Załącznik nr 2 do Zarządzenia Nr 0050.199.2021 Burmistrza Bystrzycy Kłodzkiej z dnia 25 czerwca 2021 r. w sprawie wprowadzenia Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIASTA I GMINY BYSTRZYCA KŁODZKA

Spis treści

ROZDZIAŁ I – INFORMACJE OGÓLNE

§ 1

Na podstawie:

1. Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. 2019 poz.1781t.j.);
2. 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. 2016 z roku, poz. 113 ze zm.);
3. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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 119 z 4 maja 2016 r., Polskie Wydanie Specjalne 2016 t.59);

ustanawia się **Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka.**

§ 2

Przez użyte w niniejszym dokumencie określenia należy rozumieć:

1. **IOD** – Inspektor Ochrony Danych;
2. **ASI** – Administrator Systemów Informatycznych;
3. **ADO** – Administrator Danych Osobowych;
4. **Baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;
5. **Urząd** – Urząd Miasta i Gminy Bystrzyca Kłodzka;
6. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
7. **Identyfikator Użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika);
8. **Instrukcja** – niniejszy dokument;
9. **Kopia pełna** – kopię zapasową całości danych osobowych przetwarzanych w systemie informatycznym;
10. **Niezgodność** – niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe;
11. **Nośniki danych** – płyty CD lub DVD, pamięć Flash, dyski twarde lub inne urządzenia/materiały służące do przechowywania plików z danymi;

12. **Polityka Bezpieczeństwa (PB)** – przyjęty do stosowania dokument o nazwie: Polityka Bezpieczeństwa Urzędu Miasta i Gminy Bystrzyca Kłodzka;
13. **Przetwarzane danych** – wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemie informatycznym;
14. **Raport** – przygotowane przez system informatyczny zestawienie zakresu i treści przetwarzanych danych;
15. **Rozporządzenie** – odpowiednio użyte w tekście rozporządzenie, o którym mowa w § 1 niniejszego rozdziału;
16. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
17. **Serwisant** – firma lub pracownik firmy zajmujący się instalacją, naprawą i konserwacją sprzętu komputerowego;
18. **Sieć publiczna** – sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;
19. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
20. **Użytkownik** – upoważniony przez ADO wyznaczony do przetwarzania danych osobowych pracownik, który odbył stosowne szkolenie w zakresie ochrony tych danych na wniosek bezpośredniego przełożonego;
21. **Ustawa** – odpowiednio użytą w tekście ustawę, o której mowa w § 1 niniejszego rozdziału;
22. **Zarządzenie** – aktualne Zarządzenie Burmistrza Bystrzycy Kłodzkiej w sprawie Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym w Urzędzie Miasta i Gminy Bystrzyca Kłodzka;
23. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
24. **Wydział** – komórka organizacyjna Urzędu.

§ 3

1. ASI wyznaczany jest przez ADO drogą pisemnego upoważnienia i polecenia przetwarzania danych. W przypadku niewyznaczenia ASI, jego funkcję pełni ADO.
2. ASI jest również zobowiązany do podpisania oświadczenia o zachowaniu poufności.
3. Podczas nieobecności ASI jego funkcję pełni upoważniony przez Burmistrza zastępca.

§ 4

1. Wszyscy Użytkownicy przetwarzający dane osobowe w systemie informatycznym stosowanym w Urzędzie Miasta i Gminy Bystrzyca Kłodzka są odpowiedzialni za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych.

2. Do obowiązków ASI należy kontrola przepływu informacji pomiędzy systemami informatycznymi a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej i systemu informatycznego.
3. ASI odpowiada za wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych, o którym mowa w § 20 KRI (Rozporządzenie 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).
4. Obowiązkiem ASI jest również zabezpieczenie użytkowanego sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.
5. Rolą IOD jest monitorowanie stanu prawnego i wsparcie ASI w zakresie spełnienia wymogów prawnych. IOD na żądanie ADO i ASI dokonuje oceny planowanych lub przyjętych środków pod kątem ich zgodności z przepisami prawa.

§ 5

Zgodnie z rozporządzeniem, uwzględniając fakt, że użytkowany w Urzędzie Miasta i Gminy Bystrzyca Kłodzka system informatyczny służący do przetwarzania danych osobowych jest połączony z siecią Internet, wprowadza się wysoki poziom bezpieczeństwa.

