfy, ochrona Urzędu, system monitorowanego dostępu do pomieszczeń, system kontroli wejścia do pomieszczeń,

3) wejście do pomieszczenia serwerowni jest chronione przez system monitoringu, drzwi oraz niezależny alarm przy wejściu,

4) archiwalne kopie danych wykonywane są na urządzeniach archiwizujących w serwerowni, a przechowywane są wg zasad określonych w procedurze tworzenia i przechowywania kopii bezpieczeństwa - stanowiącej **Załącznik nr 17** do zarządzenia,

5) indywidualne zakresy obowiązków pracowników powinny określać zakres odpowiedzialności tych osób za ochronę tych danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem - w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.

§ 5. 1. Wprowadza się zabezpieczenie danych i dostępu do danych.

2. Zabezpieczenie danych zorganizowane jest poprzez:

1) odpowiednią ochronę zbiorów i sposobu dostępu do nich,

2) zapisywanie wszystkich zbiorów zawierających dane osobowe na dyskach komputerów głównych – serwerów,

3) wprowadzenie w głównych serwerach systemu zapisu na macierzy dyskowej zwiększającej poprawność zapisu i bezpieczeństwo danych,

4) codzienną archiwizację danych,

5) bieżącą ochronę przed wirusami serwerów i stacji roboczych za pomocą zainstalowanych programów kontrolujących zawartość zbiorów uruchamianych razem z komputerem.

3. W celu zapewnienia poufności stosuje się zabezpieczenia kryptograficzne oraz działania uświadamiające pracowników w zakresie zachowania tajemnicy pracodawcy i danych osobowych. Aby zachować dostępność danych stosuje się podwojenie rozwiązań teleinformatycznych (budowa klastrów serwerów, wykorzystywanie macierzy dyskowych do przechowywania danych wraz z zabezpieczeniem nadmiarowej ilości dysków twardych, redundancja łącza internetowego itp.). W Urzędzie stosuje się fizyczną granicę obszaru bezpiecznego. Dostęp do obszarów jest systematycznie kontrolowany przez ABI oraz ASI (A10.1.1*).

4. Dostęp do danych posiadają tylko upoważnione osoby, odpowiednio przeszkolone w zakresie ochrony i zasad udostępniania danych.

5. W pomieszczeniach, do których mają wstęp osoby nieupoważnione, monitory ustawione są w ten sposób, aby osoby te nie widziały zapisów na ekranie. W przypadkach, w których ustawienie monitora umożliwia wgląd do danych, stosuje się filtry ochronne, które zapewniają oglądanie danych tylko przez osobę obsługującą komputer.

6. Osoby mające dostęp do danych zawartych w wydrukach komputerowych zobowiązane są do zabezpieczenia ich przed dostępem osób nieuprawnionych, zagubieniem i zniszczeniem. Dokumenty przeznaczone do likwidacji powinny zostać zniszczone w przeznaczonych do tego celu urządzeniach lub odpowiednio zanonimizowane (trwale pozbawione danych osobowych). ASU określa kto i jakie wydruki ma prawo generować.

§ 6. Wprowadza się zabezpieczenie magnetycznych nośników danych (A 8.3 *):

1) rejestracja generowanych i zapisywanych magnetycznych nośników danych oraz zasad ich niszczenia,

2) nośniki magnetyczne zawierających dane osobowe przekazywane na zewnątrz są pozbawione zapisów Niszczenie poprzednich zapisów odbywa się przez formatowanie lub inicjowanie nośnika,

3) należy zastosować szyfrowanie danych w celu uniemożliwienia odczytu nośnika przez osoby nie znające zastosowanej zasady szyfrowania w przypadku konieczności przekazania nośnika z danymi,

4) sprawdzenie poprawności przygotowania nośnika magnetycznego wykonuje ASU,

5) nośniki magnetyczne przeznaczone do likwidacji lub uszkodzone należy dodatkowo po usunięciu z nich danych - fizycznie zniszczyć.

§ 7. Wprowadza się zabezpieczenia organizacyjne i techniczne:

1) dostęp do systemów informatycznych i danych w nich zawartych otrzymują wyłącznie pracownicy wyznaczeni przez AD, na pisemny wniosek kierownika, w której zatrudniony jest pracownik. ABI prowadzi rejestr tych pracowników obejmujący listę nazw użytkowników (nazwisko, imię, identyfikator) w systemie, daty założenia lub wycofania aktywności konta,

2) użytkownik rozpoczyna pracę w systemie po jego uwierzytelnieniu tzn. po wprowadzeniu przyznanego mu identyfikatora oraz własnego hasła. Użytkownik ma obowiązek zmieniać hasło zgodnie z obowiązującymi w Instrukcji zasadami,

