INSTRUKCJA

ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH

Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie

ul. Pstrowskiego 28B

10-602 Olsztyn

Data wprowadzenia:	**07. 05. 2008**
Wersja:	**4**
Daty aktualizacji:	**30. 04. 2021**
Zarządzenie Dyrektora	**17/2021 z dnia 30.04.2021**
Opracował:	**Krzysztof Grzymkowski** **Jolanta Janiszewska**
Zatwierdził:	**Marek Myszkowski** Dyrektor

SPIS TREŚCI

ROZDZIAŁ I

CEL WPROWADZENIA DOKUMENTU

Celem niniejszego dokumentu jest określenie zasad eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych zgodnie z obowiązującymi wymaganiami prawnymi, w szczególności:

- Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2019 r. poz. 1781) zwaną dalej Ustawą, oraz art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 r. Nr 100, poz. 1024).

ROZDZIAŁ II

POJĘCIA STOSOWANE W DOKUMENCIE

1. **Administrator Danych (ADO)** – podmiot decydujący o celach i środkach przetwarzania danych osobowych tj. Wojewódzka Stacja Pogotowia Ratunkowego w Olsztynie. Za jej działania w zakresie ochrony danych osobowych odpowiada Dyrektor WSPR,
2. **Informatyk** – osoba administrująca wybranym systemem informatycznym, w którym przetwarzane są dane osobowe lub wybraną aplikacją,
3. **Aplikacja** – oprogramowanie dedykowane do przetwarzania danych osobowych,
4. **Bezpośredni przełożony** – Kierownik komórki organizacyjnej w Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie (np.: Kierownik Działu, Sekcji, Zespołu Wyjazdowego bądź innych wydzielonych części organizacyjnych WSPR) będący bezpośrednim zwierzchnikiem służbowym podległego pracownika zgodnie z Regulaminem Organizacyjnym w WSPR w Olsztynie,
5. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której

tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań,

6. **Dane służbowe** – dane osobowe pracowników lub współpracowników służące do kontaktowania się z nimi w sprawach służbowych, tj. imię i nazwisko, stanowisko służbowe (zawód), służbowy numer telefonu, służbowy adres e-mail, ewentualnie informacje związane ze stanowiskiem służbowym (np. godziny pracy, miejsce pracy),
7. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
8. **Hasło administracyjne** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie ASI i IDO po wprowadzeniu, którego można zarządzać system informatycznym z panelu administratora.
9. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
10. **Inspektor Ochrony Danych** - osoba, która w imieniu i z upoważnienia Administratora danych realizuje nadzór nad bezpieczeństwem przetwarzania danych osobowych w Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie, zwany również IDO;
11. **Instrukcja** – niniejszy dokument,
12. **Odbiorca danych** – każdy, komu udostępnia się dane osobowe, z wyłączeniem:
    - ❖ osoby, której dane dotyczą,
    - ❖ osoby upoważnionej do przetwarzania danych,
    - ❖ podmiotu, któremu powierzono przetwarzanie danych osobowych
    - ❖ organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
13. **Polityka Bezpieczeństwa** – Polityka Bezpieczeństwa danych osobowych w Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie,
14. **Poufność -** rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
15. **Powierzenie przetwarzania danych** – zlecenie wykonania czynności przetwarzania danych innemu podmiotowi, w drodze odrębnej umowy zawartej na piśmie (umowa powierzenia) lub stosownego zapisu do umowy, wyłącznie w zakresie i celu w niej przewidzianym,
16. **Pracownik** – osoba zatrudniona na podstawie stosunku pracy. Ilekroć w Polityce jest mowa o pracowniku, należy przez to rozumieć także osoby wykonujące zadania i/lub prace w Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie, niezależnie od rodzaju stosunku

formalnego łączącego tę osobę z WSPR (np. umowa zlecenie, o dzieło, kontrakt, staż, specjalizacja, praktyka, wolontariat etc.),

