Załącznik Nr 2
do Zarządzenia Wójta Gminy
Nr 0050.19.2020
z dnia 09.03.2020 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM służącym do przetwarzania danych osobowych w Urzędzie Gminy

Zatwierdzam do stosowania

SPIS TREŚCI

Rozdział 1.
Postanowienia ogólne

§ 1
Podstawy prawne

1. Rozporządzenie 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 (RODO);

2. 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 .

§ 2
Słownik pojęć

1. **Administrator Danych Osobowych** (**ADO**) - organ, jednostka organizacyjna, podmiot lub osoba decydujące o celach i środkach przetwarzania danych osobowych. W tym przypadku Administratorem Danych Osobowych jest Gmina, reprezentowana przez Wójta Gminy.
2. **Inspektor Ochrony Danych Osobowych (IOD)** - osoba fizyczna upoważniona przez Administratora Danych Osobowych, zajmująca się zapewnianiem przestrzegania przepisów o ochronie danych osobowych.
3. **Administrator Systemów Informatycznych (ASI)** – osoba fizyczna wyznaczona przez Administratora Danych Osobowych, zajmująca się sprawowaniem ogólnego nadzoru nad bezpieczeństwem organizacyjnym, fizycznym oraz technicznym danych osobowych, przetwarzanych w systemie informatycznym.
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. **Jednostka organizacyjna –** Urząd Gminy
6. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym**.**
7. **Identyfikator / login** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
8. **IZSI / Instrukcja** – niniejszy dokument**.**
9. **Kopia pełna** - kopia zapasowa całości danych osobowych przetwarzanych w systemie informatycznym.
10. **Niezgodność** - niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe.
11. **Elektroniczne nośniki danych** – przedmioty fizyczne, na których możliwe jest zapisanie informacji w celu ich przechowywania, przetwarzania i transmisji. Każdy

nośnik danych charakteryzuje określona gęstość zapisu, wynikająca z jego właściwości fizycznych**.**

12. **Polityka Bezpieczeństwa Informacji (PBI) –** przyjęty do stosowania dokument Polityka Bezpieczeństwa Informacji w Urzędzie Gminy .
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. **System informatyczny (system IT)** - zespół współpracujących ze sobą urządzeń, programów, systemów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych osobowych.
16. **Serwisant** – pracownik firmy zewnętrznej lub pracownik Urzędu Gminy zajmujący się instalacją, naprawą oraz konserwacją sprzętu komputerowego**.**
17. **Sieć publiczna** – sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych.
18. **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.
19. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu**.**
20. **Użytkownik** - wyznaczony do przetwarzania danych osobowych pracownik, który odbył stosowne szkolenie w zakresie ochrony tych danych oraz uzyskał upoważnienie i uprawnienia dostępu do systemu informatycznego służącego do przetwarzania danych osobowych.
21. **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

§ 3
Cel i zakres stosowania instrukcji

1. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Priorytetowe jest zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności oraz integralności systemów informatycznych stosowanych w Jednostce Organizacyjnej.
2. Istotnym elementem osiągnięcia celu, o którym mowa w ust. 1 jest zapewnienie odpowiedniego poziomu oraz kontroli dostępu:
    1) do sieci, w tym urządzeń serwerowych,
    2) do systemów operacyjnych,
    3) do aplikacji,
    4) do informacji i zbiorów danych, wraz z określeniem trybu dostępu.

§ 4

1. Instrukcja została opracowana zgodnie z wymogami określonymi w Rozporządzeniu 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 (RODO);

2. 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

§5

Konfiguracja sprzętu komputerowego użytkownika systemu

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych oraz logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, w tym kontroli przepływu informacji pomiędzy system a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu.
2. Każdy dostęp do danych osobowych, musi być zarejestrowany.
3. Urządzenie mobilne (laptop, tablet itp.) zawierające dane osobowe musi być zabezpieczone przed nieuprawnionym dostępem poprzez wykorzystanie szyfrowania dysku twardego lub inny sposób szyfrowania i ochrony dostępu do danych.
4. Minimalne środki ochrony to:
    1) zainstalowanie na stacjach zapory sieciowej firewall i oprogramowania antywirusowego,
    2) wdrożenie systemu aktualizacji systemu operacyjnego oraz jego składników,
    3) wymaganie podania hasła przed uzyskaniem dostępu do systemu operacyjnego,
    4) niepozostawianie niezablokowanych stacji roboczej bez nadzoru.