ROZDZIAŁ II – INFORMACJE SZCZEGÓŁOWE

§ 6

Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym stosowanym w Urzędzie określa się w sposób następujący:

1. Kierownicy komórek organizacyjnych Urzędu zostali upoważnieni i zobowiązani przez ADO do wnioskowania o nadawanie, zmianę oraz odwoływanie uprawnień. Wszelkie wnioski w tym zakresie winny być kierowane do ADO za pośrednictwem IOD. ADO może w każdym czasie nadawać, zmieniać oraz odwoływać upoważnienia do przetwarzania danych osobowych. W przypadku samodzielnych stanowisk o uprawnienia i ich zmianę oraz odwołanie wnioskuje bezpośredni przełożony. Po nadaniu upoważnienia IOD jest zobowiązany do przekazania zakresu upoważnienia Użytkownika do ASI. Ciężar obowiązku wnioskowania do ADO o nadawanie, zmianę oraz odwoływanie uprawnień leży wyłącznie po stronie bezpośrednich przełożonych.
2. ASI przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia do przetwarzania danych osobowych nadanego przez Administratora Danych Osobowych, określającego zakres uprawnień Użytkownika.
3. Po pozytywnym zweryfikowaniu upoważnienia, ASI zobowiązany jest niezwłocznie przydzielić Użytkownikowi identyfikator i hasło. Podanie użytkownikowi hasła nie może nastąpić w sposób umożliwiający zapoznanie się z nim osobom trzecim.

4. Użytkownikom nadawane są uprawnienia do prac tylko w modułach i funkcjach programu wymaganych dla realizacji powierzonych im zadań.
5. Użytkownik systemu informatycznego ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
6. W przypadku wygaśnięcia przesłanek uprawniających Użytkownika do przetwarzania danych osobowych, w szczególności odwołania upoważnienia do ich przetwarzania, ASI zobowiązany jest do dopełnienia czynności uniemożliwiających ponowne wykorzystanie identyfikatora użytkownika, którego uprawnienia wygasły. Kierownicy komórek organizacyjnych (bezpośredni przełożeni użytkownika) są zobligowani do odwoływania upoważnień, o czym pisemnie powiadamiają IOD i ASI. Obligatoryjnie w powiadomieniu należy wskazać datę ustania uprawnień.
7. Wyłączenie użytkownika z ewidencji osób upoważnionych do przetwarzania informacji obliguje ASI do zablokowania go we wszystkich systemach informatycznych, do których miał dostęp.
8. ASI dysponuje wykazem identyfikatorów przekazanych poszczególnym pracownikom, który wiąże identyfikator z imiennie wskazanym pracownikiem.
9. Hasło składa się z co najmniej 8 znaków (liter, cyfr i znaków specjalnych).
10. Osobą odpowiedzialną za przydział identyfikatora i pierwszego hasła jest ASI.
11. Użytkownik jest zobowiązany do zabezpieczenia swojego hasła przed nieuprawnionym dostępem osób trzecich.
12. W przypadku nieumyślnego ujawnienia hasła osobie nieuprawnionej lub podejrzenia ujawnienia, należy bezzwłocznie dokonać zmiany hasła na nowe.
13. Kolejne hasła zmienia sam użytkownik, chyba, że użytkowany system sam wymusza jego zmianę.
14. Identyfikatory dla użytkowników przydziela ASI. Identyfikator po wylogowaniu danej osoby z systemu, nie może być przydzielony innemu użytkownikowi.
15. Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu identyfikatora i hasła, którymi się posługuje lub posługiwał.

§ 7

1. Zarejestrowanie użytkownika w systemie wymaga spełnienia następujących warunków:
    a) zgłoszenie pisemne przez bezpośredniego przełożonego do IOD konieczności dostępu do przetwarzania danych osobowych w konkretnych zbiorach (zgodnie z zajmowanym stanowiskiem i zakresem obowiązków);
    b) podpisanie przez osobę, ubiegającą się o dostęp, oświadczenia dotyczącego zapoznania się z obowiązującymi przepisami o ochronie danych osobowych oraz z aktualnym Zarządzeniem Burmistrza Bystrzycy Kłodzkiej w sprawie wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka oraz zobowiązania do zachowania w tajemnicy informacji związanych z ich przetwarzaniem wydania przez Administratora (lub osobę upoważnioną).
    c) upoważnienia i polecenie dla użytkownika do dostępu i przetwarzania danych osobowych.