17. **Procesor** - podmiot, z którym Administrator danych zawarł umowę powierzenia,
18. **Przetwarzanie danych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalania, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
19. **Rejestr Przetwarzania Danych** -wewnętrzny firmowy dokument, prowadzony w formie elektronicznej oraz w formie dokumentu papierowego. Jest to dokument, który ma pokazywać w szczególności w jakich procesach w organizacji są przetwarzane dane osobowe, w jakim celu, kogo dotyczą oraz jak są zabezpieczane. Dokument ten będzie musiał zostać udostępniony na każde wezwanie GIODO,
20. **System informatyczny** lub **system** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
21. **Udostępnianie danych** – czynności na danych osobowych umożliwiające dostęp do nich osobom niebędącymi pracownikami podmiotów przetwarzających dane osobowe oraz nieposiadającymi upoważnienia do przetwarzania danych osobowych w WSPR, np. przekazywanie, rozpowszechnianie lub ujawnienie poprzez transmisję,
22. **Usuwanie danych** – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą (anonimizacja danych), dokonane w sposób trwały, tj. bez możliwości ich odzyskania (np. za pomocą dedykowanego systemu do bezpiecznego usuwania danych, demagnetyzacja, zniszczenie fizyczne nośnika danych,
23. **Uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja tożsamości podmiotu,
24. **Użytkownik** - osoba, która zgodnie z obowiązującymi w WSPR regulacjami otrzymała upoważnienie do przetwarzania danych oraz uprawnienia i hasła dostępu do pracy w systemie bądź aplikacji,
25. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

ROZDZIAŁ III

PROCEDURA NADAWANIA, MODYFIKACJI ORAZ ODBIERANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH

1. Nadanie uprawnień do systemów przetwarzających dane osobowe może nastąpić jedynie po wcześniejszym nadaniu upoważnienia do przetwarzania danych osobowych zgodnie z procedurą opisaną w Polityce.
2. Wniosek o nadanie uprawnień wystawiany jest w formie papierowej przez Bezpośredniego przełożonego pracownika (w przypadku pracowników WSPR) lub osobę odpowiedzialną za współpracę z daną osobą (w sytuacji, o której mowa w rozdziale VIII pkt 7 Polityki). Wzór wniosku jest tożsamy z wnioskiem o nadanie/odwołanie upoważnienia do przetwarzania danych osobowych i stanowi załącznik nr 2 Polityki.
3. Informatykowi przysługuje prawo weryfikacji wniosku pod względem zakresu uprawnień, jakie mają zostać nadane pracownikowi.
4. W sytuacji, gdy Informatyk uzna, iż wnioskowany zakres uprawnień jest niewłaściwy (zbyt szeroki bądź zbyt wąski), dokonuje zmiany zakresu uprawnień, czyniąc o tym wzmiankę na wniosku oraz potwierdzając to datą i własnoręcznym podpisem.
5. O zmianie zakresu uprawnień Informatyk informuje Bezpośredniego przełożonego osoby upoważnianej bądź pracownika WSPR w Olsztynie odpowiedzialnego za współpracę z upoważnianą osobą, o której mowa w rozdziale VII pkt 7 Polityki.
6. W razie zaistnienia sporu dotyczącego zakresu uprawnień, decyzje w tej sprawie podejmuje Dyrektor WSPR (ADO).
7. Informatyk nadaje uprawnienia we wnioskowanych systemach informatycznych osobie, której wniosek dotyczył, na podstawie przekazanego przez kierownika komórki organizacyjnej upoważnienia zatwierdzonego przez ADO, zawierającej imię, nazwisko oraz zakres uprawnień, ze wskazaniem systemu informatycznego, w którym uprawnienia mają zostać nadane.
8. W przypadku nadawania Użytkownikowi po raz pierwszy uprawnień do systemu informatycznego, Informatyk dokonuje wygenerowania identyfikatora Użytkownika oraz hasła tymczasowego. Hasło tymczasowe umożliwia pierwsze zalogowanie się Użytkownika do systemu informatycznego, które po zalogowaniu się Użytkownik zobowiązany jest zmienić.
9. Informatyk przekazuje do IDO informację o wygenerowaniu identyfikatora Użytkownika i/lub nadaniu uprawnień, celem uzupełnienia ewidencji osób upoważnionych do przetwarzania danych. IDO informuje przełożonego użytkownika o możliwości korzystania z systemu

informatycznego w zakresie przyznanych uprawnień oraz wygenerowanym haśle tymczasowym. Przekazanie hasła tymczasowego Użytkownikowi powinno nastąpić w sposób uniemożliwiający zapoznanie się z hasłem przez osoby nieupoważnione,