3) wszystkie systemy, programy i dane przechowywane na serwerach są archiwizowane,

4) prowadzenie bieżącej profilaktyki antywirusowej polegającej na stałym „śledzeniu" programów i zbiorów użytkowanych w sieci komputerowej,

5) zobowiązanie użytkowników do nie instalowania własnych programów na komputerach Urzędu,

6) w celu ochrony prawidłowej pracy urządzeń komputerowych, w razie awarii zasilania, wszystkie urządzenia systemu informatycznego Urzędu, np.: komputery, drukarki, urządzenia aktywne zasilane są w energię elektryczną ze specjalnej sieci, która jest wyposażona w urządzenia podtrzymujące napięcie (UPS). Użytkownicy komputerów zobowiązani są do wykorzystywania wydzielonej sieci energetycznej tylko dla urządzeń komputerowych przydzielonych im do obsługi.

§ 8. Wprowadza się zabezpieczenia programowe:

zabezpieczenia programowe realizowane są poprzez identyfikację użytkownika (wprowadzanie identyfikatora i hasła) oraz autoryzację - polegającą na przyznaniu każdemu użytkownikowi określonych praw w systemie,

prawa użytkownika wynikają z wniosku jego kierownika oraz decyzji kierownika odpowiedzialnego za system i są nadawane użytkownikowi przez:

a) ASU lub osobę przez niego upoważnioną w zakresie dostępu do zasobów,

b) ASI w zakresie przydziału uprawnień do poszczególnych części lub funkcji systemu.

§ 9. Wprowadza się monitorowanie zabezpieczeń (A 12.4*):

1) do monitorowania systemu zabezpieczeń, stosownie do swojego zakresu czynności zobligowani są:

   a) Administrator Bezpieczeństwa Informacji,

   b) Administratorzy Systemów Użytkowych,

   c) Administratorzy Systemów Informatycznych,

   d) osoby odpowiedzialne za wykonywanie i testowanie jakości kopii archiwalnych.

2) w ramach monitoringu należy przeprowadzić następujące działania:

a) bieżącą kontrolę pracy w sieci i systemach komputerowych,

b) analizowanie wszelkich informacji o nieprawidłowej pracy urządzeń,

c) okresowe - zgodnie z instrukcją sprawdzenie kopii bezpieczeństwa pod względem ich przydatności do odtworzenia danych,

d) kontrolę ewidencji nośników magnetycznych z danymi archiwalnymi,

e) sprawdzanie częstotliwości zmiany haseł,

f) przeprowadzanie symulowanych włamań.

§ 10. 1. Zasady postępowania w sytuacji naruszenia ochrony danych osobowych określono w Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie - stanowiącej **Załącznik nr 15** do zarządzenia - określającej tryb postępowania w przypadku, gdy:

1) stwierdzono naruszenie zabezpieczeń systemu informatycznego,

2) istnieje podejrzenie naruszenia zabezpieczeń systemu informatycznego.

2. Instrukcja postępowania o której mowa w ust. 1 określa zasady postępowania wszystkich osób, które po stwierdzeniu naruszenia zabezpieczeń systemu informatycznego lub uzyskaniu informacji na ten temat niezwłocznie zobowiązane są zawiadomić o tym ABI, ASI, ASU lub osoby ich zastępujące, Referat Wsparcia WInf, a w przypadku braku kontaktu: bezpośredniego przełożonego, następnie Służbę Ochrony Mienia, Sekretarza Miasta, Zastępców Prezydenta Miasta oraz Prezydenta Miasta.

§ 11. 1. Wprowadza się w Urzędzie następujące rodzaje i zasady szkoleń: (A.7.2.2*)

1) szkolenia podstawowe dotyczące bezpieczeństwa danych prowadzone dla wszystkich pracowników Urzędu mających dostęp do danych osobowych niezależnie od formy zatrudnienia oraz stażystów i praktykantów,

2) system szkoleń szczegółowych dla pracowników skierowanych do odbycia szkoleń w ramach służby przygotowawczej w Urzędzie.

3) system szkoleń ponownych/aktualizujących dla osób wymienionych w pkt 1) w przypadku istotnych zmian w przepisach prawa lub regulacjach wewnętrznych (np. wprowadzenie nowej PBI)

2. Tematyka szkoleń obejmuje:

1) zaznajomienie pracowników z PBI i IZSI,

2) wymogi, jakie stawia osobom upoważnionym do przetwarzania danych osobowych ustawa i rozporządzenia wykonawcze do ustawy,

3) wymogi, jakie stawia pracownikom rozporządzenie KRI

4) obowiązki pracowników upoważnionych do przetwarzania danych osobowych,

5) obowiązki i wymagania jakie dla pracowników wynikają z Instrukcji postępowania,

6) sposoby realizacji zasady czystego biurka i ekranu,

7) odpowiedzialność osób w związku z przetwarzaniem danych osobowych,

8) zagrożeń bezpieczeństwa.