§ 6

1. Użytkownik jest zobowiązany do stałego monitorowania komunikatów pochodzących z oprogramowania antywirusowego zainstalowanego na stacji roboczej oraz na urządzeniach mobilnych i reagowania na nie.
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.

Rozdział 2.

Procedury nadawania uprawnień. Metody i środki uwierzytelniania. Wygaszacze ekranu

§ 7
Procedury nadawania uprawnień

1. Dostęp do systemu informatycznego służącego do przetwarzana danych osobowych może uzyskać wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych nadane przez ADO (załącznik nr 1 do PBI), która podpisała oświadczenie o zachowaniu poufności (załącznik nr 2 do PBI).
2. Uprawnienia dostępu do systemu informatycznego służącego do przetwarzania danych osobowych nadaje ASI.
3. Uprawnienia, o których mowa w ust. 2 określają poziom dostępu do sieci, w tym urządzeń serwerowych, do systemów operacyjnych, do aplikacji i informacji;
4. ASI jest zobowiązany upoważnić co najmniej jednego pracownika obsługującego system informatyczny do rejestracji Użytkowników w tym systemie w czasie swojej nieobecności.

§ 8

1. Po nadaniu uprawnień w systemie informatycznym, ASI przydziela Użytkownikowi login i hasło tymczasowe.
2. Po otrzymaniu hasła tymczasowego Użytkownik ma obowiązek niezwłocznego zalogowania się do systemu informatycznego przy użyciu tego hasła oraz jego zmiany na hasło osobiste.
3. Zakazuje się przekazywania haseł tymczasowych poprzez osoby trzecie lub przy użyciu metod, które nie gwarantują zachowania jego poufności oraz niezaprzeczalnego ustalenia nadawcy i odbiorcy hasła, np. przez niechronione wiadomości przekazywane elektronicznie.
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 bezpieczeństwo danych osobowych przetwarzanych we wszystkich operacjach wykonanych przy użyciu jego loginu i hasła dostępu.
6. W przypadku wygaśnięcia przesłanek uprawniających Użytkownika do przetwarzania danych osobowych, w szczególności cofnięcia upoważnienia do ich przetwarzania, ASI przy współpracy z IOD zobowiązany jest do wyrejestrowania Użytkownika z systemu informatycznego, do którego był uprawniony.
7. Wyrejestrowanie Użytkownika z ewidencji osób upoważnionych do przetwarzania informacji następuje poprzez zablokowanie go we wszystkich opcjach systemu informatycznego, do których miał dostęp.

§ 9
Metody oraz środki uwierzytelniania,

1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym odbywa się na podstawie uwierzytelnienia, poprzez podanie indywidualnej nazwy (identyfikatora/loginu) i hasła Użytkownika.

2. Celem stosowania identyfikatora (loginu) Użytkownika jest jednoznaczne określenie osoby, która się nim posługuje.
3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika ASI za zgodą IOD nadaje inny identyfikator, odstępując od zasady określonej w ust. 1.
4. W przypadku zmiany imienia lub nazwiska może pozostać pierwotnie nadany identyfikator.
5. Identyfikator Użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
6. System informatyczny, w którym przetwarzane są dane osobowe musi automatycznie wymuszać podanie identyfikatora i hasła Użytkownika.

