Zarządzenie nr 28/2021
Rektora Państwowej Uczelni Zawodowej
im. Ignacego Mościckiego w Ciechanowie
z dnia 12 maja 2021 roku

w sprawie: wprowadzenia Instrukcji Zarządzania Systemami Informatycznymi w Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie

na podstawie:

- art. 23 ust. 2 pkt 2 oraz art. 365 pkt. 5 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (tj. Dz. U. z 2021 r. poz. 478),

- § 37 ust.2 pkt 2 Statutu Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie zarządzam, co następuje:

§1

Wprowadzam Instrukcję Zarządzania Systemami Informatycznymi w Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie, stanowiącą załącznik do Zarządzenia.

§2

Do przestrzegania wprowadzonych regulacji zobowiązani są wszyscy pracownicy/współpracownicy Uczelni.

§ 3

Odpowiedzialnym za nadzór nad przestrzeganiem Instrukcji czynię kierownika Działu Informatycznego.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor

Dr inż. Grzegorz Koc

Załącznik
do Zarządzenia Rektora PUZ im. Ignacego Mościckiego w Ciechanowie
nr 28/2021 z dnia 12.05.2021 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

PAŃSTWOWA UCZELNIA ZAWODOWA im. Ignacego Mościckiego w Ciechanowie

Ciechanów, maj 2021 r.

SPIS TREŚCI

WYKAZ PODSTAWOWYCH SKRÓTÓW

Skrót	Opis
u.o.d.o.	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz. U. 2019 r, poz. 1781 z późn. zm.).
RODO	Rozporządzenie Parlamentu Europejskiego i Radu UE z dnia 27 kwietnią 2016 r. 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
PUODO	Prezes Urzędu Ochrony Danych Osobowych
ADO	Administrator Danych Osobowych
IOD	Inspektor Ochrony Danych
LADO	Lokalny Administrator Bezpieczeństwa Informacji
ASI	Administrator Systemów Informatycznych
SI	System Informatyczny
SBDO	System Bezpieczeństwa Danych Osobowych
IZSI	Instrukcja Zarządzania Systemami Informatycznymi
PUZIM	Państwowa Uczelnia Zawodowa im. Ignacego Mościckiego w Ciechanowie

1. WYKAZ PODSTAWOWYCH DEFINICJI

Ilekroć w niniejszej Instrukcji Zarządzania Systemem Informatycznym mowa o:

1) **Komórce organizacyjnej** – rozumie się przez to odpowiednio wydziały, o których mowa w Regulaminie Organizacyjnym Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie (PUZIM).
2) **Kierowniku komórki organizacyjnej –** rozumie się przez to kierownika i samodzielne stanowiska pracy;
3) **Administratorze Danych Osobowych** – rozumie się przez to Państwową Uczelnię Zawodową im. Ignacego Mościckiego w Ciechanowie, która decyduje o celach i środkach przetwarzania danych osobowych;
4) **Inspektorze Ochrony Danych** – rozumie się przez to pracownika Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie /podmiot zewnętrzny/ wyznaczonego przez Administratora Danych Osobowych, monitorujący przestrzeganie zasad, o których mowa w art. 39 RODO;
5) **Administratorze Systemów Informatycznych** – rozumie się przez to pracownika uczelni, odpowiedzialnego za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów i sieci teleinformatycznych;
6) **Osobie upoważnionej** – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Użytkownikiem może być pracownik PUZIM, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż.
7) **Osobie nieupoważnionej** – rozumie się przez to osobę nieposiadającą upoważnienia do przetwarzania danych osobowych;
8) **Osobie nieuprawnionej** – rozumie się przez to osobę nieposiadającą uprawnień nadanych w systemie informatycznym PUZIM;
9) **Danych osobowych** – rozumie się przez to informacje o zidentyfikowanej, lub możliwej do zidentyfikowania osobie fizycznej (możliwa do zidentyfikowania osoba fizyczna to osoba, którą może bezpośrednio lub pośrednio zidentyfikować), w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

10) **Zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
11) **Przetwarzaniu danych osobowych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adoptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie; przetwarzanie danych zgodne z prawem, rzetelnie i przejrzyste;
12) **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
13) **Zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
14) **Bezpieczeństwie informacji** – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania informacji, by w każdych okolicznościach dostęp do nich był zgodny z założeniami;
15) **Usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
16) **Zgodzie osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda może być odwołana w każdym czasie;
17) **Odbiorcy danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
18) **Państwie trzecim** – rozumie się przez to państwo należące do Europejskiego Obszaru Gospodarczego;

