Zarządzenie Nr 8c /2019
Dyrektora Powiatowego Centrum Pomocy Rodzinie w Łowiczu
z dnia 11 lutego 2019 roku
w sprawie **wprowadzenia Instrukcji Zarządzania Systemem Informatyczny służącym do przetwarzania danych osobowych w Powiatowym Centrum Pomocy Rodzinie w Łowiczu**

Na podstawie art. 24 ust 2 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 (ogólne rozporządzenie o ochronie danych osobowych), § 20 ust. 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), oraz § 18 pkt. 11 Regulaminu Organizacyjnego Powiatowego Centrum Pomocy Rodzinie w Łowiczu stanowiącego załącznik do Uchwały Nr 761/2018 r. z dnia 30 maja 2018 roku Zarządu Powiatu Łowickiego zarządzam, co następuje:

§ 1

Wprowadzam w Powiatowym Centrum Pomocy Rodzinie w Łowiczu dokument o nazwie Instrukcja Zarzadzania Systemem Informatycznym służącym do przetwarzania danych osobowych Załącznik Nr 1 do Zarządzenia.

§ 2

Uchyla się Zarządzenie Nr 22/2018 Dyrektora Powiatowego Centrum Pomocy Rodzinie w Łowiczu z dnia 01 października 2019 roku w sprawie zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych w Powiatowym Centrum Pomocy Rodzinie w Łowiczu.

§ 3

Każdy pracownik zgodnie z wykazem, jest obowiązany zapoznać się z treścią Załącznika Nr 1.

§ 4

Dyrektor zobowiązuje wszystkich pracowników do przestrzegania Instrukcji Zarządzania Systemem Informatycznym pod groźbą konsekwencji służbowych, przewidzianych prawem.

§ 5

Wykonanie zarządzenia powierzam Administratorowi Systemów Informatycznych w PCPR w Łowiczu.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

p.o. DYREKTORA
Powiatowego Centrum Pomocy Rodzinie
w Łowiczu
Justyna Haczykowska - Kotlarska

RADCA PRAWNY
Joanna Bociąga

Załącznik Nr 1 ·
do Zarządzenia Nr 8c/2019 r.
z dnia 11 lutego 2019 roku
Dyrektora PCPR w Łowiczu

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM
INFORMATYCZNYM SŁUŻĄCYM
DO PRZETWARZANIA DANYCH OSOBOWYCH

Rozdzielnik:	Dokument do użytku wewnętrznego
Podmiot:	Powiatowe Centrum Pomocy Rodzinie w Łowiczu 99-400 Łowicz, ul. Podrzeczna 30
Wersja:	Nr 2
z dnia:	11 lutego 2019 roku
Zatwierdził:	p.o. DYREKTORA Powiatowego Centrum Pomocy Rodzinie w Łowiczu Justyna Haczykowska - Kollarska ..... Podpis administratora danych

Spis treści **Nr strony**

I. WPROWADZENIE

Niniejszy dokument stanowi Instrukcję zarządzania systemem Informatycznym służącym do przetwarzania danych osobowych w Powiatowym Centrum Pomocy Rodzinie w Łowiczu zwany dalej Instrukcją, wypełnieniem obowiązku wynikającego z art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 lub RODO), § 20 ust. 1 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. z 2017 r. poz. 2247), oraz § 18 pkt. 11 Regulaminu Organizacyjnego Powiatowego Centrum Pomocy Rodzinie w Łowicz.

Instrukcja określa sposób zarządzania Systemem informatycznym w PCPR w Łowiczu w celu zabezpieczenia zgromadzonych w nim danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

Do stosowania postanowień Instrukcji obowiązani są wszyscy pracownicy jak i inne osoby, które przetwarzają dane osobowe w systemie informatycznym PCPR w Łowiczu.

Przed przystąpieniem do pracy przez pracownika lub innej osoby zatrudnionej w jednostce obowiązkowe jest zapoznanie się z regulacjami dotyczącymi przetwarzania danych w PCPR w Łowiczu, w szczególności z:

1) Polityką Bezpieczeństwa Informacji;
2) Instrukcją Zarządzania Systemem Informatycznym;
3) Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych.