§ 10

1. Hasło Użytkownika:
   1) musi się składać co najmniej z 8 znaków, w tym zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
   2) nie może zawierać znaków następujących po sobie na klawiaturze bądź tych samych liter lub cyfr,
   3) nie może zawierać imion, nazwisk, przezwisk, inicjałów, dat, numerów rejestracyjnych samochodów, numerów telefonów i innych kombinacji znaków mogących doprowadzić do łatwego rozszyfrowania go przez osoby nieupoważnione,
   4) nie może być zapisywane w systemie w postaci jawnej**,**
   5) nie może być wyświetlane na ekranie komputera w sposób jawny**,**
   6) nie może być ujawnione innej osobie, nawet po utracie ważności**,**
   7) musi być zabezpieczone przez Użytkownika przed nieuprawnionym dostępem osób trzecich.
2. W przypadku nieumyślnego ujawnienia hasła osobie nieuprawnionej lub podejrzenia ujawnienia, należy bezzwłocznie powiadomić ASI i dokonać zmiany hasła na nowe**.**
3. System informatyczny, w którym przetwarzane są dane osobowe automatycznie wymusza zmianę hasła nie rzadziej niż co 30 dni.
4. ASI może, w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez Użytkownika oraz zapewniać automatyczną weryfikację spełniania wymogów dotyczących hasła**.**

§ 11
Wygaszacze ekranu

1. Wygaszacze ekranu systemowo ustawiane są na aktywację po 15 minutach bezczynności na danej stacji roboczej oraz w razie potrzeby (np. opuszczenie miejsca przetwarzania danych) skrótem klawiaturowym.
2. Uruchomienie wygaszacza ekranu wiąże się z koniecznością ponownego zalogowania, celem wznowienia pracy stacji roboczej.

Rozdział 3.

Procedury rozpoczynania, zawieszania i kończenia pracy w systemie informatycznym

§ 12
Rozpoczęcie pracy

1. Procedura rozpoczęcia pracy w systemie informatycznym następuje poprzez zalogowanie się Użytkownika do komputera przez podanie loginu i hasła dostępu.
2. W przypadku zapomnienia przez Użytkownika konstrukcji hasła, winien on niezwłocznie zawiadomić ASI, który nadaje nowe hasło, postępując zgodnie z procedurą obowiązującą przy nadawaniu uprawnień dostępu do systemu informatycznego.

§ 13
Zawieszenie pracy

1. Ustala się następującą procedurę zawieszenia pracy w systemie informatycznym:
   1) przy każdorazowym opuszczeniu stanowiska komputerowego, należy dopilnować, aby osoby postronne nie miały dostępu do danych przetwarzanych na tym stanowisku,
   2) każdy Użytkownik ma obowiązek stosowania wygaszacza ekranu zabezpieczonego hasłem oraz wylogowania się z systemu lub jego blokowania,
   3) zablokowanie komputera odbywa się poprzez naciśnięcie kombinacji klawiszy,
   4) niezależnie od powyższego, wygaszacz ekranu aktywuje się nie później niż w 15 minucie bezczynności Użytkownika,
   5) odblokowanie odbywa się poprzez ponowne zalogowanie się tego samego Użytkownika,
2. W pomieszczeniu, w którym przetwarzane są dane osobowe mogą znajdować się osoby postronne wyłącznie za zgodą i w towarzystwie Użytkownika lub ASI.
3. W przypadku zawieszenia pracy w systemie informatycznym z powodu konieczności załatwienia sprawy z osobą postronną znajdującą się w tym samym pomieszczeniu, Użytkownik ma obowiązek zabezpieczenia ekranu komputera lub urządzenia mobilnego oraz dokumentów i wydruków znajdujących się na biurku w sposób uniemożliwiający podgląd zawartych w nich treści.

§ 14
Zakończenie pracy

1. Zakończenie pracy w systemie informatycznym polega na wybraniu odpowiedniego polecenia systemowego umożliwiającego zakończenie pracy.
2. Zaleca się zamknięcie wszystkich programów i zapisanie wszystkich otwartych plików. Użytkownik powinien pozostać przy komputerze do chwili ich zamknięcia.
3. Użytkownik kończący pracę powinien sprawdzić, czy wszystkie elektroniczne nośniki informacji lub wydruki i dokumenty zawierające dane osobowe zostały zabezpieczone przed dostępem osób nieupoważnionych.
4. Osoba opuszająca pomieszczenie jako ostatnia powinna zamknąć okna oraz zamknąć drzwi od pomieszczenia na klucz.