3. Szkolenie pracowników podmiotów zewnętrznych obsługujących Urząd, np.: pracownicy ochrony, obsługi remontowej, gospodarczej oraz sprzątania zapewniają firmy, które w ramach umów kierują pracowników do pracy na terenie Urzędu. Wymóg przeszkolenia osób zawarty jest w warunkach przetargowych określanych przez Biuro Obsługi Urzędu i MJOG.

4. Ponownemu szkoleniu podlega osoba, która mając ciągłość zatrudnienia miała przerwę w pracy w Urzędzie ponad 2 lata.

5. Ponownemu szkoleniu podlegają wszyscy zatrudnieni pracownicy Urzędu w przypadku istotnych zmian w SZBI, w szczególności wynikających z ustaw lub rozporządzeń.

6. Za realizację szkoleń w Urzędzie odpowiedzialni są:

1) Wydział Organizacyjny Urzędu w ramach służby przygotowawczej.

2) ABI dla nowoprzyjętych pracowników Urzędu oraz szkoleń ponownych w zakresie ochrony danych osobowych, podstawowych funkcji niektórych systemów ze szczególnym uwzględnieniem bezpieczeństwa teleinformatycznego.

3) WInf w zakresie obsługi systemów użytkowych (m.in. ZSFK, systemu obiegu dokumentów Rejestr BOI) i portali.

§ 12. Do obsługi programu komputerowego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, użytkownik może być dopuszczony jeżeli posiada pisemne upoważnienie wydane przez AD lub upoważnioną przez niego osobę. (A.9.1.2*)

§ 13. Użytkownik ma obowiązek zmieniać hasło minimum 8 znakowe z częstotliwością nie mniejszą niż 30 dni, hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. (A.9.4.2*)

§ 14. Bezpośredni dostęp do danych użytkownik ma dopiero po wprowadzeniu identyfikatora i właściwego hasła. Użytkownik nie może udostępniać identyfikatora, hasła i stanowiska roboczego osobom nieuprawnionym. (A.9.3.1*)

§ 15. Użytkownik ma obowiązek zamykania systemu, programu po zakończeniu pracy. Stanowisko komputerowe z uruchomionym systemem, programem nie może pozostawać bez kontroli pracującego na nim użytkownika.

§ 16. Użytkownik ma obowiązek używania wygaszacza (systemu Windows, programu użytkowego) lub zablokowania stacji roboczej w przypadku przerwy w obsługiwaniu komputera dłuższej niż 10 minut.

§ 17. Osoby dopuszczone do obsługi programu komputerowego zobowiązane są do zachowania tajemnicy w zakresie zasad dostępu do danych i ich merytorycznej treści, również po ustaniu zatrudnienia.

§ 18. 1. Wszelkie wydruki zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, zaś po upływie czasu ich przydatności powinny być niszczone w niszczarce.

2. Zawartość pojemników niszczarek należy umieścić w przeznaczonym do tego worku na makulaturę ciętą i przekazać pracownikowi wyznaczonemu przez MJOG.

3. Zabrania się umieszczania makulatury z niszczarek w koszu na śmieci.

§ 19. Zabrania się użytkownikowi:

1) udostępniania stanowisk roboczych oraz dostępnych na nich danych (w postaci pisemnej jak i elektronicznej) osobom nieupoważnionym,

2) wykorzystywania sieci komputerowej w celach innych niż wyznaczone przez Administratora,

3) samowolnego instalowania i używania programów komputerowych (posiadających lub nie posiadających licencji (A.12.6.2),

4) trwałego lub czasowego kopiowania programów komputerowych w całości lub w części jakimkolwiek środkami i w jakiejkolwiek formie,

5) publicznego rozpowszechniania, programów komputerowych lub ich kopii dla osób nieuprawnionych,

6) przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko,

7) tłumaczenia, przystosowywania, zmiany układu lub jakichkolwiek innych zmian w programie komputerowym,

8) używania oprogramowania, które posiada sfałszowane znaki firmowe lub nie posiada w ogóle znaków firmowych, etykiet, oryginalnych nośników, dokumentacji łącznie z elektroniczną,

9) udostępniania osobom nieuprawnionym programów komputerowych przez możliwość dostępu do zasobów sieci wewnętrznej lub Internetu,

10) wykorzystywania oprogramowania lub materiałów ściągniętych z Internetu do masowego rozprowadzania bez licencji lub wyraźnego upoważnienia autora,

11) używania nośników udostępnianych przez osoby nieuprawnione nośników danych (FDD, HDD, CDR, DVD, USB-drive),

12) używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna.