2. Z chwilą zarejestrowania w systemie użytkownik jest informowany przez ASI o ustalonym dla niego identyfikatorze i obowiązku posługiwania się hasłem dostępu.
3. Dokumenty, o których mowa w ust. 1 podlegają przechowaniu:
    a) oryginał oświadczenia osoby ubiegającej się o dostęp przechowuje się w aktach osobowych pracownika i w aktach IOD (w przypadku osoby niebędącej pracownikiem Urzędu – w dokumentach tej osoby, przechowywanych u pracownika odpowiedzialnego za kadry;
    b) upoważnienia do dostępu i przetwarzania danych przechowuje się w aktach osobowych pracownika (w przypadku osoby niebędącej pracownikiem Urzędu – w dokumentach tej osoby), przechowywanych u pracownika odpowiedzialnego za kadry (ASI i IOD jeśli uznają to za potrzebne, mogą dysponować kopiami dokumentów wskazanych w pkt 1 i 2.
4. W przypadku konieczności powierzenia przetwarzania danych osobowych innemu podmiotowi, Administrator zawiera z tym podmiotem umowę na piśmie.
5. Podmiot, z którym zawarta jest umowa może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie;
6. Umowa sporządzana jest w dwóch egzemplarzach: jeden dla podmiotu, drugi dla Administratora. Kierownicy Wydziałów zobowiązani są zgłaszać wszelkie umowy powierzenia do IOD, który prowadzi ich rejestr. Obowiązek zgłaszania dotyczy również samodzielnych stanowisk pracy.
7. Oświadczenie, o którym mowa w ust. 1 pkt 2 składają wszyscy pracownicy Urzędu oraz inne osoby, które mogą mieć dostęp do danych osobowych nawet, jeśli nie ubiegają się o upoważnienie do przetwarzania danych osobowych w Urzędzie. Za realizację obowiązku odpowiada Wydział Organizacyjno-Prawny.
8. Użytkownika wyrejestrowuje się z systemu na zgłoszenie przełożonego – po utracie uprawnień dostępu do przetwarzania danych, co może mieć miejsce w sytuacjach:
    a) ustania zatrudnienia użytkownika;
    b) zmiany zakresu obowiązków użytkownika;
    c) zakończeniu umowy - w przypadku osoby niebędącej pracownikiem Urzędu (np. praktykant, stażysta, umowa cywilnoprawna).
9. Rozwiązanie umowy o pracę lub zaistnienie okoliczności zawartych w ust. 8 pkt 2 i 3, powoduje utratę dostępu do przetwarzania danych i niezwłoczne wyrejestrowanie użytkownika z systemu, odnotowanie w ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka oraz unieważnienie jego hasła i identyfikatora. Przełożeni użytkowników zobowiązani są do poinformowania IOD i ASI w przypadku zaistnienia okoliczności, o których mowa w ust.8.
10. Uprawnienia administratora systemów w Urzędzie posiada ASI, a w przypadku jego nieobecności inna osoba upoważniona przez Administratora Danych.
11. Hasła administratora systemów przechowywane są w dokumentacji ASI, zachowując zasady określone w niniejszej instrukcji.
12. Awaryjne użycie haseł administratora systemów może być wykonane wyłącznie przez Administratora Danych lub inna osobę upoważnioną.
13. Z każdorazowego awaryjnego użycia haseł administratora sporządzana jest notatka.

§ 8

1. Czas trwania nieaktywnej sesji (czas bezczynności) po jakim następuje automatyczne wylogowanie Użytkownika wynosi maksymalnie 15 minut.
2. Uruchomienie wygaszacza ekranu wiąże się z koniecznością ponownego zalogowania, celem wznowienia pracy stacji roboczej.