10. Modyfikacja lub odebranie uprawnień w systemach informatycznych następuje po zmianie lub odebraniu upoważnienia do przetwarzania danych osobowych zgodnie z procedurą opisaną w Polityce Bezpieczeństwa Danych Osobowych. Kadry Informują IDO o zwolnieniu bądź odejściu pracownika.
11. Każda modyfikacja zakresu uprawnień do przetwarzania danych osobowych w systemach informatycznych lub odebranie takich uprawnień dokonywane są przez Informatyka niezwłocznie po przedłożeniu mu przez IDO pisemnej informacji (w tym przesłanej drogą mailową) o odebraniu bądź modyfikacji uprawnień do przetwarzania danych osobowych.
12. W sytuacji niecierpiącej zwłoki, uprawnienia Użytkownika mogą zostać zawieszone przez Informatyka na wniosek Inspektora Ochrony Danych, gdy bieżące działanie Użytkownika może spowodować zagrożenie dla bezpieczeństwa danych osobowych.
13. Przyznawanie uprawnień w systemach informatycznych Kierownikom komórek organizacyjnych WSPR oraz osobom pracującym na samodzielnych stanowiskach pracy odbywa się z pominięciem postanowień pkt 2-5. Regulacje wynikającą z treści pkt 6 stosuje się odpowiednio.
14. IDO we współpracy z Informatykiem dokonuje raz na pół roku wyrywkowego przeglądu uprawnień nadanych Użytkownikom w wybranych systemach informatycznych i w miarę potrzeby wskazuje na konieczność dokonania działań korekcyjnych.

ROZDZIAŁ IV

STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. Użytkownicy systemu informatycznego przetwarzającego dane osobowe wykorzystują w procesie uwierzytelnienia identyfikatory i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi i nie podlega zmianie. Identyfikator Użytkownika zbudowany jest z pierwszej litery imienia, separatora (kropki) oraz nazwiska użytkownika. W identyfikatorze pomija się polskie litery. Dopuszcza się, że identyfikator zawiera inne znaki jeśli aplikacja tego wymaga.
3. Identyfikatory Użytkowników nie mogą się powtarzać i być ponownie nadawane innym osobom. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanym w systemie Informatyk za zgodą IDO odstępuje od zasady określonej w pkt 2 nadając inny identyfikator.

4. Po zalogowaniu do systemu z wykorzystaniem otrzymanego hasła tymczasowego, o którym mowa w rozdziale III pkt 9, Użytkownik zobowiązany jest do jego natychmiastowej zmiany, nawet, jeżeli system informatyczny nie wymusza takiego działania.
5. Zarówno tymczasowe, jak i zmienione przez Użytkownika hasło dostępu do systemu informatycznego przetwarzającego dane osobowe musi spełniać poniższe warunki:
   - ❖ nie jest oparte na skojarzeniach łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby,
   - ❖ nie jest krótsze niż 8 znaków,
   - ❖ zawiera małe i duże litery oraz cyfry lub znaki specjalne.