§ 20. Użytkownik ma obowiązek powiadamiać osoby określone w Instrukcji postępowania (ASI, ASU, ABI) o sytuacjach nadzwyczajnych, wszelkiego rodzaju różnicach w funkcjonowaniu programu lub systemu.

§ 21. Użytkownicy systemu, programu są niezwłocznie rejestrowani i wyrejestrowani przez ASI lub ASU gdy uzyskują lub tracą prawo do dostępu do systemu, programu, a identyfikator po wyrejestrowaniu użytkownika nie może być przydzielany innej osobie. (A.9.2.1*)

§ 22. ABI prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych (odnotowywane jest imię i nazwisko użytkownika, identyfikator, data wprowadzenia, pierwsze hasło oraz data wyrejestrowania).

§ 23. Kopie awaryjne są tworzone i przechowywane zgodnie z zasadami określonymi w Procedurze tworzenia i przechowywania kopii bezpieczeństwa. (A.12.3.1*) stanowiącej **Załącznik nr 17** do Zarządzenia

§ 24. Przeglądy i konserwacja systemów i zbiorów danych przeprowadzane są co miesiąc przez uprawnione do tego osoby pod nadzorem osoby upoważnionej przez Administratora. (A.15.2.1*).

§ 25. Urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe przed ich przekazaniem podmiotowi zewnętrznemu należy pozbawić zawartości, w przypadku likwidacji uszkodzić w sposób uniemożliwiający odczytanie danych; naprawę wymienionych urządzeń zawierających dane osobowe, o ile danych nie można usunąć, czynności powyższe należy wykonywać pod nadzorem osoby upoważnionej przez AD.

§ 26. 1. Dane osobowe udostępniać może wyłącznie AD lub osoby przez niego upoważnione.

2. Dane osobowe można udostępniać wyłącznie osobom lub podmiotom uprawnionym do ich otrzymywania na podstawie przepisów prawa na pisemny wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.

3. Wszystkie wydawane wydruki i nośniki z danymi są ewidencjonowane przez osobę wyznaczoną przez AD.

§ 27. Używanie nielegalnych programów komputerowych bez zezwolenia właściciela praw autorskich jest zabronione i podlega sankcjom wynikającym z ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r. Nr 90, poz. 631 ze zm.) oraz Regulaminu Pracy Urzędu, a odpowiedzialność ponoszą zarówno pracownik korzystający z nielegalnego oprogramowania, jak i jego kierownik.

§ 28. Przetwarzanie i udostępnianie danych osobowych przez osoby nieuprawnione oraz modyfikacja, uszkodzenie lub zniszczenie danych podlega sankcjom wynikającym z ustawy oraz Regulaminu Pracy Urzędu - także wtedy, gdy sprawca działał nieumyślnie.

§ 29. Zasady korzystania z poczty elektronicznej (A.13.2.3*)

1. Nadzór i opiekę techniczną nad systemem poczty elektronicznej sprawuje WInf. Użytkownik zobowiązany jest do sprawdzania własnej skrzynki poczty elektronicznej.

2. ASI wdraża odpowiednie systemy programowo – sprzętowe zapewniające ochronę poczty elektronicznej przed atakami spamu, poczty z niebezpiecznymi załącznikami (wirusy, oprogramowanie wyłudzające informacje, itp.). Użytkownik zobowiązany jest do sprawdzania codziennych raportów z urządzenia filtrującego i w razie konieczności wyciągania z nich źle sklasyfikowanej poczty elektronicznej, na którą oczekiwał (A.12.1*).

3. Na pisemny wniosek istnieje możliwość utworzenia innego adresu, niż standardowa struktura. We wniosku wskazuje się osobę odpowiedzialną za użytkowanie skrzynki poczty elektronicznej.

4. Poczta elektroniczna może być wykorzystywana tylko do celów służbowych.

5. Zabrania się rozsyłania m.in.:

1) ogłoszeń na inne konto wewnętrzne niż specjalny, dedykowany adres „Ogłoszenia" – dedykowany wymianie informacji pomiędzy pracownikami jednostki,

2) tzw. łańcuszków szczęścia (listów, które wykorzystując elementy socjotechniki generują niepożądany ruch na serwerach poczty elektronicznej),

treści wulgarnych,

materiałów erotycznych,

treści niezgodnych z obowiązującymi przepisami prawa,

treści prawem chronionych bez odpowiedniego zabezpieczenia np. szyfrowanie.

6. Korespondencja, którą przechowuje i dostarcza system pocztowy jest własnością Urzędu.

7. Urząd w celach dowodowych oraz bezpieczeństwa systemów ma prawo do kontroli skrzynek pocztowych użytkowników. O wynikach kontroli informuje się użytkownika.