ROZDZIAŁ III – KONFIGURACJA SPRZĘTU KOMPUTEROWEGO UŻYTKOWNIKA SYSTEMU

§ 9

1. Komputer Użytkownika powinien posiadać oprogramowanie antywirusowe, którego sygnatury wirusów powinny być aktualizowane na bieżąco. Oprogramowanie antywirusowe powinno być stale aktywne.
2. W przypadku niesprawdzenia przez użytkownika systemu pliku dostarczonego z zewnątrz, oprogramowanie antywirusowe automatycznie chroni system poprzez monitorowanie plików w stanie rzeczywistym. W przypadku wykrycia zagrożenia, oprogramowanie stosownie reaguje na to zagrożenie.
3. Użytkownik jest zobowiązany do stałego monitorowania komunikatów pochodzących z oprogramowania antywirusowego zainstalowanego na stacji roboczej i reagowania na nie.
4. Komputer Użytkownika powinien być chroniony zaporą sieciową (firewall).
5. Oprogramowanie komputera powinno być regularnie aktualizowane, w szczególności dotyczy to systemu operacyjnego.
6. Użytkownik nie może w sposób samodzielny tj. bez uzgodnienia z ASI instalować żadnych programów komputerowych na sprzęcie służbowym.
7. Wszelkie sprawy związane z oprogramowaniem na komputerze służbowym winne być zgłaszane Administratorowi Systemów Informatycznych.

ROZDZIAŁ IV – ROZPOCZYNANIE, ZAWIESZANIE I KOŃCZENIE PRACY

§ 10

1. Użytkownik rozpoczynający pracę zobowiązany jest przestrzegać procedur, które mają na celu sprawdzenie zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego, a w szczególności:
   a) przed wejściem do pomieszczenia sprawdzić czy na drzwiach i zamkach nie ma widocznych śladów prób niepowołanego ich otwierania;
   b) sprawdzić stan okien i krat (jeśli są w danym pomieszczeniu) oraz ocenić,
   c) czy w pomieszczeniu nie ma znaków wskazujących na pobyt w nim osób nieuprawnionych;
   d) sprawdzić stan sprzętu informatycznego oraz zamknięcie szaf i biurek.
2. Użytkownik przed przystąpieniem do przetwarzania danych powinien zalogować się w systemie, posługując się swoim identyfikatorem i hasłem. Po zalogowaniu się należy ocenić pracę systemu i stan przetwarzanych danych.
3. Użytkownik w czasie pracy powinien stosować zasady zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie:

a) ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwiać podgląd osób nieuprawnionych lub w przypadku niemożliwości zastosowanie filtra prywatyzującego;
b) dopilnować aby w pomieszczeniach, stanowiących obszar przetwarzania danych osobowych przebywały osoby trzecie, tylko za zgodą przełożonych i w obecności osób uprawnionych;
c) stosować urządzenia zabezpieczające przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci elektrycznej. Potrzeby w tym zakresie zgłaszają pisemnie do ASI – przełożeni Użytkownika;
d) jeżeli użytkownik komputera na stanowisku jest zalogowany do systemu i nie wykazuje aktywności przez okres dłuższy niż 15 minut, następuje jego blokada, odblokowanie jest możliwe po podaniu aktualnego hasła użytkownika
e) stosować tzw. wygaszacze ekranów, które włączają się po upływie 15 minut bezczynności komputera.

4. Po zakończeniu pracy użytkownik powinien przestrzegać następujących zasad:
   a) wylogować się z systemu i zaczekać na jego wyłączenie się;
   b) sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji;
   c) upewnić się, że szafy i biurka z dokumentacją są zamknięte;
   d) wyłączyć odbiorniki energii elektrycznej, zamknąć pomieszczenie i klucze oddać
   e) w wyznaczone miejsce, zgodnie z obowiązującą instrukcją postępowania z kluczami dostępu do pomieszczeń w Urzędzie;
   f) Po godzinach pracy Administrator lub osoba upoważniona przez niego zapewnia monitorowanie lub fizyczną ochronę pomieszczeń, w których przetwarzane są dane osobowe.
5. W przypadku stwierdzenia przez użytkownika prób niepowołanego naruszenia urządzeń, zawartość zbiorów danych, ujawnione metody pracy lub sposób działania programu mogą wskazywać na naruszenie danych osobowych – postępuje zgodnie z Procedurą postępowania w sytuacji podejrzenia naruszenia danych osobowych, zawartą w Polityce Bezpieczeństwa.
6. Rozpoczynając pracę użytkownik powinien zwrócić szczególną uwagę na okoliczności, o których mowa w ust. 1 i przypadku ich zaistnienia natychmiast informować IOD i przełożonego.