19) **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi uprawnionemu do pracy w systemie informatycznym;
20) **Identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w wyznaczonych przez Administratora Danych Osobowych obszarach systemu informatycznego uczelni;
21) **Teletransmisji danych** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnych;
22) **Poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;
23) **Adekwatności** – rozumie się przez to przetwarzanie danych stosowne lub ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych);
24) **Użytkowniku systemu informatycznego** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w systemach informatycznych, której nadano unikalny identyfikator i hasło;
25) **Uwierzytelnieniu** – rozumie się przez to proces poprawnej identyfikacji użytkownika systemu informatycznego w stopniu umożliwiającym przyznanie odpowiednich uprawnień lub przywilejów w systemie informatycznym uczelni;
26) **Sieci komputerowej** – rozumie się przez to grupę komputerów lub innych urządzeń połączonych ze sobą w celu wymiany danych lub współdzielenia różnych zasobów;
27) **Sieci lokalnej** – rozumie się przez to sieć przeznaczoną do łączenia ze sobą stanowisk komputerowych znajdujących się w uczelni;
28) **Punkcie dystrybucyjnym** – rozumie się przez to miejsce, w którym zlokalizowana jest infrastruktura teleinformatyczna oraz urządzenia umożliwiające dystrybucję połączeń sieciowych w systemie informatycznym;
29) **Stacji roboczej** – rozumie się przez to komputer użytkownika systemu informatycznego podłączony do sieci lokalnej uczelni;
30) **Naruszeniu ochrony danych** – rozumie się przez to naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;
31) **Zagrożeniu** - rozumie się przez to potencjalną możliwość wystąpienia incydentu;
32) **Działaniu korygującym** – rozumie się przez to działanie przeprowadzone w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji;
33) **Działaniu zapobiegawczym** – rozumie się przez to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.

2. WPROWADZENIE

Instrukcja Zarządzania Systemami Informatycznymi opracowana została w celu realizacji przepisów art. 24 RODO, które obligują Administratora danych osobowych do wdrożenia odpowiednich środków technicznych oraz organizacyjnych, aby przetwarzanie odbywało się zgodnie z przepisami RODO.

Niniejsza instrukcja stanowi zestaw procedur opisujących zasady bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych PUZIM.

3. OGÓLNE INFORMACJE O SYSTEMIE INFORMATYCZNYM STOSOWANYM W PUZIM

Funkcjonowanie Państwowej Uczelni Zawodowej w Ciechanowie oparte jest w dużej mierze na systemach informatycznych.

W PUZIM stosowane są następujące systemy IT:

1. Zintegrowany system zarządzani uczelnią SIMPLE, w skład, którego wchodzą:
   a) Simple. ERP – system finansowo kadrowy,
   b) Simple.EDU/Bazus – system obsługi studentów,
   c) WU - Wirtualna Uczelnia – system wirtualnego dziekanatu,
   d) IRK – Internetowa rekrutacja kandydatów.
2. Platforma e-lerningowa Moodle wspomagająca proces zdalnego nauczania.
3. Poczta uczelniana dostępna dla wszystkich pracowników i studentów zintegrowana z usługami Google.
4. System biblioteczny PATRON.
5. System POL-on - Zintegrowana Sieć Informacji o Nauce i Szkolnictwie Wyższym – zewnętrzy system, do którego przekazywane są informacje. W jego skład wchodzi również Ogólnopolskie Repetytorium Pisemnych Prac Dyplomowych – ORPPD.
6. Program Płatnik.

4. ZAKRES STOSOWANIA INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Procedury i zasady określone w niniejszym dokumencie powinny być znane i stosowane przez wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym PUZIM, bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy.

5. ZASADY BEZPIECZNEJ EKSPLOATACJI SYSTEMU INFORMATYCZNEGO

Podstawowym celem zabezpieczeń systemu informatycznego PUZIM jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzanych danych osobowych, które są w nim przetwarzane.