6. Hasło jest zmieniane przez Użytkownika nie rzadziej, niż co 30 dni (nawet jeżeli system informatyczny nie wymusza zmiany hasła z taką częstotliwością).
7. Użytkownik zobowiązany jest do:
   - ❖ nieujawniania hasła innym osobom,
   - ❖ zachowania hasła w poufności, również po jego wygaśnięciu,
   - ❖ przestrzegania zasad dotyczących jakości i częstotliwości zmian hasła,
   - ❖ wprowadzania hasła do systemu w sposób minimalizujący podejrzenie go przez innych Użytkowników systemu bądź osoby nieuprawnione.
8. W przypadku zapomnienia hasła, Użytkownik powinien zwrócić się do Informatyka o wygenerowanie nowego hasła tymczasowego.
9. Przed wygenerowaniem nowego hasła tymczasowego Informatyk kontaktuje się z IDO, w celu zweryfikowania posiadania przez osobę, o której mowa w pkt 8, aktualnego upoważnienia do przetwarzania danych osobowych.
10. Dostęp do haseł administracyjnych posiada jedynie Informatyk w zakresie powierzonych mu uprawnień do administracji systemami informatycznymi. Hasła administracyjne nie podlegają zmianie.
11. Wykaz haseł administracyjnych, którymi posługują się Informatyk ze wskazaniem systemów informatycznych, przechowuje IDO w zamkniętych kopertach w sposób uniemożliwiający wgląd do nich osobom nieupoważnionym.

ROZDZIAŁ V

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONA DLA UŻYTKOWNIKÓW SYSTEMU

1. Rozpoczynając pracę w systemie informatycznym przetwarzającym dane osobowe Użytkownik:

- ❖ wprowadza niezbędny do pracy identyfikator i hasło,
- ❖ hasło powinno być wprowadzane w sposób minimalizujący ryzyko zapoznania się z nimi przez osoby trzecie,
- ❖ w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego identyfikatora i hasła natychmiast kontaktuje się z Informatykiem,
- ❖ w przypadku niestandardowego zachowania systemu przetwarzającego dane osobowe pracownik natychmiast kontaktuje się z Informatykiem oraz informuje o tym IDO.

2. Za niestandardowe zachowanie systemu informatycznego przetwarzającego dane osobowe mogące sugerować naruszenie zasad bezpieczeństwa, w szczególności uważa się:
   - ❖ częściowy lub całkowity brak danych wcześniej zapisanych,
   - ❖ dostęp do danych w zakresie szerszym niż dotychczasowy dostęp posiadany przez Użytkownika,
   - ❖ brak dostępu do systemu informatycznego bądź aplikacji,
   - ❖ brak dostępu do katalogów przypisanych Użytkownikowi na serwerze bądź dysku sieciowym,
   - ❖ wykrycie oprogramowania niebezpiecznego, którego to nie jest w stanie program antywirusowy w sposób automatyczny zneutralizować, pojawienie się komunikatu o zalogowaniu się do systemu kolejnego Użytkownika.
3. Zawieszając pracę w systemie informatycznym (w tym odchodząc od stanowiska pracy) Użytkownik blokuje stację roboczą w sposób dostępny w systemie operacyjnym. Kontynuacja pracy może nastąpić po odblokowaniu stacji roboczej przez wprowadzenie hasła w sposób ograniczający zapoznanie się z nim przez osoby trzecie.
4. Niedozwolone jest odejście od stacji roboczej bez uniemożliwienia osobom nieupoważnionym dostępu do systemu informatycznego służącego do przetwarzania danych osobowych.
5. Kończąc pracę, Użytkownik wylogowuje się ze wszystkich systemów i aplikacji, z których korzystał.
6. Użytkownik korzystający poza obszarem przetwarzania danych osobowych z komputera przenośnego lub innego urządzenia przenośnego zawierającego dane osobowe jest zobowiązany do szczególnej ostrożność podczas jego transportu, przechowywania i użytkowania, w tym do zabezpieczenia go przed kradzieżą, utratą lub zniszczeniem.

ROZDZIAŁ VI

PROCEDURA TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Dane osobowe przetwarzane w formie elektronicznej zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych.