8. Nie zaleca się logowania do systemów poczty elektronicznej z komputerów dostępnych publicznie (np. kafejki internetowe).

9. Skrzynki pocztowe posiadają ograniczoną wielkość. Użytkownik zobowiązany jest do okresowej archiwizacji wiadomości.

§ 30. 1. Użytkownicy mogą korzystać z dostępu do Internetu tylko w celach służbowych. (A.13.2.1*)

2. Praca w sieci Internet nie może zagrażać bezpieczeństwu systemów informatycznych.

3. ASI może wprowadzić kategoryzację stron internetowych, oraz zablokować dostęp do wybranych kategorii.

4. Odblokowanie witryny internetowej może nastąpić na pisemny wniosek Kierownika.

5. Zabrania się:

1) wykorzystywania sieci Internet w sposób, który mógłby narazić Urząd na przerwanie ciągłości działania systemu, blokadę, zakłócenia oraz utratę dobrego imienia,

2) pobierania oprogramowania (w tym w wersjach darmowych), nie związanego z wykonywanymi obowiązkami służbowymi,

3) udostępniania łącza internetowego dostarczonego przez Urząd innym osobom bez zgody ASI,

4) instalowania urządzeń udostępniających Internet na sprzęcie Urzędu bez zgody ASI.

§ 31. 1. Każdorazowo po przeprowadzeniu testowego odtwarzania po awarii należy sporządzić krótki raport zawierający informację o napotkanych błędach i przybliżonym czasie odtwarzania. (A.17.1.2*)

2. Raporty należy przechowywać wraz z dokumentacją systemu. Testowanie odtwarzania awaryjnego musi odbywać się minimum raz na pół roku.

3. Po wykonaniu rocznego przeglądu i konserwacji systemu należy sporządzić raport, który będzie zawierał spis wykonanych czynności oraz osoby je wykonujące.

4. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane systemu przed oddaniem do serwisu muszą być skasowane przez nadpisanie całości nośnika losowymi danymi.

5. Zasady stosowania pamięci komputerowych i pomocniczych w Urzędzie ze wskazaniem poziomu ich bezpieczeństwa określono w **Załączniku nr 10** do Zarządzenia.

6. Niszczenie dysków twardych stacji roboczych i serwerów wykonywane jest w urządzeniu demagnetyzującym. Dyski po wykonaniu tego działania nie nadają już się do ponownego użycia.

7. Osoby wykonujące niszczenie dysków zobowiązane są sporządzić protokół zniszczenia.

8. Zezwala się na wykonywanie naprawy urządzenia przechowującego dane systemu operacyjnego bez kasowania danych tylko i wyłącznie pod warunkiem wykonania naprawy w obecności pracownika WInf odpowiedzialnego za system.

§ 32. 1. Aktualizowanie systemu odbywa się zgodnie z typem zmiany (A.12.1.2*).

2. Jeżeli instalowana poprawka niesie za sobą zagrożenie w postaci możliwości obniżenia bezpieczeństwa systemu teleinformatycznego Urzędu, poddaje się ją testom w środowisku testowym.

3. Systemy informatyczne Urzędu wykorzystują serwery świadczące usługi przesyłania poprawek.

§ 33. Metody i środki uwierzytelniania (A.9.2*)

1. Hasło pierwszego logowania użytkownika do systemu informatycznego w Urzędzie jest przekazywane w zamkniętych kopertach lub w inny sposób zapewniający poufność dostarczenia informacji.

2. Hasła pierwszego logowania dla wszystkich użytkowników nie mogą się powtarzać.

O ile system nie wymusza zmiany haseł podczas pierwszego logowania użytkownik zobowiązany jest do jego samodzielnej zmiany podczas kolejnego logowania się do systemu.

3. Hasła kont administracyjnych (np. root, administrator) systemu, przechowywane są w sejfie w zamkniętych kopertach w sposób uniemożliwiający dostęp do nich osób nieuprawnionych.

4. Dostęp do hasła administratora systemu użytkowego posiada ASU - osoba odpowiedzialna za system oraz jej kierownik.

5. O użyciu zdeponowanego hasła administracyjnego należy poinformować ASI.

§ 34. Zabezpieczenie systemu informatycznego przed szkodliwym oprogramowaniem oraz awarią zasilania (A.12.2, A.9.4*)

1. Do systemu szkodliwe oprogramowanie może dostać się z następujących źródeł:

1) sieci publicznej (nieautoryzowana poczta, spam, spreparowane strony internetowe),

2) ataków sieciowych (aktywne próby penetrowania systemu Urzędu),

3) niezgodnego z zasadami IZSI działania użytkowników.