1) W celu zachowania odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych, dostęp do systemu informatycznego przetwarzającego dane osobowe powinien być możliwy wyłącznie po podaniu identyfikatora odrębnego dla każdego użytkownika systemu i poufnego hasła lub innego elementu uwierzytelniającego.
2) Administratora Systemu Informatycznego zapewnia poufność, integralność i rozliczalność danych osobowych przetwarzanych w systemie informatycznym PUZIM.
3) Administratora Systemu Informatycznego zapewnia, aby użytkownicy systemu informatycznego służącego do przetwarzania danych osobowych nie posiadali wyższych poziomów uprawnień w tym systemie niż wymagane jest to do wykonywania powierzonych obowiązków.
4) Prawidłowy poziom zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych zostaje zapewniony poprzez przestrzeganie przez pracowników mających dostęp do systemu IT następujących zasad:
   a) uniemożliwiania osobom trzecim uzyskiwania nieupoważnionego dostępu do systemu informatycznego,
   b) niepodejmowanie przez użytkowników systemu prób wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie, a także poprzez instalowanie nowego lub aktualizowanie już

zainstalowanego oprogramowania,

c) korzystanie z systemu informatycznego dla celów innych niż związane z wykonywaniem obowiązków służbowych jest zabronione.

5) Dostęp do poszczególnych usług systemu informatycznego powinien być chroniony kontrolą dostępu.
6) Przesyłanie danych osobowych drogą teletransmisji odbywa się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń logicznych chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna.
7) Inne technologie sieciowe takie jak sieci lokalne oparte na falach radiowych nie mogą być wykorzystywane do przekazu informacji, o ile połączenie nie jest szyfrowane. Takie połączenia mogą być używane jedynie dla wymiany poczty elektronicznej, o ile wiadomo, że nie zawiera ona danych osobowych.
8) Wszystkie połączenia zewnętrzne do systemu informatycznego powinny być monitorowane Administratora Systemu Informatycznego, a logi połączeń archiwizowane w trybie ciągłym i bezterminowym.
9) Użytkownicy systemu powinni podlegać okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji. Inspektor Ochrony Danych we współpracy z Administratorem Systemów Informatycznych organizują rzeczone szkolenie.

6. ZASADY POSTĘPOWANIA Z KOMPUTERAMI PRZENOŚNYMI

1) Użytkownik systemu informatycznego, używający komputer przenośny zawierający dane osobowe, zobowiązany jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.
2) Użytkownik systemu informatycznego używający komputer przenośny zawierający dane osobowe w szczególności powinien:
   a) stosować ochronnę kryptograficzną;
   b) zabezpieczyć dostęp do komputera przenośnego na poziomie systemu operacyjnego - identyfikator i hasło;
   c) nie zezwalać na używanie komputera przenośnego osobom nieupoważnionym;

d) zachować szczególną ostrożność przy podłączaniu do sieci publicznych.

3) Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego faktyczny użytkownik.

7. PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIE TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Zasady regulujące nadawanie uprawnień do przetwarzania danych oraz rejestrowania uprawnień w systemie informatycznym określono w procedurze (załącznik Nr 1) - „Nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym."

Procedura obowiązuje wszystkie osoby zaangażowane w proces nadawania uprawnień w systemie informatycznym, a w szczególności kierowników komórek organizacyjnych lub bezpośrednich przełożonych użytkowników systemu informatycznego, Administratora Systemu Informatycznego, a także Inspektorem Ochrony Danych.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

8. STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM

Zasady dotyczące stosowanych metod i środków uwierzytelniania w systemie informatycznym PUZIM określono w procedurze - Załącznik Nr 2 - „Stosowane metody i środki uwierzytelniania. Ogólne zasady";

Procedura obowiązuje wszystkie osoby mające uprawnienia do przetwarzania danych osobowych w systemie informatycznym, a także Administratora Systemu Informatycznego.

Inspektor Ochrony Danych jest odpowiedzialny za nadzór nad stosowaniem niniejszych procedur.

9. PROCEDRY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

Zasady dotyczące rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym określono w procedurze (Załącznik Nr 3) - „Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym".

Procedura obowiązuje wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym PUZIM.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

10. PROCEDURY TWORZENIA KOPII ZAPASOWYCH

Zasady dotyczące tworzenia kopii zapasowych zawierających dane osobowe, a także programów i narzędzi wykorzystywanych do przetwarzania danych określono w procedurze (Załącznik Nr 7) - „Tworzenie kopii zapasowych zbiorów danych osobowych".

Procedura obowiązuje Administratora Systemu Informatycznego.