Fakt zapoznania się z regulacjami, o których mowa powyżej, potwierdzany jest poprzez podpisanie oświadczenia o zachowaniu poufności informacji uzyskiwanych w związku z przetwarzaniem danych osobowych oraz zapoznaniu się z zasadami przetwarzania danych. Oświadczenie takie stanowi załącznik nr 1 do Polityki Bezpieczeństwa Informacji.

Instrukcja określa zasady zarządzania Systemem informatycznym w PCPR w Łowiczu służącym do przetwarzania danych osobowych, a w szczególności:

1) nadawanie i cofanie uprawnień do przetwarzania danych w systemach informatycznych;
2) wymogi oraz sposób użytkowania haseł w systemie informatycznym;
3) rozpoczęcie, zawieszenie i zakończenie pracy w Systemie informatycznym;
4) tworzenie kopii zapasowych danych oraz programów i narzędzi programowych służących do przetwarzania danych osobowych w systemie informatycznym;
5) sposoby zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania oraz dostępem do nich osób nieupoważnionych;
6) wykonywanie przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych;
7) eksploatacja sprzętu i oprogramowania wchodzącego w skład systemu informatycznego

8) zarzadzanie systemem informatycznym w przypadkach awaryjnych;
9) postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa Systemu informatycznego.

Definicje

1. **RODO** - 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).
2. **Ustawa** - rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych.
3. **Rozporządzenie** – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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. z 2004 r. Nr 100, poz. 1024).
4. **PCPR w Łowiczu** – Powiatowe Centrum Pomocy Rodzinie w Łowiczu.
5. **Administrator Danych Osobowych – Administrator lub ADO** - Powiatowe Centrum Pomocy Rodzinie w Łowiczu, reprezentowanie przez Dyrektora.
6. **Inspektor Ochrony Danych – Inspektor lub IOD** - osoba powołana przez administratora danych oraz zarejestrowana w Urzędzie Ochrony Danych Osobowych w celu zapewnienia prawidłowości przetwarzanych danych w PCPR w Łowiczu.
7. **Administrator Systemów Informatycznych - ASI** - pracownik lub podmiot zewnętrzny odpowiedzialny za prawidłową pracę systemów informatycznych.
8. **Użytkownik/pracownik** - osoba przetwarzająca dane w systemie oraz poza nim (np. dokumentacji w formie tradycyjnej), niezależnie od formy zatrudnienia w PCPR w Łowiczu lub formy prawnej wiążącej z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie podpisanej umowy cywilnoprawnej.
9. **Osoba upoważniona do przetwarzania danych osobowych** - osoba, która upoważniona została do przetwarzania danych osobowych przez ADO na piśmie.
10. **Identyfikator** - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
11. **Hasło** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi.
12. **Instrukcja** - rozumie się przez niniejszą Instrukcję Zarządzania Systemem Informatycznym.
13. **Polityka** – rozumie się przez to Politykę Bezpieczeństwa Informacji wprowadzoną w PCPR w Łowiczu.
14. **Zbiór danych** - to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
15. **Odbiorcy danych** - osoba fizyczna lub prawna, organ publiczny, jednostka 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 powszechnie obowiązującym, 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. Przy czym przez sformułowanie „strona trzecia" rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia Administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe.

16. **Dane osobowe lub dane** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można 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.
17. **Przetwarzanie danych** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
18. **Systemie informatycznym / System** - sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych. W systemie tym pracuje, co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną ADO.
19. **Bezpieczeństwo informacji** - stan, w którym informacja jest chroniona przed wieloma różnymi zagrożeniami w taki sposób, aby zapewnić ciągłość prowadzenia działalności, zminimalizować straty i maksymalizować zwrot nakładów na inwestycje i działania o charakterze biznesowym; niezależnie od tego, jaką formę informacja przybiera lub za pomocą, jakich środków jest udostępniana lub przechowywana, zawsze powinna być w odpowiedni sposób chroniona; bezpieczeństwo informacji oznacza w szczególności zachowanie: poufności, integralności, dostępności i rozliczalności.
20. **Kopia bezpieczeństwa** - kopie plików danych lub plików programowania tworzone na nośnikach wymiennych lub dysku twardym komputera w celu ich odtworzenia w przypadku utraty lub uszkodzenia danych.
21. **Przetwarzający dane** - podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy, zgodnie z art. 28 RODO.
22. **Uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
23. **Usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
24. **Trwałe usunięcie informacji** - sposób postępowania z nośnikiem informacji mający na celu usunięcie zapisanych na nim informacji tak, aby ich odtworzenie w całości lub w części było niemożliwe.