ROZDZIAŁ V – ZABEZPIECZANIE DANYCH W SYSTEMIE

§ 11

1. Dane osobowe przetwarzane w systemie informatycznym Urzędu Miasta i Gminy Bystrzyca Kłodzka podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.
2. Za tworzenie i przechowywanie kopii zapasowych w sposób zgodny z przepisami ustawy oraz niniejszej Instrukcji odpowiedzialny jest Administrator Systemów Informatycznych.
3. Stosuje się następujące procedury tworzenia oraz przechowywania kopii zapasowych baz danych:
   a) codziennie ASI wykonuje kopię przyrostową;
   b) raz tydzień ASI wykonuje kopię pełną;

c) system Acronis odpowiedzialny za wykonywanie kopii zapasowych kopii wirtualnych serwerów. Wykonywane są kopie zapasowe baz danych systemów informatycznych. Kopie zgrywane są na serwer oraz na urządzenie do wykonywania kopii Qnap znajdujące się na innej kondygnacji budynku Urzędu (serwerownia znajduje się na kondygnacji -1 , kopie zapasowe znajdują się na kondygnacji 2);
d) nośniki zawierające kopie zapasowe przechowywane są maksymalnie przez 5 lat, w wyznaczonym do tego celu pomieszczeniu, innym niż zbiory danych osobowych użytkowane na bieżąco;
e) w przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych, Użytkownicy systemu informatycznego zobowiązani są do przechowywania danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych.

4. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność. ASI testuje kopie zapasowe posiadanych zasobów informacyjnych w celu zminimalizowania ryzyka utraty informacji.

§ 12

1. Elektroniczne nośniki informacji zawierające dane osobowe przechowywane są zgodnie z zasadami opisanymi w paragrafie 10 niniejszej instrukcji.
2. Dane są przechowywane przez okres, w którym istnieją przesłanki do ich przetwarzania.
3. Sprzęt komputerowy, na którego dyskach twardych zawarte są dane osobowe przechowywany jest w pomieszczeniach odpowiednio zabezpieczonych znajdujących się w obszarze przetwarzania danych osobowych.
4. Kopiowanie danych osobowych na nośniki informacji oraz wykonywanie wydruków jest zabronione chyba, że istnieje konieczność ich sporządzania, która wynika z nałożonych na użytkownika obowiązków i dozwolona jest przepisami prawa.
5. Wykorzystywanie nośników informacji lub wydruków w innym celu niż wskazany w ust. 5 jest zabronione.
6. Dane są przechowywane przez okres, w którym istnieją przesłanki do ich przetwarzania. Po ustaniu przesłanek do przetwarzania, dane muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie.
7. Kopie zapasowe przechowuje ASI w miejscu, zapewniającym im odpowiednie warunki bezpieczeństwa.
8. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe – uszkadza się w sposób uniemożliwiający ich odczytanie.
9. Zdezaktualizowane i uszkodzone kopie zapasowe należy mechanicznie niszczyć w sposób uniemożliwiający ich ponowne użycie.
10. Nie wolno sporządzać wydruków z kopii zapasowych i innych nośników informacji, które podlegają zniszczeniu.

§ 13

1. Systemy informatyczne zabezpieczone są przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego w następujący sposób:
   a) dane przetwarzane są przy użyciu systemów pracujących w wewnętrznej sieci oddzielonej fizycznie od sieci publicznej przy pomocy bramy internetowej wyposażonej w firewall;
   b) zastosowano działający w „tle" program antywirusowy na komputerach użytkowników.
2. Użytkownik ma obowiązek na bieżąco sprawdzać obecność wirusów komputerowych. Czynność ta powinna być zaprogramowana w systemie, który automatycznie sygnalizuje obecność wirusów, w trakcie włączania systemu lub wprowadzania danych z zewnętrznych nośników informacji.
3. Kontrola antywirusowa systemu obejmować powinna wszystkie nośniki magnetyczne i optyczne, służące zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
4. Obowiązkiem ASI jest dostarczanie, uaktualnianie i instalowanie nowego oprogramowania antywirusowego.
5. Instalację nowego oprogramowania systemowego oraz oprogramowania użytkowego, gwarantującego bezpieczeństwo przetwarzania danych osobowych wykonuje ASI lub osoba upoważniona przez Burmistrza.