11. SPOSÓB ORAZ MIEJSCE PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI

Zasady dotyczące sposobu, miejsca i okresu przechowywania zarówno elektronicznych nośników informacji, jak i kopii zapasowych zawierających dane osobowe określono w procedurze (Załącznik Nr 4) - „Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych".

Procedura obowiązuje wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym przy użyciu elektronicznych nośników informacji, a także Administratora Systemu Informatycznego.

12. ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO

Zasady dotyczące stosowania profilaktyki antywirusowej określono Załączniku nr 8 - „Zabezpieczenie systemu informatycznego przed działalnością nieuprawnionego oprogramowania”.

Procedura obowiązuje wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym, a także Administratora Systemu Informatycznego.

Inspektor Ochrony Danych jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

13. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW

Przeglądy i konserwacja systemów informatycznych oraz nośników informacji służących do przetwarzania danych przeprowadzane są doraźnie, na zlecenie Administratora Systemu Informatycznego.

ZAŁĄCZNIKI

Załącznik Nr 1 - Nadawanie uprawnień
Załącznik Nr 2 - Metoda uwierzytelniania
Załącznik Nr 3 - Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym
Załącznik Nr 4 - Nośniki informacji
Załącznik Nr 5 - Urządzenie sieciowe
Załącznik Nr 6 - Stacje robocze
Załącznik Nr 7 - Kopie zapasowe
Załącznik Nr 8 - Oprogramowanie szkodliwe

Załącznik nr 1
do Instrukcji Zarządzania Systemami Informatycznymi w PUZ im. Ignacego Mościckiego w Ciechanowie
wprowadzonej
Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie
nr 28 /2021 z dnia 12.05.2021 r.

NADAWANIE UPRAWNIEŃ DO SYSTEMÓW

1. Cel

Określenie zasad zarządzania prawami dostępu dla użytkowników systemu informatycznego oraz administratorów systemu.

2. Zakres obowiązywania

Procedura obowiązuje wszystkie osoby zaangażowane w proces nadawania uprawnień w systemie informatycznym.

3. Opis postępowania

1) W celu zapewnienia wyłącznie prawidłowego i uzasadnionego dostępu do systemu informatycznego oraz dla zapobiegania nieuprawnionemu dostępowi do systemu informatycznego, nadawanie uprawnień do systemów teleinformatycznych odbywa się z uwzględnieniem poniższych zasad:
   a) Pracownikowi mogą być nadane wyłącznie uprawnienia, które są konieczne do realizacji zleconych mu zadań (stosuje się zasadę minimalnych uprawnień, tzn. domyślnie stosuje się brak jakichkolwiek uprawnień).
   b) Uprawnienia do systemu nadawane są przez Administratora Systemów Informatycznych.
   c) Pracownikom nadawane są unikalne identyfikatory. Nazwy kont pracowników muszą zapewniać jednoznaczną identyfikację.
   d) Konta umożliwiające działania administracyjne (np. root, Administrator) muszą zapewniać pełną rozliczalność i identyfikalność działań. W tym celu konta z uprawnieniami administracyjnymi winny być przypisane do konkretnych osób.
   e) Hasła administracyjne ustala Administrator Systemów Informatycznych.
   f) Administrator Systemów Informatycznych jest zobowiązany do prowadzenia metryk haseł administratora.
   g) Wszyscy użytkownicy systemu zobowiązani są do stosowania polityki haseł zgodnie z wytycznymi zawartymi w Instrukcji Zarządzania Systemami Informatycznymi.
   h) Wszelkie zmiany dotyczące użytkownika, takie jak rozwiązanie umowy o pracę lub cofnięcie upoważnienia do przetwarzania danych osobowych są przesłanką do niezwłocznego zablokowania konta użytkownika systemu informatycznego.
   i) Administrator Systemów Informatycznych ma obowiązek okresowej kontroli i weryfikacji zasadności posiadanych przez użytkowników uprawnień. W przypadku braku zasadności, dostęp do systemu powinien zostać niezwłocznie cofnięty.
   j) Nie dopuszcza się tworzenia kont grupowych.

Załącznik nr 2
do Instrukcji Zarządzania Systemami Informatycznymi w PUZ im. Ignacego Mościckiego w Ciechanowie wprowadzonej
Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie
nr 28 /2021 z dnia 12.05.2021 r.

METODY UWIERZYTELNIANIA

1. Cel

Określenie zasad związanych z zarządzaniem identyfikatorami oraz hasłami użytkowników systemu informatycznego.