25. **Raport** - przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych.
26. **Serwisant** - firma lub pracownik firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego.

II. POZIOM BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

W związku z tym, iż system informatyczny obsługujący PCPR w Łowiczu połączony jest z siecią publiczną, zapewnia się **wysoki poziom bezpieczeństwa** przetwarzania danych osobowych w systemach informatycznych/aplikacjach/programach.

III. NADAWANIE I COFANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMACH INFORMATYCZNYCH

1. Za bezpieczeństwo danych w systemie informatycznym w PCPR w Łowiczu odpowiedzialny jest Administrator Systemów Informatycznych ASI.
2. ASI odpowiada za nadawanie, modyfikowanie i usuwanie uprawnień użytkownika do przetwarzania danych osobowych w systemach informatycznych, a także za rejestrowanie takich uprawnień w tymże systemie.
3. Uprawnienia dla nowego użytkownika mogą być nadane wyłącznie osobie upoważnionej do przetwarzana danych osobowych zgodnie z Polityką.
4. Każdemu Użytkownikowi ASI przyznaje unikalny identyfikator.
5. Identyfikator Użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
6. Dostęp do Systemu informatycznego ma być możliwy wyłącznie po wprowadzeniu identyfikatora użytkownika i dokonaniu uwierzytelnienia.
7. Jako identyfikatora użytkownika możliwe jest zastosowanie certyfikatu umieszczonego na karcie elektronicznej (karta kryptograficzna, chipowa, zbliżeniowa).
8. W przypadku cofnięcia upoważnienia dla użytkownika do korzystania z Systemu informatycznego (w tym cofnięcia upoważnienia do przetwarzania danych osobowych) ASI zobowiązany jest do unieważnienia i zablokowania identyfikatora i hasła wyrejestrowanego użytkownika oraz podejmnje inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych dostępu.
9. ASI może zablokować użytkownikowi dostęp do systemu informatycznego w każdym czasie, jeśli uzna to za konieczne dla zapewnienia bezpieczeństwa danych osobowych.
10. Po zakończeniu pracy w systemie informatycznym, Użytkownik zobowiązany jest wylogować się z systemu.

IV. WYMOGI ORAZ SPOSÓB UŻYTKOWANIA HASEŁ W SYSTEMIE INFORMATYCZNYM

1. Za bezpieczeństwo danych w systemie informatycznym w PCPR w Łowiczu odpowiedzialny jest Administrator systemów informatycznych ASI.
2. Hasło jest obowiązkowe dla każdego użytkownika posiadającego identyfikator użytkownika w Systemie informatycznym.
3. Po założeniu lub zmianie hasła przez ASI użytkownik ma obowiązek zarejestrować się do Systemu informatycznego i zmienić hasło.
4. Hasło składa się minimalnie z 8 znaków, które nie powinny być łatwe do zidentyfikowania (nie należy używać jako hasła np.: imion, nazwisk, daty urodzenia, identyfikatora w systemie informatycznym, wyrazów lub cyfr będących danymi osobowymi użytkownika lub dotyczących zbioru danych).
5. Hasło powinno się składać z małych i wielkich liter, cyfr oraz co najmniej jednego znaku specjalnego.
6. Hasła nie należy nigdzie zapisywać.
7. W przypadku ujawnienia hasła musi ono zostać niezwłocznie zmienione, a niniejszy incydent zgłoszony do ASI.
8. Zmiana hasła następuje nie rzadziej, niż co 30 dni.
9. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
10. Użytkownik, który utracił hasło, zobowiązany jest zgłosić to niezwłocznie ASI, który ustali nowe hasło.

V. PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY DLA UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika lub ASI.
3. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), a także wydruki i dokumenty leżące na biurkach oraz w otwartych szafach.
4. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
   1) uruchamia komputer;
   2) uwierzytelnienia się (logowania) w systemie informatycznym za pomocą swojego identyfikatora i hasła;
   3) uwierzytelnienia się (logowania) w ramach bazy danych.