2. Kopie zapasowe poszczególnych systemów informatycznych wykorzystywanych do przetwarzania danych osobowych oraz kopie zbiorów danych przetwarzanych w tych systemach wykonywane są na serwery bądź dyski sieciowe. Szczegółowy opis sposobu wykonywania kopii zapasowych oraz harmonogram ich wykonywania zawiera Załącznik nr 1 do niniejszego dokumentu.
3. Każdy pracownik zobowiązany jest do przechowywania elektronicznych dokumentów zawierających dane osobowe, na przypisanym mu na serwerze bądź dysku sieciowym.
4. Za tworzenie kopii danych osobowych zgromadzonych na dyskach sieciowych odpowiada Informatyk,
5. Kopie zapasowe zbiorów, o których mowa w pkt 4 wykonuje się na serwery bądź dyski sieciowe.
6. Dostęp do kopii zapasowych posiadają jedynie upoważnione osoby.
7. Kopia zapasowa podlega sprawdzaniu pod względem poprawności zapisu. W przypadku jej wadliwości, kopię sporządza się ponownie.
8. Pod koniec każdego roku kopie podlegają okresowemu sprawdzaniu pod kątem ich przydatności do odtworzenia danych na wypadek awarii systemów informatycznych.
9. Decyzję o odtworzeniu zbioru danych z kopii zapasowej w przypadku awarii systemu podejmuje Dyrektor bądź Zastępca Dyrektora. Przed dokonaniem odtworzenia danych z kopii zapasowej, Informatyk zobligowany jest upewnić się, że odtwarzana kopia nie zawiera oprogramowania złośliwego, który spowodował lub mógł spowodować konieczność odtworzenia zbioru danych lub systemu informatycznego.
10. Administrator Systemów Informatycznych odnotowuje w dzienniku sporządzonych kopii zapasowych jeżeli wykonuje kopie danych poza harmonogramem (załącznik nr. 1). Wzór dziennika stanowi Załącznik nr 2 do Instrukcji.

ROZDZIAŁ VII

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

1. Pracownicy WSPR zobowiązani są do przechowywania danych na serwerach bądź dyskach sieciowych w przypisanych im folderach.
2. Dozwolone jest wykorzystywanie jedynie dedykowanych (tj. dopuszczonych do użytku w WSPR) systemów informatycznych i aplikacji służących do przetwarzania danych osobowych.

3. Czas przechowywania danych osobowych na nośnikach danych jest uzależniony od celu, w jakim dane są przetwarzane i wymagań dotyczących archiwizacji, wynikających z obowiązujących przepisów prawa.
4. W przypadku aktualizacji danych nośniki sprzed aktualizacji, których nie można nadpisać (np. CD/DVD), a które utraciły przydatność powinny zostać zniszczone w przeznaczonych do tego celu niszczarkach.

5. Nośniki danych, które uległy uszkodzeniu oraz nie jest możliwa ich naprawa (np. dyski twarde, pendrive) podlegają fizycznemu zniszczeniu.
6. Niedozwolone jest przekazywanie danych osobowych na elektronicznych nośnikach danych (np. pendrive, CD/DVD, przenośna karta pamięci). W Wyjątkowych sytuacjach dopuszcza się przekazanie danych w formie zaszyfrowanej za zgoda ADO lub IDO.
7. Przekazywanie rozmów telefonicznych na nośnikach danych pomiędzy komórkami organizacyjnymi oraz do urzędów lub organów wnioskujących o rozmowy następuje poprzez zaszyfrowanie danych np. aplikacją 7zip stosując złożoność haseł (rozdział IV punkt 5).
8. Nośniki magnetyczne, cyfrowe, optyczne lub inne z danymi osobowymi są opisywane i przechowywane w zamykanych na klucz szafach.
9. Osoba użytkująca elektroniczny nośnik danych, zobowiązana jest do:
   - ❖ niepozostawiania nośnika bez nadzoru,
   - ❖ przechowywania nośnika w szafie zamykanej na klucz po zakończeniu na nim pracy.