2. Zakres obowiązywania

Procedura obowiązuje wszystkie osoby mające uprawnienia do przetwarzania danych osobowych w systemie informatycznym.

3. Opis postępowania

1) Pierwsze hasło do systemów nadaje Administrator Systemów Informatycznych. Nadzoruje on również obowiązek zmiany hasła, co 30 dni, dokonywane przez użytkownika.
2) Wymagania odnośnie tworzenia i używania haseł i identyfikatorów:
   a) Hasło musi zawierać nie mniej niż 8 znaków.
   b) Hasło musi składać się z liter (małych i dużych) oraz cyfr i znaków specjalnych.
   c) Hasło musi być zmieniane nie rzadziej niż raz na 30 dni.
   d) Hasła nie mogą być ujawniane innym osobom.
   e) Hasła do różnych systemów powinny być różne, za wyjątkiem sytuacji, gdy jest możliwe zastosowanie mechanizmu jednokrotnego logowania.
   f) Hasła nie mogą być przechowywane w czytelnej postaci (jako tekst w pliku jak i zapisane na papierze).
   g) Hasło powinno zostać niezwłocznie zmienione w przypadku ujawnienia lub podejrzenia ujawnienia osobie nieuprawnionej.
   h) Hasła tymczasowe lub startowe powinny być zmienione po pierwszym logowaniu.
   i) Hasła domyślne tzw. defaultowe powinny być niezwłocznie zmienione.
   j) W przypadku zakończenia świadczenia pracy lub odbiorze upoważnienia do przetwarzania danych, konto użytkownika powinno zostać niezwłocznie zablokowane.
   k) Identyfikator raz użyty nie może być wykorzystywany ponownie.
   l) Hasła wykorzystywane w systemach informatycznych organizacji nie mogą być używane w innych miejscach np. do zabezpieczania zasobów prywatnych użytkownika.
   m) Hasła powinny być trudne do odgadnięcia (zaleca się nie stosować nazw potocznych, imion, nazwisk, dat urodzenia, numerów dokumentów, innych danych osobistych oraz standardowych kombinacji znaków, np. 12345678).
   n) 3-krotna błędna próba wprowadzenia hasła powinna skutkować zablokowaniem konta użytkownika oraz odpowiednią adnotacją w systemie .
   o) Hasła nie powinny być tworzone według stałego schematu, np.: Kowal_01, Kowal_02 itp.

p) Hasła powinny być wprowadzane w sposób maskowany.

q) Powinna zostać tworzona historia haseł (przynajmniej 10 wstecz) w celu zablokowania ich powtarzania.

ROZPOCZĘCIE, ZAWIESZENIE I ZAKOŃCZENIE PRACY W SYSTEMIE INFORMATYCZNYM

1. Cel

Określenie zasad dotyczących postępowania zapewniającego bezpieczeństwo danych osobowych w systemie informatycznym.

2. Zakres obowiązywania

Procedura obowiązuje wszystkich użytkowników upoważnionych do przetwarzania danych osobowych w systemie informatycznym.

3. Opis postępowania

1) Stosowane są następujące zasady rozpoczęcia pracy w systemie informatycznym:
   a) Przed przystąpieniem do pracy, użytkownik zobowiązany jest do sprawdzenia czy stacja robocza wykorzystywana do przetwarzania danych osobowych w systemie informatycznym nie wskazuje na ingerencję osób trzecich, a także czy stanowisko pracy zastano w takim stanie jak pozostawiono po zakończeniu pracy.
   b) Przed uruchomieniem stacji roboczej, użytkownik zobowiązany jest do upewnienia się, czy ekran monitora jest ustawiony w sposób uniemożliwiający osobom nieupoważnionym podglądnięcie jego zawartości.
   c) Każde rozpoczęcie pracy w danym systemie wymaga logowania.
   d) W trakcie pracy, użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych.
   e) W trakcie pracy, użytkownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych.
2) Stosowane są następujące zasady zawieszenia pracy w systemie informatycznym:
   a) W przypadku chwilowego opuszczenia stanowiska pracy użytkownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane.
   b) W przypadku opuszczenia stanowiska pracy materiały zawierające dane wymagające ochrony powinny być zabezpieczane przed dostępem osób nieuprawnionych.
   c) W przypadku bezczynności użytkownika na stacji roboczej trwającej więcej niż 10 min, uruchamiany jest automatycznie wygaszacz ekranu. Wznowienie pracy możliwe jest po ponownym uwierzytelnieniu się poprzez podanie własnego hasła.
3) Stosowane są następujące zasady zakończenia pracy w systemie informatycznym:
   a) Po zakończeniu pracy należy wylogować się z systemu.
   b) Po zakończeniu dnia pracy użytkownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających dane osobowe, w celu uniemożliwienia dostępu do nich osób nieupoważnionych. Należy uprzątnąć z miejsca pracy wszelkie dokumenty, nośniki, notatki i umieścić je w miejscu niedostępnym dla osób nieupoważnionych.