5. Niedopuszczalne jest logowanie się z wykorzystaniem identyfikatora i hasła innego użytkownika.
6. Przy opuszczaniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy uniemożliwić osobom nieuprawnionym dostęp do systemu informatycznego, np. poprzez zastosowanie wygaszacza ekranu wymagającego podania hasła lub poprzez wylogowanie się z Systemu.
7. Każdorazowa zmiana użytkownika stacji roboczej musi poprzedzać wylogowanie się użytkownika, który poprzednio z niej korzystał.
8. Zakończenie przez użytkownika pracy w systemie informatycznym następuje po wylogowaniu się z Systemu i wyłączeniu zasilania komputera.
9. Po zakończeniu pracy użytkownik zobowiązany jest zabezpieczyć swoje stanowisko pracy, w szczególności informatyczne nośniki danych, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych oraz wyłączyć komputer.

VI. TWORZENIE KOPII ZAPASOWYCH DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZECHOWYWANIA

Kopie zapasowe

1. W celu zwiększenia poziomu bezpieczeństwa oraz zapewnienia ciągłości działania jednostki tworzy się regularnie zgodnie z harmonogramem kopie zapasowe danych.
2. Za tworzenie kopii zapasowych i archiwalnych odpowiedzialny jest ASI.
3. Kopie zapasowe tworzy się wykorzystując narzędzia programowe oraz narzędzia systemu.
4. W systemie informatycznym wykorzystującym technologię klient-serwer kopie zapasowe wykonuje się po stronie serwera.
5. Dostęp do kopii bezpieczeństwa ma tylko ASI.
6. Pozostałe kopie tworzy się na oddzielnych nośnikach informatycznych.
7. Nośniki zawierające kopie zapasowe należy odpowiednio oznaczyć "Kopia zapasowa dzienna/tygodniowa/miesięczna" wraz z podaniem daty sporządzenia.
8. Kopie ulegają niezwłocznie zniszczeniu w sposób uniemożliwiający ich użycie, jeżeli zostanie stwierdzona ich nieprzydatność albo pojawią się okoliczności wyłączające legalność archiwizowania danych.

Kopie archiwalne

1. Zbiory danych, oprogramowanie oraz konfiguracja systemów operacyjnych serwerów Administratora powinny być zabezpieczone w postaci cyklicznie wykonywanych kopii bezpieczeństwa lub archiwalnych.

2. Kopie bezpieczeństwa należy wykonać:
   1) przed dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania;
   2) przed dokonaniem zmian w programach – np. zmiana wersji;
   3) przed i po każdej istotnej zmianie danych w bazie danych;
   4) w co najmniej dwóch egzemplarzach i przechowywać do czasu wykonania nowszej kopii.
3. Kopie archiwalne należy wykonywać:
   1) miesięczne – na koniec danego miesiąca;
   2) roczne – na koniec danego roku;
   3) w co najmniej dwóch egzemplarzach i przechowywać przez okres roku licząc od dnia ich wykonania
4. Pliki użytkowników systemu informatycznego powinny być przechowywane na indywidualnie udostępnionych dyskach serwerów.
5. Dyski serwerów, d których tu mowa zabezpiecza się przed utrata danych w postaci kopii bezpieczeństwa lub kopii archiwalnej.

Nośniki danych wykorzystywane do sporządzania kopii zapasowych

1. Kopie zapasowe baz danych są nagrywane na zewnętrzne nośniki, takie jak:
   1) pamięć USB;
   2) płyty CD/DVD;
   3) zewnętrzne dyski pamięci.
2. Nośniki zawierające kopie zapasowe należy oznaczać, jako "Kopia zapasowa dzienna/tygodniowa/miesięczna" wraz z podaniem daty sporządzenia.

Sposób i miejsce przechowywania kopii zapasowych i archiwalnych

1. Wszystkie nośniki bez względu na ieh rodzaj są zabezpieczane przed nieautoryzowaną zmianą, zniszczeniem i dostępem.
2. Nośniki z kopiami archiwalnymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, przed zniszczeniem czy kradzieżą w zamykanych szafach metalowych.
3. Nośników z danymi zarchiwizowanymi nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych używane na bieżąco.
4. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
5. Nośniki danych oraz kopie, które są już nieprzydatne, należy zniszczyć fizycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane.
6. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.

7. Zabrania się wynoszenia jakichkolwiek nagranych nośników zawierających dane osobowe z miejsca pracy bez zgody ASI lub IDO.