Rozdział 4.

Procedury użytkowania urządzeń mobilnych i elektronicznych nośników informacji

§ 15

1. Przy przetwarzaniu danych osobowych na urządzeniach mobilnych oraz elektronicznych nośnikach informacji należy stosować procedury obowiązujące w przypadku użytkowania komputerów i urządzeń stacjonarnych.
2. Obowiązuje zakaz używania urządzeń mobilnych oraz elektronicznych nośników informacji przez osoby inne niż Użytkownicy, którym zostały one powierzone.
3. Pliki zawierające dane osobowe przechowywane na urządzeniach mobilnych elektronicznych nośnikach informacji muszą być zaszyfrowane i opatrzone hasłem dostępu.
4. Urządzenia mobilne i elektroniczne nośniki informacji powinny być wyposażone w odpowiednie programy ochrony antywirusowe.

Rozdział 5.

Zabezpieczanie danych w systemie informatycznym

§ 16

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.
2. Za tworzenie i przechowywanie kopii zapasowych, o których mowa w ust. 1, w sposób zgodny z przepisami, o których mowa w § 1 ust. 1 i 2 oraz niniejszej Instrukcji odpowiedzialny jest ASI.
3. Dostęp do kopii zapasowych posiada wyłącznie ASI lub w wyjątkowych wypadkach, osoba przez niego upoważniona.

§ 17

Sposób, miejsce i okres przechowywania kopii zapasowych i elektronicznych nośników informacji

1. Kopie zapasowe i elektroniczne nośniki informacji przechowywane są w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem, a kopie awaryjne należy bezzwłocznie usuwać po ustaniu ich użyteczności w przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych.
2. Kopie zapasowe i elektroniczne nośniki informacji przechowywane są przez okres, w którym istnieją przesłanki do ich przetwarzania. Po ustaniu przesłanek, o których mowa w zdaniu pierwszym, dane znajdujące się na kopiach zapasowych muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie.

§ 18

Sposób zabezpieczania systemu informatycznego

1. Zasady zachowania bezpieczeństwa w systemie informatycznym obejmują wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę informacji, stanowiących tajemnicę służbową przed ich nieuprawnionym przetwarzaniem oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami sieci zasilającej.
2. System informatyczny musi być chroniony równolegle na wielu poziomach m.in. poprzez stosowanie oprogramowania antywirusowego, systemów typu firewall, odpowiednią konfigurację systemu aktualizacji systemu operacyjnego oraz realizację kopii bezpieczeństwa.
3. Oprogramowanie antywirusowe jest instalowane na wszystkich stanowiskach komputerowych oraz urządzeniach mobilnych i elektronicznych nośnikach informacji.
4. Użytkownik na stanowisku komputerowym, importujący dane do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów i szkodliwego oprogramowania.

5. O pojawiających się komunikatach wskazujących na wystąpienie zagrożenia spowodowanego szkodliwym oprogramowaniem, Użytkownik jest zobowiązany niezwłocznie powiadomić ASI
6. Za wdrożenie, oraz aktualizację i korzystanie z oprogramowania, o którym mowa w ust. 2 odpowiada ASI.

§ 19

1. W celu zapewnienia ochrony systemu informatycznego może być stosowany monitoring wykorzystania infrastruktury informatycznej, w szczególności obejmujący następujące elementy:
    1) analizę oprogramowania wykorzystanego na stacjach roboczych,
    2) analizę stacji roboczych pod względem wykorzystania nielegalnego oprogramowania, plików multimedialnych oraz innych elementów naruszających prawo autorskie;
    3) analizę odwiedzanych stron WWW,
    4) analizę godzin pracy na stanowiskach komputerowych;
    5) analizę dostępów (autoryzowanych oraz nieautoryzowanych),
    6) analizę ruchu sieciowego pod względem komunikacji, szkodliwej dla bezpieczeństwa danych przetwarzanych w systemie.
2. Monitoring bezpieczeństwa musi odbywać się z zachowaniem obowiązującego prawa.