2. Użytkownik powinien być poinformowany o postępowaniu w przypadku wykrycia szkodliwego oprogramowania.

3. W przypadku wykrycia zdarzenia/incydentu związanego z bezpieczeństwem informacji należy postępować zgodnie zasadami IPNBI.

§ 35. Sposób rejestracji udostępniania informacji rejestrowanych w systemie (A.9.2 – A.9.4*)

1. ASU prowadzi rejestr udostępnionych informacji w systemie informatycznym. Rejestr udostępnień prowadzony jest przypadku danych z ewidencji ludności w module Ewid systemu Mieszkańcy, a dla pozostałych ewidencji w informatycznym systemie obiegu dokumentów Rejestr BOI.

2. Systemy informatyczne Urzędu zapewniają odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu,

2) identyfikatora użytkownika wprowadzającego informację, w tym dane osobowe do systemu,

3) źródła danych, w przypadku zbierania danych, nie od osoby której one dotyczą,

4) informacji o odbiorcach, którym informacja, w tym dane osobowe zostały udostępnione w tym dacie i zakresie tego udostępnienia,

5) sprzeciwu wobec przetwarzania informacji, w tym danych osobowych, w przypadku gdyby Urząd zamierzał przetwarzać dane w celach innych niż zakres ustawowych i statutowych uprawnień lub wobec przekazywania danych osobowych innemu administratorowi.

3. Wzór „Raportu z udostępnionych informacji, w tym danych osobowych, ważnych z punktu widzenia bezpieczeństwa informacji", stanowi złącznik nr 12 do niniejszej IZSI.

§ 36. Realizacja nadzoru nad połączeniem z siecią publiczną (A.12 – A.13*)

1. ASI jest zobowiązany do przestrzegania i aktualizacji niniejszej IZSI oraz połączeń z siecią publiczną systemu Urzędu w zakresie m.in.:

1) szczegółowego opisu realizacji połączenia z siecią Internet,

2) opisu kontroli przepływu informacji pomiędzy systemem informatycznym Urzędu przetwarzającym dane, a siecią publiczną,

3) opisu kontroli działań inicjowanych z sieci publicznej i systemu informatycznego,

4) sposobu zbierania i archiwizacji logów opisujących komunikację systemu informatycznego Urzędu z siecią Internet,

5) sposobu detekcji włamań do systemu informatycznego Urzędu.

§ 37. 1. Zakazuje się przechowywania na komputerowych stanowiskach pracy i sieciowych pamięciach masowych jakichkolwiek plików o charakterze prywatnym, niezwiązanych z obowiązkami służbowymi pracownika określonymi w opisie stanowiska pracy.

2. Powyższy zakaz obejmuje wszystkie dzieła, utwory i programy komputerowe, do których Urząd Miasta Szczecin nie posiada praw autorskich z określonymi polami eksploatacji lub odpowiedniej licencji.

3. Zakazuje się instalowania na stanowiskach komputerowych oprogramowania, które nie spełnia jednego z warunków, zwanych warunkami legalności:

1) jest licencjonowane dla Urzędu Miasta Szczecin;

2) zostało przekazane dla Urzędu przez inny podmiot z zastosowaniem cesji;

3) zostało określone, przez jego wytwórcę lub właściciela praw autorskich, jako wolne lub publicznie dostępne, w szczególności darmowe, bez opłat licencyjnych i zostało dopuszczone do użytkowania w Urzędzie.

4. Warunki, określone w ust.3 pkt 1) i 2) potwierdza się za pomocą dokumentów licencyjnych, mechanizmów przewidzianych przez producenta, jak specjalne naklejki lub umów z postanowieniami licencyjnymi dotyczącymi zakupu lub przekazania oprogramowania ze wskazanymi polami eksploatacji.

5. Dla oprogramowania określonego w ust. 3. pkt 3 określa się procedurę akceptacyjną dopuszczającą oprogramowanie rozprowadzane na zasadach darmowych (bez opłat licencyjnych, przykładowo shareware lub freeware), o ile w sposób udokumentowany nie zabraniają tego warunki jego używania. Oprogramowanie takie może być instalowane i wykorzystywane jedynie po wypełnieniu następujących warunków określonych, jako procedura akceptacyjna:

1) analizie prawnej postanowień licencyjnych przeprowadzonej przez Koordynatora Radców Prawnych Urzędu;

2) zgłoszeniu zapotrzebowania na program do WInf i uzyskaniu akceptacji ASI, który dopuszcza program do użytkowania w Urzędzie. Rejestr programów rozprowadzanych na zasadach darmowych i dopuszczonych do użytkowania w Urzędzie prowadzony jest przez WInf i udostępniany w Intranecie.