VII. SPOSOBY ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ SZKODLIWEGO OPROGRAMOWANIA ORAZ DOSTĘPEM DO NICH OSÓB NIEUPOWAŻNIONYCH

1. W jednostce istnieje bezwzględny wymóg instalacji oprogramowania antywirusowego oraz zapory (firewall) na każdym stanowisku roboczym, zarówno na komputerach stacjonarnych, jak i przenośnych wykorzystywanych do przetwarzania danych.
2. Oprogramowanie antywirusowe uruchamiane jest przy starcie systemu i sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami a użytkownik nie posiada uprawnień do jego wyłączenia.
3. Niezależnie od ciągłego nadzoru, ASI okresowo przeprowadza pełną kontrolę obecności wirusów komputerowych w całym systemie Administratora w tym również na urządzeniach przenośnych.
4. Za prawidłowe funkcjonowanie oprogramowania antywirusowego odpowiada ASI.
5. Użytkownik jest obowiązany zawiadomić ASI o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
6. Do obowiązków ASI należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.
7. Niedopuszczalne jest otwieranie plików pobranych z Internetu lub korzystania z zewnętrznych nośników bez uprzedniego przeskanowania zawartości nośnika przez program antywirusowy.
8. Przesyłanie danych osobowych pocztą elektroniczną dopuszczalne jest tylko w plikach zabezpieczonych hasłem i w postaci zaszyfrowanej.

VIII. WYKONYWANIE PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Przegląd i konserwacja urządzeń systemu winna być dokonywana zgodnie z zaleceniami producenta nie rzadziej, niż co 12 miesięcy.
2. Przeglądu i konserwacji systemu dokonuje doraźnie ASI, który odpowiedzialny jest za terminowość i rzetelność przeglądów i konserwacji urządzeń.
3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale ASI nie rzadziej niż raz na miesiąc.

4. Zapisy logów systemowych powinny być przeglądane każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.
5. Kontrole i przeprowadzane testy powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.
6. Wszelkie nieprawidłowości wykryte w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny oraz okoliczności sprzyjające przeanalizowane. O ile to możliwe, stosuje się odpowiednie środki w celu zapobieżenia występowaniu nieprawidłowości w przyszłości.
7. Przegląd programów i narzędzi przeprowadzany jest w przypadku zmiany wersji oprogramowania, zmiany systemu operacyjnego chyba, że zmiany te wynikają z aktualizacji automatycznej.

IX. ZASADY EKSPLOATACJI SPRZĘTU I OPROGRAMOWANIA WCHODZĄCEGO W SKŁAD SYSTEMU INFORMATYCZNEGO

Skład Systemu informatycznego

1. Na System informatyczny w PCPR w Łowiczu składają się:
   1) komputery stacjonarne - PC;
   2) komputery przenośne – laptopy;
   3) tablety;
   4) smartfony;
   5) drukarki i urządzenia wielofunkcyjne;
   6) modemy;
   7) monitory;
   8) switche;
   9) routery;
   10) osprzęt: zasilacze, torby, klawiatury, myszki komputerowe.
2. Za prawidłowe działanie sprzętu komputerowego odpowiada ASI. Nadzór nad tym sprzętem może wykonywać sam lub poprzez podmioty zewnętrzne.
3. W przypadku wykorzystywania urządzeń mobilnych (np. tabletów, smartphony) wymaga się zastosowania środków bezpieczeństwa:
   1) blokada ekranu;
   2) program antywirusowy;
   3) wyłączenie nieużywanych usług;
   4) instalowanie usług z zaufanego źródła.
4. ASI jest zobowiązany do prowadzenia spisu sprzętu komputerowego wraz z kluczami licencyjnymi programów, który pozostaje pod jego pieką.
5. ASI odpowiedzialny jest za przygotowanie sprzętu komputerowego do prawidłowej i zgodnej z przeznaczeniem pracy.

6. W przypadku niepoprawnego i niezgodnego z przeznaczeniem użytkowania sprzętu komputerowego przez użytkownika ASI informuje o tym fakcie Inspektora.
7. ASI ma obowiązek instalowania wyłącznie licencjonowane oprogramowanie lub oprogramowanie nie wymagajcie opłat licencyjnych z godnie z warunkami gwarancji.
8. Użytkownik nie może samodzielnie zmieniać konfiguracji powierzonego mu do użytkowania sprzętu oraz instalować lub usuwać oprogramowania w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.
9. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za prawidłowe zabezpieczenie sprzętu przed używaniem go przez osoby nieupoważnione oraz ochrony przed kradzieżą lub zgubieniem.
10. Użytkownik nie może udostępniać powierzonego mu sprzętu służbowego osobom trzecim.