§ 14

1. Instalację nowego oprogramowania systemowego oraz oprogramowania użytkowego, gwarantującego bezpieczeństwo przetwarzania danych osobowych wykonuje ASI lub osoba upoważniona przez Burmistrza.
2. Okresowe przeglądy i konserwacje sprzętu komputerowego, wynikające z eksploatacji, warunków zewnętrznych oraz ważności systemu dla funkcjonowania Urzędu, wykonuje ASI lub osoba upoważniona przez Burmistrza.
3. Bieżącą konserwację i naprawę sprzętu wykonuje ASI lub osoba upoważniona przez Burmistrza.
4. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw w firmach zewnętrznych, pozbawia się przed naprawą zapisu danych osobowych albo naprawia się je pod nadzorem ASI.
5. W przypadku stwierdzenia przez ASI nieprawidłowości w działaniu elementów systemu opisanych w ust.1 pkt a, podejmuje on niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania. IOD powiadamiany jest w przypadku wystąpienia podejrzenia naruszenia ochrony danych lub stwierdzenia naruszenia ochrony danych.
6. Jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym dokonywane w obszarze przetwarzania danych osobowych, powinny odbywać się w obecności ASI.
7. Stosuje się następujące procedury wykonywania przeglądów nośników informacji służących do przetwarzania danych:

a) Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do likwidacji należy pozbawić zapisu, a w przypadku, gdy nie jest to możliwe, uszkodzić mechanicznie w sposób uniemożliwiający ich odczytanie.

Podlegające likwidacji uszkodzone lub przestarzałe nośniki a w szczególności twarde dyski z danymi osobowymi ze stacji roboczych i laptopów / pendrive / pamięci flash / płyty DVD / telefony komórkowe / smartfony są niszczone w sposób fizyczny w tym również komisyjnie. Stosowana metoda niszczenia, to fizyczne niszczenie (pocięcie, nawiercenie, młotkowanie) wymontowanych nośników zmielenie w specjalistycznej firmie potwierdzone protokołem zniszczenia lub certyfikatem bezpieczeństwa firmy utylizacyjnej lub nagraniem z procesu transportu i utylizacji.

b) Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do przekazania innemu podmiotowi, który nie jest uprawniony do otrzymania takich danych, należy wcześniej pozbawić zapisów danych – postępując zgodnie z zasadami opisanymi w niniejszej instrukcji.

§ 15

1. System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed utratą danych spowodowaną awarią lub zakłóceniami w sieci poprzez stosowanie:
    a) Centralnego UPS o odpowiednich parametrach;
    b) listew przepięciowych, połączonych pomiędzy siecią a komputerami;
    c) skrzynek rozdzielczych z bezpiecznikami.
2. Systemy informatyczne zabezpieczone są przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego w następujący sposób:
3. Użytkownik ma obowiązek na bieżąco sprawdzać obecność wirusów komputerowych. Czynność ta powinna być zaprogramowana w systemie, który automatycznie sygnalizuje obecność wirusów, w trakcie włączania systemu lub wprowadzania danych z zewnętrznych nośników informacji. Kontrola antywirusowa systemu obejmować powinna wszystkie nośniki magnetyczne i optyczne, służące zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
4. Obowiązkiem ASI jest dostarczanie, uaktualnianie i instalowanie nowego oprogramowania antywirusowego. Użytkownicy nie mogą instalować samodzielnie żadnego oprogramowania na sprzęcie służbowym, wszelkie zmiany wyłącznie za wiedzą ASI.
5. Instalację nowego oprogramowania systemowego oraz oprogramowania użytkowego, gwarantującego bezpieczeństwo przetwarzania danych osobowych wykonuje ASI, zastępca ASI lub inna osoba upoważniona przez Burmistrza.
6. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.