6. Użytkownik nie może dokonywać zmian konfiguracyjnych systemu operacyjnego ani instalować jakiegokolwiek oprogramowania.

7. Użytkownik, na podstawie pisemnego zgłoszenia potwierdzonego przez kierownika/dyrektora merytorycznego, może uzyskać pełne uprawnienia administracyjne na swoim komputerze. Zgody udziela Dyrektor WInf. Rozszerzenie uprawnień dotyczy możliwości samodzielnej instalacji oprogramowania, które spełnia warunki legalności określone powyżej. ASI prowadzi rejestr użytkowników o pełnych uprawnieniach administracyjnych.

8. Szczegółowe uregulowania dotyczące uprawnień dostępu określa **Załącznik Nr 6** do Zarządzenia.

9. Wykrycie czy odnotowanie na stanowisku komputerowym plików oraz oprogramowania, które nie spełnia warunków określonych, w ust. 3 podlega procedurze usunięcia wraz z danymi, z którymi jest bezpośrednio powiązane i które agreguje. Zdarzenie to należy opisać w notatce służbowej i przekazać informację do Sekretarza Miasta oraz ABI. Powyższe procedury realizuje WInf.

10. Dyrektor WInf, ABI oraz ASI działając wspólnie lub niezależnie są uprawnieni do przeprowadzania kontroli przestrzegania postanowień Zarządzenia na wszystkich komputerowych stanowiskach pracy Urzędu. W przypadku stwierdzenia nieprawidłowości podejmują działania w celu przywrócenia stanu zgodności z zarządzeniem oraz przygotowują notatkę służbową dla Sekretarza Miasta.

§ 38. 1. Ochrona przed szkodliwym oprogramowaniem dotyczy wszystkich zasobów teleinformatycznych (niezależnie od faktu przetwarzania danych osobowych).

2. Ochrona przed wirusami i innymi szkodliwym oprogramowaniem jest obowiązkowa i jest realizowana przez system ochrony antywirusowej, którym administruje WInf.

3. Ochrona dotyczy wszystkich komputerów (serwery i stacje robocze) oraz danych przetwarzanych w systemach informatycznych.

4. Niedopuszczalne jest eksploatowanie komputerowych stanowisk pracy (stacji roboczej) bez uruchomionego systemu antywirusowego lub jego samowolne wyłączanie czy ograniczanie jego funkcjonalności.

5. Każdy zewnętrzny nośnik danych, z którego informacja ma być wprowadzona do komputerowego stanowiska pracy musi najpierw zostać sprawdzony przez systemem ochrony antywirusowej. W przypadkach wątpliwych użytkownik zobowiązany jest przekazać nośnik do sprawdzenia w serwisie WInf.

6. Wszystkie stacje robocze są cyklicznie, przynajmniej 1 raz w tygodniu sprawdzane systemem ochrony antywirusowej, gdzie automatyczne procedury, analizy i raportowanie realizuje WInf.

7. Aktualna wersja systemu ochrony antywirusowej jest dystrybuowana automatycznie poprzez sieć LAN Urzędu. W przypadkach indywidualnych dystrybucja odbywa się poprzez sieć publiczną i przy pomocy, którą należy uzyskać poprzez HelpDesk.

8. Hasłami dostępu do warstwy systemów operacyjnych stacji roboczych, serwerów i aktywnych urządzeń sieciowych administruje WInf. Hasła te stosuje się obowiązkowo. Parametry haseł na serwerach są ustalane przez Dyrektora WInf a wszystkie informacje dotyczące haseł do serwerów i urządzeń sieciowych przechowywane są w sposób bezpieczny w WInf, pod nadzorem ABSI.

§ 39. 1. Obowiązkowe jest wykonywanie kopii zapasowej danych i systemów teleinformatycznych:

1) codziennej - danych systemów wielodostępnych kluczowych dla funkcjonowania Urzędu;

2) okresowej - danych systemów autonomicznych, eksploatowanych samodzielnie w jednostkach Urzędu. Kierownicy określają czas przechowywania danych oraz odpowiedzialnych pracowników za wykonywanie kopii;

3) codziennej - zasobów sieciowych udzielonych dla poszczególnych stanowisk pracy.

2. Kierownicy jednostek Urzędu są odpowiedzialni za kopie zapasowe danych systemów teleinformatycznych, które posiadają lub, które eksploatują.

3. Systemy autonomiczne, których terminale eksploatowane są w Urzędzie podlegają procedurom zabezpieczającym dane określonym przez ich właścicieli.

4. Użytkownicy komputerowych stanowisk pracy w celu zabezpieczenia się przed skutkami utracenia informacji z dysków lokalnych obowiązani są sporządzać kopie danych na udostępnionych im zasobach sieciowych, gdzie obowiązek cyklicznej kopii zapasowej realizuje WInf.