Korzystanie z komputerów przenośnych

1. Przetwarzanie danych poza obszarem przetwarzania na komputerze przenośnym wymaga zgody indywidualnej ADO.
2. O ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej Instrukcji, dotyczące pracy na komputerach stacjonarnych, w tym:
   1) zabezpieczenia dostępu hasłem;
   2) zastosowanie oprogramowania i zabezpieczeń analogicznie do rozwiązań przyjętych na stacjonarnych stacjach roboczych.
3. Pliki zawierające dane osobowe przechowywane na komputerach przenośnych są opatrzone hasłem dostępu.
4. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.
5. Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub szerokich z nich wypisów.
6. Użytkownicy przetwerzający dane osobowe na komputerach przenośnych obowiązani są do systematycznego wprowadzania tych danych w określone miejsca na serwerze ADO, a następnie do trwałego usuwania ich z pamięci powierzonych komputerów przenośnych.
7. Osoba wykorzystująca komputer przenośny obowiązana jest do:
   1) wykorzystywania go wyłącznie do określonych celów, mieszczących się w zakresie upoważnienia;
   2) nieudostępniania komputera nieupoważnionym osobom;
   3) zachowania szczególnej ochrony przed kradzieżą, zwłaszcza podczas transportu;
   4) zaniechania jakichkolwiek zmian oprogramowania.
8. W przypadku konieczności zmiany, aktualizacji albo naprawy komputera należy zgłosić ten fakt ASI.

9. ASI w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa zasady:
   1) postępowania w razie nieobecności w pracy dłuższej niż 30 dni. Jeśli komputer przenośny nie może być zwrócony przed okresem nieobecności, to użytkownik tego komputera powinien niezwłocznie powiadomić o tym ASI i uzgodnić z nim zwrot komputera;
   2) zwrotu sprzętu w razie ustania stosunku zatrudnienia.

Korzystanie ze służbowej poczty elektronicznej

1. Użytkownikowi systemu zostaje nadany dedykowany adres służbowej skrzynki poczty elektronicznej.
2. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej PCPR w Łowiczu.
3. Adres skrzynki poczty elektronicznej może służyć wyłącznie do celów służbowych.
4. Zabronione jest:
   1) wysyłanie materiałów służbowych na konta prywatne;
   2) wykorzystywanie służbowej poczty elektronicznej do działań niezgodnych z prawem i mogącym zaszkodzić wizerunkowi PCPR w Łowiczu;
   3) odbieranie wiadomości z nieznanych źródeł;
   4) otwierania wiadomości z załącznikami zawierającymi pliki samorozpakowującymi (com, exe, itp.)
   5) ukrywanie luk modyfikowanie zmian tożsamości nadawcy;
   6) czytanie, usuwanie, kopiowanie luz zmiany zawartości skrzynek pocztowych innych użytkowników;
   7) posługiwanię się adresem poczty służbowej w celu rejestrowania na stronach internetowych w celach handlowych czy forach dyskusyjnych, które nie dotyczą bezpośrednio wykonywania zakresu pracy.

Zasady korzystania z sieci publicznej – Internet

1. Sieć, w której pracują urządzenia komputerowe Administratora musi być zabezpieczona zaporo ogniową – firewall.
2. Systemy informatyczne powinny korzystać z szyfrowanych protokołów wymiany danych
3. Zdalny dostęp do serwerów w celach administracyjnych może mieć miejsce po zastosowaniu uwierzytelnienia użytkownika i szyfrowanego kanału transmisji.
4. Dostęp użytkowników do sieci Internetowej powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.
5. Zabrania się całkowicie dostępu do treści powszechnie uznanych za pornograficzne, rasistowskie, traktującej o przemocy, przestępstwach, jaki również do protokołów umożliwiających wymianę plików w sieci z naruszeniem prawa.