§ 20

Udostępnianie danych w systemie informatycznym

1. Dla każdej osoby, której dane są przetwarzane, system informatyczny służący do przetwarzania danych osobowych (z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie) zapewnia odnotowanie:
    1) daty pierwszego wprowadzenia danych do systemu,
    2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
    3) źródła danych (jedynie w przypadku zbierania danych nie od osoby, której dotyczą),
    4) informacji o odbiorcach,
    5) sprzeciwu odnośnie przetwarzania danych osobowych.
2. Dla każdej osoby, której dane osobowe są przetwarzane, system informatyczny zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1 pkt 1-5.
3. Odnotowanie informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia (z wyłączeniem osób, których dane dotyczą, osób posiadających upoważnienie do przetwarzania danych, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem), odbywa się poprzez zapisanie tej informacji w utworzonym na dysku twardym komputera pliku dotyczącym danej osoby.

§ 21
Obowiązki Administratora Systemów Informatycznych w zakresie zabezpieczenia systemu informatycznego

1. Do obowiązków ASI w zakresie zabezpieczenia systemu informatycznego należy :
   1) nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemów,
   2) nadzór nad czynnościami związanymi ze sprawdzaniem systemów pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji,
   3) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,
   4) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
   5) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych, w tym zarządzanie kontami użytkowników (ustalenie identyfikatorów i haseł, ich przyznawanie, anulowanie, resetowanie i ochrona) oraz w porozumieniu z IOD dbałość o właściwe ustawienie urządzeń, tak aby minimalizować możliwość nieuprawnionego dostępu,
   6) podejmowanie natychmiastowych działań zabezpieczających stan systemów informatycznych w przypadku otrzymania informacji o naruszeniu zabezpieczeń, informacji o zmianach w sposobie działania systemu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych, w tym podjęcie działań mających na celu wykrycie przyczyny lub sprawcy zaistniałej sytuacji i jej usunięcie.

§ 22

1. W celu zabezpieczenia integralności systemu informatycznego ASI może wykorzystywać w trakcie pracy oprogramowanie lub narzędzia monitorujące i rejestrujące aktywność Użytkowników na stanowiskach komputerowych.
2. Zabezpieczenie integralności systemu informatycznego realizowane jest również poprzez zakaz:
   1) wysyłania masowej poczty kierowanej do losowych odbiorców (spam),
   2) przechowywania w systemie informatycznym treści łamiących prawo autorskie (filmy, utwory muzyczne lub oprogramowanie),
   3) nieuzasadnionego wynoszenia lub wysyłania danych osobowych poza obszar przetwarzania danych,
   4) instalowania przez Użytkownika oprogramowania na sprzęcie komputerowym, które nie uzyskało akceptacji ASI,
   5) wykorzystywania przeglądarek internetowych, które nie uzyskały akceptacji ASI oraz odwiedzania witryn internetowych zawierających potencjalnie niebezpieczne treści,
   6) przemieszczania sprzętu komputerowego do innej lokalizacji (pokoju) lub zmiany Użytkownika bez uzgodnienia z ASI,

7) fizycznego ingerowania w konfigurację sprzętową urządzeń,
8) podejmowania prób wykorzystania obcego konta, uruchamiania aplikacji deszyfrujących hasła, prowadzenia działań mających na celu podsłuchanie lub przechwycenie informacji przepływających w systemach informatycznych.