5. Nośniki informatyczne wykorzystywane jednorazowo należy opatrywać identyfikatorem zawierającym datę sporządzenia, zawartość, identyfikator pracownika wykonującego kopię zapasową. W przypadku wielokrotnego wykorzystywania nośnika informacje te umieszcza się w odpowiednim spisie.

6. Nośniki z kopiami zapasowymi systemów informatycznych oraz inne elektroniczne nośniki informacji zawierające dane osobowe powinny być przechowywane w pomieszczeniach niedostępnych dla osób trzecich z zastosowaniem szaf metalowych, zamykanych na klucz i poza serwerownią, w której znajdują się urządzenia przetwarzające te dane.

§ 40. Przypadki stwierdzenia naruszenia bezpieczeństwa danych osobowych polegają na:

1) uszkodzeniu lub niewłaściwym stanie danych osobowych przechowywanych w postaci fizycznej, dotyczy przykładowo segregatorów, kartotek czy archiwów;

2) nieprawidłowym działaniu systemu informatycznego przetwarzającego dane osobowe;

3) stwierdzeniu nowego, nieznanego faktu przetwarzania danych osobowych;

4) zmienionej zawartości zbiorów danych osobowych;

5) zmienionym obiegu dokumentów lub przebiegu procesów pracy mogących powodować nieuprawniony dostęp do danych osobowych.

2. W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych należy bezzwłocznie:

1) powiadomić bezpośredniego przełożonego oraz ABI;

2) podjąć działania minimalizujące powstałe zagrożenia.

3. Przełożony pracownika lub ABI przejmują nadzór nad stanowiskiem pracy, na którym stwierdzono naruszenie bezpieczeństwa danych osobowych. Równolegle kierownik pracownika decyduje o odsunięciu pracownika od pracy na stanowisku, na którym stwierdzono naruszenie.

4. ABI lub upoważniony przez niego pracownik zobowiązany jest do sporządzenia pisemnego raportu dotyczącego naruszenia bezpieczeństwa danych osobowych w zakresie, co najmniej:

1) czasu i miejsca wystąpienia naruszenia;

2) zbadania przyczyn, okoliczności i rozmiaru naruszenia bezpieczeństwa danych osobowych;

3) określenia osób, które mogły naruszyć bezpieczeństwo danych osobowych;

4) określenia osób odpowiedzialnych za naruszenie danych osobowych;

5) zabezpieczenia dowodów umożliwiających ustalenie przyczyn, skutków czy sprawcy naruszenia ochrony danych;

6) zakresu ujawnionych lub zmienionych danych.

5. Powyżej określony raport definiuje się, jako incydent naruszenia bezpieczeństwa danych osobowych. ABI przekazuje go AD, Sekretarzowi Miasta i kierownikowi jednostki, w której wystąpił incydent.

6. Po przeprowadzeniu uzgodnień z Sekretarzem Miasta i kierownikiem jednostki, w której wystąpił incydent - ABI obowiązany jest przedstawić projekt działań naprawczych w celu eliminowania podobnych zdarzeń w przyszłości.

7. Za naruszenie ochrony danych osobowych stosuje się kary przewidziane przepisami ustawy. Niezależnie od tego AD może stosować kary wynikające z Kodeksu Pracy.

8. Wszelkie fakty dotyczące innych zdarzeń czy podejrzeń naruszenia bezpieczeństwa systemów teleinformatycznych powinny być zgłaszane do WInf poprzez funkcję Pomoc zdalna – zgłoszenie dostępną na stacji roboczej użytkownika lub do ASI w formie notatki pocztą elektroniczną.

§ 40. 1. Przeglądy i konserwacje systemów teleinformatycznych oraz zbiorów danych muszą być wykonywane w obecności pracownika WInf - Administratora systemu, natomiast zbiory danych osobowych dodatkowo za pisemnym upoważnieniem ABI lub ASI.

2. Administratorzy Systemów, w ramach swoich obowiązków są zobowiązani do prowadzenia bieżącej obserwacji, administracji, konserwacji i raportowania systemów, którymi zarządzają.

3. Mechanizmy zasilania rezerwowego podlegają okresowym procedurom potwierdzającym stałą gotowość do pracy.

4. Do zasilania komputerów i urządzeń peryferyjnych należy obowiązkowo stosować podłączenia do gniazd wydzielonej sieci elektrycznej, przeznaczonych wyłącznie do zasilania sprzętu komputerowego.

5. Zakazuje się podłączania innych urządzeń (w szczególności czajników, wentylatorów czy grzejników) do gniazd wydzielonej sieci elektrycznej zasilającej sprzęt komputerowy.

*) Zgodnie z PN ISO/IEC 27001:2014-12