6. Wszelkie odstępstwa od tych reguł są możliwe po uzyskaniu zgody od Administratora.

Zasady korzystania z nośników informacji

1. Wszystkie nośniki informacji podlegają właściwej ochronie stosownie do klasyfikacji informacji, na wszystkich etapach ich używania, od momentu zapisu informacji, aż do momentu wycofania z użycia lub fizycznego zniszczenia opisanego w Instrukcji;
2. Za zapewnienie właściwej ochrony nośników informacji odpowiada ich użytkownik;
3. Osoby korzystające z nośników informacji powinny być świadome zagrożeń i zobowiązane są do zachowania należytej staranności poprzez zastosowanie obowiązujących środków organizacyjno-technicznych i prawnych opisanych w Instrukcji;
4. W przypadku wycofywania z użycia nośników informacji zawierających informacje stanowiące tajemnicę, na osobie, której nośnik przekazano do używania, spoczywa obowiązek wykonania procedury opisanej w Instrukcji;
5. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby ADO nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Komputery przenośne należy przewozić w służbowych torbach;
6. Nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w miejscach publicznych ani też w samochodach;
7. Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu;
8. Wykorzystywanie komputerów przenośnych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione. W konsekwencji korzystanie z komputera przenośnego będzie z reguły niedozwolone w restauracjach czy środkach komunikacji publicznej;
9. W domu niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do ADO. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym.
10. Jeśli nośnik danych (dysk, dyskietka, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie.

Korzystanie z urządzeń komunikacji głosowej, faksowej i wizyjnej

1. Każdy z użytkowników w PCPR w Łowiczu zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji danych osobowych lub informacji poufnych, jeśli rozmowy te odbywają się w miejscach publicznych lub otwartych pomieszczeniach, gdy nie można zagwarantować zachowania poufności danych.

2. Zabronione jest przekazywanie za pomocą urządzeń faksowych dokumentów zawierających dane osobowe wrażliwe lub informacje poufne.
3. Odczytywanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno się odbywaé tak, aby zabezpieczyć je przed dostępem osób nieuprawnionych.

Bezpieczeństwo oprogramowania

1. Oprogramowanie stosowane w jednostce może pochodzić wyłącznie ze źródeł legalnych oraz posiadać aktualną i kompletną dokumentację użytkownika, eksploatacyjną i techniczną, a w przypadku gdy przy jego pomocy przetwarzane są dane osobowe - zgodną z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych.
2. Instalacja i deinstalacja dokonywana jest wyłącznie przez ASI.
3. Użytkownicy obowiązani są do powstrzymania się od jakiejkolwiek ingerencji w oprogramowanie.
4. Wszelkie oprogramowanie wykorzystywane w jednostce musi być użytkowane z poszanowaniem praw własności intelektualnej, a w szczególności zgodnie z ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.
5. Za określanie oraz zmiany w obowiązujących standardach sprzętu i oprogramowania odpowiada ASI. Standard sprzętu i oprogramowania powinien być zgodny z wymaganiami biznesowymi, uwzględniać opłacalność ekonomiczną oraz wymagania w zakresie bezpieczeństwa.
6. Sprzęt i oprogramowanie powinny być eksploatowane, serwisowane i wycofywane z eksploatacji z zachowaniem właściwych procedur bezpieczeństwa.
7. Wszelkie działania związane z utrzymaniem i eksploatacją systemu informatycznego mogą być podejmowane wyłącznie przez upoważniony, wykwalifikowany personel jednostki lub upoważnione osoby.

Naprawy urządzeń komputerowych z chronionymi danymi osobowymi

1. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym przeprowadzane są o ile to możliwe przez ASI lub podmiot zewnętrzy pod nadzorem ASI.
2. Naprawy i zmiany w systemie informatycznym przeprowadzane przez serwisanta prowadzone są pod nadzorem i w siedzibie ADO o ile to możliwe lub poza siedzibą ADO, po uprzednim nieodwracalnym usunięciu danych w nim przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.
3. Jeśli nośnik danych (dysk, dyskietka, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie uniemożliwiając jego odczyt.