3. Dla zachowania integralności systemu informatycznego ASI może podjąć decyzję o:
   1) deinstalacji niebezpiecznego oprogramowania,
   2) usunięciu nielegalnych, niebezpiecznych oraz utrudniających wykonanie kopii bezpieczeństwa plików,
   3) zablokowaniu dostępu Użytkownika w przypadku stwierdzenia, że komputer lub urządzenie dołączone do systemu informatycznego generuje strumień danych zakłócający pracę sieci lub w razie podejrzenia używania komputera jako niezarejestrowanego serwera danych. O tym fakcie powiadamiany jest IOD i bezpośredni przełożony Użytkownika,
   4) w porozumieniu z IOD, zablokowaniu konta Użytkownika.

§ 23
Procedury wykonywania przeglądów i konserwacji systemu informatycznego.

1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację platformy sprzętowej, na której eksploatowany jest system informatyczny wykorzystywany w Jednostce Organizacyjnej.
2. Przeglądy i konserwacja urządzeń wchodzących w skład platformy sprzętowej, o której mowa w ust. 1 powinny być wykonywane nie rzadziej niż w terminach określonych przez producenta sprzętu.
3. Jeśli producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych lub nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decyduje ASI.
4. Wszelkie naprawy urządzeń komputerowych, w tym urządzeń mobilnych i elektronicznych nośników informacji, oraz zmiany w systemie informatycznym przeprowadza, w miarę możliwości, ASI.
5. 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 lub w sytuacji wyjątkowej – osoby przez niego wyznaczonej.
6. W przypadku niemożności dokonania naprawy uszkodzonego sprzętu komputerowego zawierającego dane osobowe, należy go zniszczyć mechanicznie w sposób trwale uniemożliwiający odczytanie jego zawartości.
7. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez Użytkownika potrzeby wprowadzenia zmian pozwalających dostosować ich funkcjonalność do obsługi bieżących lub planowanych potrzeb Jednostki Organizacyjnej. Zgłoszenia rozpatruje ASI.

§ 24

1. Nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji, powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane przez ASI.
2. Przegląd aplikacji przeprowadzany jest w celu sprawdzenia poprawności działania i wykonywany jest w następujących przypadkach:
   1) zmiany wersji oprogramowania aplikacji,
   2) zmiany systemu operacyjnego platformy sprzętowej, na której eksploatowana jest aplikacja,

3) wykonania zmian w aplikacji spowodowanych koniecznością naprawy lub modyfikacji systemu;

3. Przed dokonaniem zmian w aplikacji należy, o ile to możliwe, dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych, na testowej bazie danych. Sprawdzenie powinno obejmować w szczególności:
   1) poprawność logowania się do systemu w zależności od posiadanych uprawnień (symulacja pracy wszystkich typów uprawnień Użytkownika),
   2) techniczną poprawność działania aplikacji.

§ 25

Procedura w przypadku stwierdzenia naruszenia zasad bezpieczeństwa systemu informatycznego

1. W przypadku stwierdzenia przez Użytkownika naruszenia zabezpieczeń systemu informatycznego przez osoby nieuprawnione, jest on zobowiązany niezwłocznie poinformować o tym fakcie ASI.
2. ASI jest zobowiązany niezwłocznie podjąć czynności zmierzające do ustalenia przyczyn naruszeń zasad bezpieczeństwa i zastosować środki uniemożliwiające ich naruszanie w przyszłości.
3. W przypadku wykrycia zagrożenia automatycznym działaniem, możliwe jest zablokowanie pracy w systemie do chwili podjęcia decyzji o sposobie postępowania.
4. W celu minimalizacji zagrożeń dąży się, w miarę możliwości organizacyjnych, do maksymalnej unifikacji sprzętu, stosowanego oprogramowania, konfiguracji sprzętu i oprogramowania, a także rozwiązań organizacyjnych.

Rozdział 6.

Postanowienia końcowe

§ 26

1. W sprawach nieuregulowanych niniejszą Instrukcją, znajdują zastosowanie przepisy wymienione w § 1 ust. 1 - 2.
2. Nad aktualnością Instrukcji czuwa IOD w porozumieniu z ASI.
3. IOD we współpracy z ASI może prowadzić kontrolę przestrzegania Instrukcji. Wyniki kontroli doraźnych przedstawiane są ADO.