NOŚNIKI INFORMACJI

1. Cel

Określenie zasad dotyczących postępowania zapewniającego bezpieczeństwo nośników informacji zawierających dane osobowe.

2. Uczestnicy

Procedura obowiązuje wszystkich użytkowników upoważnionych do przetwarzania danych osobowych w systemie informatycznym.

3. Opis postępowania

1) Przekazywanie, niszczenie nośników zawierających dane osobowe:
   a) Nośniki danych przeznaczone do likwidacji należy wcześniej pozbawiać zapisanych danych w sposób uniemożliwiający ich odzyskanie lub uszkodzone, w taki sposób, aby odczyt danych stał się niemożliwy.
   b) Z urządzeń i/lub nośników danych zawierających dane osobowe przed przekazaniem podmiotowi nieuprawnionemu należy te dane usunąć w sposób trwały, uniemożliwiający późniejsze ich odczytanie/odtworzenie.
   c) Z urządzeń i/lub nośników danych zawierających dane osobowe przed przekazaniem do naprawy należy usunąć te dane w sposób trwały uniemożliwiający późniejsze odczytanie/odtworzenie lub naprawiać w obecności osoby upoważnionej.
   d) Dopuszcza się przekazanie nośników danych bez usunięcia danych osobowych jedynie w przypadku przekazywania ich specjalistycznej firmie w celu odzyskania danych i po uzyskaniu zgody Inspektora Ochrony Danych oraz podpisania umowy powierzenia danych osobowych.
   e) Transport nośników zawierających dane osobowe poza granice obszarów przetwarzania firmy powinien być dokonywany w sposób uniemożliwiający uzyskanie dostępu do nich przez osoby nieuprawnione (szyfrowanie).
   f) Transport nośników zawierających dane osobowe poza granice obszarów przetwarzania firmy powinien być dokonywany z zachowaniem szczególnej uwagi tak, aby nośnik informacji nie został zgubiony, skradziony lub uszkodzony. W przypadku zlecania transportu nośników danych należy korzystać z godnego zaufania transportu i kurierów.
   g) Zabrania się wynoszenia nośników danych poza obszar zidentyfikowany, jako obszar przetwarzania danych bez zgody Administratora Bezpieczeństwa Informacji.

2) Przechowywanie nośników danych:
   a) W przypadku przechowywania danych osobowych (nośników) poza obszarem wyznaczonym, jako obszar przetwarzania danych osobowych, dane te powinny być zabezpieczone środkami dodatkowymi w celu zachowania poufności i integralności (szyfrowanie).

b) Nośniki danych (w tym również kopie zapasowe i archiwalne) należy przechowywać w wydzielonym pomieszczeniu i/lub szafie/sejfie w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.

c) Kopie zapasowe usuwa się (niszczy) niezwłocznie po ustaniu ich użyteczności.

d) W przypadku, jeśli dostęp do nośników ma więcej niż jedna osoba zaleca się, aby wprowadzony system kontroli dostępu zapewniał identyfikacje, autoryzację oraz rozliczalność osoby.

URZĄDZENIA SIECIOWE

1. Cel

Określenie zasad dotyczących środowiska i warunków pracy urządzeń sieciowych, serwerów i stacji roboczych wykorzystywanych w firmie.

2. Zakres obowiązywania

Procedura obowiązuje Administratora Systemów Informatycznych.