IX. PROCEDURA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W PRZYPADKACH AWARYJNYCH

1. Poprzez przypadek awaryjny należy rozumieć awarię systemu informatycznego służącego do przetwarzania danych osobowych pod nieobecność Administratora systemu informatycznego lub konieczność dokonania czynności administracyjnych przez firmy serwisujące sprzęt i oprogramowanie na podstawie umów z użyciem identyfikatorów i haseł użytkowników systemu.
2. W przypadkach awaryjnych możliwe jest udostępnienie za zgodą ASI lub osoby przez niego wyznaczonej identyfikatorów i haseł użytkowników na poziomie administratora systemów informatycznych.
3. W przypadku zaistnienia okoliczności określonych w punkcie 2 udostępnienie identyfikatorów i haseł musi odbywać się przy obecności osoby upoważnionej, a po usunięciu awarii hasło musi zostać natychmiast zmienione, lub identyfikator i hasło zablokowane do czasu zmiany hasła.
4. Przypadek awaryjny musi zostać niezwłocznie odnotowany w Systemie informatycznym w postaci notatki służbowej przekazanej IDO oraz ADO.
5. Identyfikatory i hasła administracyjne do Systemu informatycznego wraz z instrukcją ich użycia w przypadku awaryjnym przechowywane są w zamykanej szafie u ADO.

X. POSTĘPOWANIE W PRZYPADKU STWIERDZENIA NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

Definicja naruszenia bezpieczeństwa systemu

1. Za naruszenie bezpieczeństwa systemu informatycznego uznawany jest każdy stwierdzony fakt oraz uzasadnione podejrzenie, w szczególności:
   1) nieuprawnionego ujawnienia danych, udostępnienia;
   2) naruszenia hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła);
   3) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;
   4) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera;
   5) wykryciu wirusa komputerowego;
   6) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego;
   7) znacznym spowolnieniu działania systemu informatycznego;
   8) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe;
   9) istotnej zmianie położenia sprzętu komputerowego;
   10) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf;
   11) umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę

nieupoważnioną;

12) uszkodzenie lub zniszczenie danych lub jakiegokolwiek elementu systemu informatycznego;
13) działanie wbrew postanowieniom Instrukcji.

Tryb postępowania w przypadku naruszeń bezpieczeństwa systemu informatycznego

1. Każdy użytkownik systemu posiadający informacje o naruszeniu albo uzasadnione podejrzenie naruszenia bezpieczeństwa systemu informatycznego obowiązany jest bezzwłocznie poinformować o danym fakcie ASI.
2. Użytkownik do czasu przybycia na miejsce ASI podejmuje tylko takie czynności, które zmierzają do:
   1) zabezpieczenia śladów naruszenia,
   2) zapobieżenia dalszym zagrożeniom,
   3) powstrzymania skutków naruszenia,
   4) ustalenia przyczyny i sprawcy naruszenia ochrony,
   5) rozważenia wstrzymania bieżącej pracy w celu zabezpieczenia miejsca zdarzenia,
   6) przygotowania opisu incydentu.
3. Pracownik nie opuszcza bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia ASI lub osoby przez niego wskazanej.
4. ASI po otrzymaniu zawiadomienia, o którym mowa powinien niezwłocznie przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych i podjąć działania chroniące system przed ponownym naruszeniem.
5. W przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego.
6. ASI może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.
7. W razie odtwarzania danych z kopii zapasowych ASI obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej).
8. ASI podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego bądź zastosowaniu środków ochrony fizycznej.

XI. POSTANOWIENIA KOŃCOWE

1. Instrukcja jest dokumentem wewnętrznym jednostki i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.
2. W sprawach nieokreślonych niniejszą Instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać

się przed dopuszczeniem do przetwarzania danych z niniejszą Instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.

3. Niezastosowanie się do procedur określonych w niniejszej Instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane, jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 ustawy z dnia 26.06.1974 r. - Kodeks pracy.
4. Instrukcja wchodzi w życie z dniem podpisania.

Dotyczy Zarządzenia 8c/2019 Dyrektora PCPR w Łowiczu

Lp.	Imię i nazwisko pracownika	Podpis
1.	Małgorzata Janich	
2.	Bożena Jasińska	
3.	Gosiorska Ilona	Gosiorska Ilona
4.	Maria Bonk	
5.	Irena Idzi	
6.	Grażyna Urbańska	
7.	Aduba Natalia	
8.	Magdalena [illegible]	
9.	Ewelina Redon	Redon
10.	Marta Kot	Kot
11.	Justyna [illegible]-Wilk	
12.	Karolina [illegible]	
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		