ROZDZIAŁ VIII

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:

- ❖ połączenia wychodzące do sieci Internet i przychodzące z sieci Internet obsługiwane są poprzez Router z firewallem ;
- ❖ zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych w systemach informatycznych;
- ❖ dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora Użytkownika oraz hasła składającego się z minimum 8 znaków, zawierających duże i małe litery oraz znaki specjalne;
- ❖ zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów systemu operacyjnego dla poszczególnych Użytkowników;

- ❖ zastosowano mechanizmy wymuszające okresową zmianę haseł dostępu do systemów informatycznych służących do przetwarzania danych osobowych;
- ❖ komputery i serwery zabezpieczone są przed działaniem szkodliwego oprogramowania za pomocą systemów antywirusowych, które dodatkowo zabezpieczają przed atakami sieciowymi i ograniczają rozprzestrzenianie się wrogich kodów;
- ❖ aktualizację automatyczną oprogramowania celem usunięcia podatności, które mogą być wykorzystane w celu uzyskania nieuprawnionego dostępu;
- ❖ dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora Użytkownika oraz hasła składającego się z 8 znaków zawierających duże i małe litery oraz znaki specjalne.

ROZDZIAŁ IX

PROCEDURA WYKONANIA PRZEGLĄDU I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Przegląd i konserwacja sprzętu informatycznego oraz systemów internetowych w WSPR są realizowane przez Informatyków WSPR oraz upoważnione do tego firmy zewnętrzne.
2. Prace serwisowe sprzętu informatycznego oraz systemów internetowych wykonywane są w miarę możliwości na terenie WSPR, w asyście upoważnionego pracownika WSPR,
3. Część prac serwisowych systemów internetowych realizowana jest w sposób zdalny. Dostęp zdalny mogą uzyskać jedynie uprawnieni pracownicy firm serwisowych, wyłącznie na czas realizacji prac serwisowych.
4. W celu uzyskania do wybranego komputera dostępu, o którym mowa w pkt 3, uprawniony pracownik firmy serwisowej kontaktuje się telefonicznie z Użytkownikiem komputera, u którego zaistniała potrzeba wykonania serwisu podając swoje imię i nazwisko oraz firmę, której jest pracownikiem. Użytkownik komputera w trakcie rozmowy telefonicznej dokonuje zatwierdzenia w systemie operacyjnym dostępu zdalnego.
5. W przypadku pojawienia się wątpliwości, co do tożsamości pracownika firmy serwisowej, który nawiązuje kontakt telefoniczny w celu uzyskania dostępu zdalnego bądź zasadności uzyskania przez niego dostępu, Użytkownik odmawia akceptacji dostępu zdalnego oraz niezwłocznie kontaktuje się z IDO.
6. Po zakończeniu prac serwisowych Użytkownik, o którym mowa w pkt 4 dezaktywuje opcję dostępu zdalnego.

7. Przekazanie sprzętu informatycznego do naprawy bądź konserwacji poza teren WSPR w Olsztynie jest dopuszczalne w wyjątkowych przypadkach, jeżeli spełnione zostaną poniższe warunki:
   - ❖ sprzęt przekazywany uprzednio pozbawiony został nośników zawierających dane osobowe,
   - ❖ fakt przekazania sprzętu do naprawy/konserwacji oraz stwierdzenia braku nośników danych jest potwierdzany protokołem (Wzór protokołu zawiera załącznik nr 3).
8. Wszelkie prace serwisowe związane z dostępem do danych osobowych, wykonywane przez podmioty zewnętrzne odbywają się pod nadzorem upoważnionego pracownika, a ponadto wymagają sporządzenia protokołu serwisowego zawierającego, co najmniej poniższe informacje:
   - ❖ wskazanie osoby przeprowadzającej prace serwisowe oraz firmy, którego osoba ta jest pracownikiem,
   - ❖ wskazanie osoby nadzorującej przebieg prac serwisowych,
   - ❖ przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu),
   - ❖ zakres prac serwisowych i ich wynik,
   - ❖ czas przeprowadzania prac serwisowych.

ROZDZIAŁ X

WYKAZ ZAŁACZNIKÓW

Załącznik nr 1 – Procedura tworzenia kopii zapasowych

Załącznik nr 2 – Dziennik sporządzania kopii

Załącznik nr 3 – Protokół przekazania sprzętu informatycznego do naprawy/konserwacji

Dokument sporządzono:	**Podpis Administratora Danych:**	**Pieczęć**
Data: 30/04/2021 Miejsce: Olsztyn		