3. Opis postępowania

1) Urządzenia sieciowe i serwerowe:
   a) Urządzenia są zainstalowane w szafie teleinformatycznej.
   b) Szafa teleinformatyczna chroniona jest przed dostępem osób nieuprawnionych.
   c) Urządzenia należy tak instalować, aby był możliwy swobodny obieg powietrza zgodnie ze ścieżką chłodzenia przewidzianą przez producenta w każdym z urządzeń.
   d) W pomieszczeniu zapewniona jest odpowiednia temperatura powietrza zgodnie z wytycznymi producenta urządzenia.
   e) W pomieszczeniu zapewniona jest odpowiednia wilgotność powietrza zgodnie z wytycznymi producenta urządzenia.
   f) Urządzenia powinny być tak zainstalowane, aby był do nich możliwy swobodny dostęp fizyczny dla osób uprawnionych na potrzeby wykonywania czynności przeglądowo-naprawczych.
   g) Okablowanie powinno być uporządkowane w sposób maksymalnie ograniczający możliwość przypadkowego rozłączenia oraz opisane umożliwiając łatwą identyfikację.
   h) Urządzenia powinny być podłączone pod system zasilania awaryjnego umożliwiający (przynajmniej) podtrzymanie zasilania na czas niezbędny do bezpiecznego wyłączenia urządzeń .
   i) Infrastruktura sieciowa (okablowanie) powinna być poprowadzona torami bezpiecznymi tzn. podtynkowo, torem ziemnym lub na ścianie w odpowiednich korytach/rurach montażowych zapewniających ochronę przed uszkodzeniem oraz podsłuchem.
   j) W przypadku, gdy gniazdko sieciowe jest niewykorzystywane wówczas zakończenie połączenia po stronie dostępowej powinno być fizycznie odłączone od urządzeń aktywnych.
2) Stacje robocze:
   b) Stacje robocze muszą być tak zainstalowane, aby był możliwy swobodny obieg powietrza zgodnie ze ścieżką chłodzenia przewidzianą przez producenta w każdym z urządzeń.
   c) Musi zostać zapewniona odpowiednia temperatura i wilgotność powietrza zgodnie z wytycznymi producenta urządzenia przy zachowaniu norm przewidzianych dla warunków świadczenia pracy (odpowiednie przepisy BHP).
   d) Stacje robocze powinny być tak zainstalowane, aby uniemożliwić dostęp osobom nieuprawnionym.

e) Stacje robocze powinny być tak zainstalowane, aby uniemożliwić osobom nieuprawnionym podgląd ekranu.
f) Stacje robocze powinny być tak zainstalowane, aby zabezpieczyć je przed zalaniem lub działaniem kurzu.
g) Urządzenia (monitor, klawiatura, mysz, czytnik kart) powinny być tak zainstalowane, aby był do nich możliwy swobodny dostęp fizyczny zapewniający wygodę oraz ergonomię pracy.
h) Okablowanie powinno być uporządkowane w sposób maksymalnie ograniczający możliwość przypadkowego (lub umyślnego – przez osoby nieuprawnione) rozłączenia.

STACJE ROBOCZE

1. Cel

Określenie zasad dotyczących konfiguracji stacji roboczych.

2. Zakres obowiązywania

Procedura obowiązuje Administratora Systemów Informatycznych.

3. Opis postępowania

1) Użytkownik nie posiada praw administracyjnych do stacji roboczej.
2) Dostęp do BIOS jest chroniony hasłem.
3) Stacje robocze używane w systemie informatycznym firmy są wyposażone w oprogramowanie systemowe Microsoft Windows, dla którego wymaga się:
   a) Wykonywania aktualizacji systemu operacyjnego zgodnie z zaleceniami producenta. Aktualizacje należy instalować również dla innych wykorzystywanych aplikacji.
   b) Wyłączenia możliwości korzystania z pulpitu zdalnego o ile nie jest wykorzystywany. W przeciwnym przypadku dostęp należy zawęzić do uprawnionych użytkowników oraz uprawnionych źródeł.
   c) Włączenia wygaszacza ekranu z hasłem uruchamianego automatycznie po zdefiniowanym okresie czasu. Czas należy dobrać indywidualnie tak, aby nie obniżać komfortu pracy użytkowników. Nie powinien on być jednak dłuższy niż 10 minut bezczynności.
   d) Ustawienia konta użytkownika na potrzeby normalnej pracy z systemem z ograniczeniem uprawnień do minimum.
   e) W przypadku korzystania z jednej stacji roboczej przez dwóch lub więcej użytkowników wymaga się stosowania systemu identyfikatorów zapewniających rozliczalność (identyfikator raz użyty nie może być powtórnie wykorzystany przez innego użytkownika).
   f) Włączenia i skonfigurowania zapory systemowej poprzez ustawienie możliwości komunikacji tylko niezbędnych aplikacji dla poprawnego działania systemu.
   g) Dostosowania do polityki haseł.
   h) Ograniczenie dostępu do dzienników zdarzeń tylko dla kont administratora oraz systemowych.
   i) Wyłączenie autologowania.
   j) Zablokowanie możliwości korzystania z przenośnych nośników danych (np: pamięci USB, płyt CD i DVD) w zakresie, w jakim to jest możliwe.