§ 16

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   a) **likwidacji** – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   b) **przekazania podmiotowi nieuprawnionemu do przetwarzania danych** – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
   c) **naprawy** – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI; (umowa powierzenia)
2. W celu usunięcia danych zapisanych na elektronicznych nośnikach, ASI może dokonać ich fizycznego uszkodzenia w taki sposób, by nie istniała możliwość odtworzenia zapisanych na nich danych.
3. Zabronione jest, aby Użytkownik wynosił poza swoje miejsce przydzielone przez Administratora, w szczególności poza pomieszczenia lub budynki Administratora, jakichkolwiek dokumentów i sprzętu IT wytworzonych u Administratora zawierających dane osobowe, chyba że Administrator wyrazi na to konkretnej osobie indywidualną zgodę na wynoszenie dokumentacji.

§ 17

1. Stosuje się następującą procedurę w przypadku stwierdzenia naruszenia zasad bezpieczeństwa systemu informatycznego:
   a) w przypadku stwierdzenia przez Użytkownika naruszenia zabezpieczeń przez osoby nieuprawnione, jest on zobowiązany niezwłocznie poinformować o tym fakcie IOD;
   b) IOD jest zobowiązany niezwłocznie podjąć czynności zmierzające do ustalenia przyczyn naruszeń zasad bezpieczeństwa i zastosować środki uniemożliwiające ich naruszanie w przyszłości określone w Polityce Bezpieczeństwa;
   c) w przypadku wykrycia zagrożenia automatycznym działaniem, możliwe jest zablokowanie pracy w systemie do chwili podjęcia decyzji o sposobie postępowania;
   d) w celu minimalizacji zagrożeń dąży się, w miarę możliwości organizacyjnych, do maksymalnej unifikacji sprzętu działającego w systemie informatycznym, stosowanego oprogramowania, konfiguracji sprzętu i oprogramowania, a także rozwiązań organizacyjnych;
   e) w Urzędzie funkcjonuje zakaz samowolnego korzystania z prywatnych lub pochodzących ze źródła innego, niż miejsce pracy, nośników informacji (magnetycznych, optycznych, urządzeń podłączanych do stacji roboczych). Mechanizmem zapobiegającym zmaterializowaniu się ryzyka zainfekowania systemu oprogramowaniem złośliwym jest obowiązek regularnego poddania nośników informacji badaniu oprogramowaniem antywirusowym.

§ 18

2. W przypadku stwierdzenia:
   a) błędu użytkownika systemu – ASI przeprowadza dodatkowe szkolenie osób zatrudnionych przy przetwarzaniu danych w komórce organizacyjnej. ASI dokumentuje odbycie szkolenia;
   b) uaktywnienia wirusa – należy zgłosić ASI, który ustali źródło jego pochodzenia oraz uaktualni zabezpieczenia antywirusowe;
   c) zaniedbania ze strony użytkownika – należy w stosunku do niego zastosować konsekwencje wynikające z właściwych przepisów prawa;
   d) włamania, w celu nielegalnego pozyskania danych – należy dokonać szczegółowej analizy wdrożonych środków zabezpieczenia i zapewnić skuteczniejszą ochronę;
   e) złego stanu urządzenia lub złego działania programu – należy niezwłocznie powiadomić ASI i przeprowadzić kontrolę czynności serwisowo-programowych.

ROZDZIAŁ VI – POSTANOWIENIA KOŃCOWE

§ 19

Wprowadzanie do systemu informacji z zewnątrz jest dopuszczalne tylko przy stwierdzeniu legalności i wiarygodności źródeł informacji i przez użytkownika posiadającego uprawnienia, wynikające z zakresu jego obowiązków.

§ 20

Pomieszczenie, w którym znajdują się serwery systemów, jest wydzielone wyłącznie dla potrzeb systemów informatycznych. Dostęp do w/w pomieszczenia powinien mieć wyłącznie ASI oraz osoby upoważnione przez Burmistrza.

§ 21

1. Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie, zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować jej przepisy na swoim stanowisku pracy.
2. Nadużycie przez użytkownika postanowień niniejszej Instrukcji, może stanowić podstawę do pociągnięcia go do odpowiedzialności przewidzianej właściwymi przepisami prawa.

§ 22

W sprawach nieuregulowanych niniejszą Instrukcją, znajdują zastosowanie przepisy wymienione w § 1 pkt 1 – 6.

§ 23

Niniejszy dokument wchodzi w życie z dniem 1 lipca 2021 r.

……..……

podpis Administratora Danych Osobowych