Załącznik nr 7
do Instrukcji Zarządzania Systemami Informatycznymi w PUZ im. Ignacego Mościckiego w Ciechanowie wprowadzonej
Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie
nr 28/2021 z dnia 12.05.2021 r.

KOPIE ZAPASOWE

1. Cel

Określenie zasad dotyczących wykonywania kopii zapasowych.

2. Uczestnicy

Procedura obowiązuje użytkowników systemów informatycznych

3. Opis postępowania

1) Wszystkie dane osobowe przetwarzane w systemie informatycznym są zachowywane w kopiach zapasowych w serwerowni.

2) Kopie zapasowe tworzy się w taki sposób, aby zapewnić odtworzenie wszystkich informacji w przypadku awarii. Administrator Systemu Informatycznego nadzoruje prawidłowość procesu tworzenia kopii zapasowych.

3) Kopią zapasową objęty jest system ERP.

4) Kopie zapasowe tworzone są na serwerze oraz dysku kopii zapasowych NAS, do którego dostęp ma wyłącznie Administrator Systemu Informatycznego (ASI).

5) W celu zweryfikowania poprawności danych przechowywanych na kopiach zapasowych oraz możliwości przywrócenia za ich pomocą systemu do stanu sprzed awarii, Administrator Systemu Informatycznego zobowiązany jest do wykonywania okresowych testów odtworzenia kopii zapasowych. Wyniki testów powinny zostać udokumentowane.

Załącznik nr 8
do Instrukcji Zarządzania Systemami Informatycznymi w PUZ im. Ignacego Mościckiego w Ciechanowie
wprowadzonej
Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie
nr 28/2021 z dnia 12 .05.2021 r..

OPROGRAMOWANIE SZKODLIWE

1. Cel

Określenie zasad dotyczących zabezpieczenia systemu informatycznego przed działalnością nieuprawnionego oprogramowania.

2. Zakres obowiązywania

Procedura obowiązuje wszystkich użytkowników upoważnionych do przetwarzania danych w systemie informatycznym oraz Administratora Systemów Informatycznych.

3. Opis postępowania

1) Administrator Systemów Informatycznych jest zobowiązany do wprowadzenia obligatoryjnej ochrony antywirusowej, a także zabezpieczenia zaporą sieciową, która obejmuje wszystkie stacje robocze oraz serwery.

2) Oprogramowanie antywirusowe powinno być skonfigurowane w sposób wymuszający automatyczne usuwanie wirusów, zaś w przypadku, gdy ich usunięcie jest niemożliwe, obejmowanie ich kwarantanną, okresowe skanowanie wszystkich dysków lokalnych, a także sporządzanie raportów oraz powiadamianie osoby odpowiedzialnej o wykrytych wirusach, „robakach" czy innym szkodliwym oprogramowaniu.

3) Dokonywanie zmian w konfiguracji oprogramowania antywirusowego oraz zapory sieciowej jest możliwe tylko przez Administratora Systemów Informatycznych.

4) Przeprowadzane są okresowe szkolenia z zakresu bezpiecznej pracy z aplikacjami wykorzystywanymi na stacjach roboczych ze szczególnym uwzględnieniem aplikacji wykorzystywanych do łączności z sieciami zewnętrznymi (np: przeglądarka internetowa, klient poczty itp.). Szkolenia powinny uświadamiać użytkownikom skalę i typy zagrożeń oraz metody jak ich uniknąć lub obniżyć prawdopodobieństwo infekcji. Inspektor Ochrony Danych we współpracy z Administratorem Systemów Informatycznych organizują rzeczone szkolenie.

5) Bezpieczeństwo pracy z aplikacjami nadzoruje Administrator Systemów Informatycznych.

6) Użytkownicy zobowiązani są do sprawdzania programem antywirusowym wszelkich elektronicznych zewnętrznych nośników informacji.