POWIATOWE
CENTRUM INTEGRACJI SPOŁECZNEJ
w Legionowie
ul. gen. Władysława Sikorskiego 11
05-119 Legionowo
-2-

Zarządzenie Nr 10

Dyrektora Powiatowego Centrum Integracji Społecznej w Legionowie

z dnia 01.06.2017 r.

w sprawie wprowadzenia w Powiatowym Centrum Integracji Społecznej w Legionowie Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych.

Na podstawie § 13 ust. 12 Regulaminu Organizacyjnego Powiatowego Centrum Integracji Społecznej w Legionowie w związku z art. 36 ust 1 i 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2016, poz. 922) oraz na podstawie § 3 § 4 § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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. 2004 r. Nr 100, poz.1024) zarządzam co następuje:

§ 1

Wprowadzam do stosowania „Politykę bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Powiatowym Centrum Integracji Społecznej w Legionowie" stanowiącą załącznik nr 1 do Zarządzenia.

§ 2

1. Zobowiązuję pracowników Powiatowego Centrum Integracji Społecznej w Legionowie do zapoznania się z treścią " Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Powiatowym Centrum Integracji Społecznej w Legionowie" i złożenia oświadczenia o zapoznaniu się z dokumentem.
2. Traci moc Zarządzenie nr 12/2014 Kierownika Powiatowego Centrum Integracji Społecznej w Legionowie z dnia 01.09.2014 roku.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Powiatowego Centrum Integracji Społecznej
w Legionowie
Dorota Wróbel-Gorecka

RADCA PRAWNY
Sylwia Gawlik

Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Powiatowym Centrum Integracji Społecznej w Legionowie

Czerwiec 2017r.

hcl

SPIS TREŚCI

Definicje

- **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 z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;
- **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje);
- **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie; zwłaszcza takie, które wykorzystuje się w systemach informatycznych;
- **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- **Bezpieczeństwo systemu informatycznego** – wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
- **Administrator Danych Osobowych (ADO)** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Dyrektor Powiatowym Centrum Integracji Społecznej w Legionowie, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego ustawowej dyspozycji;
- **Administrator Bezpieczeństwa Informacji (ABI)** – należy przez to rozumieć pracownika urzędu wyznaczonego przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
- **Administrator Systemów Informatycznych (ASI)** – należy przez to rozumieć pracownika lub pracowników Informatyki odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych,
- **Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez ADO lub osoba uprawniona przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem;
- **Osoba uprawniona** – osoba posiadająca uprawnienie wydane przez ADO na mocy którego wykonuje w jego imieniu określone czynności;
- **Sieć Lokalna (LAN** Local Area Network**)** – Lokalna sieć teleinformatyczna;
- **Sieć rozległa (WAN)** – Rozległa sieć teleinformatyczna;
- **Identyfikator użytkownika (LOGIN)** – ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- **Hasło (Password)**– ciąg znaków literowych i cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

hgl

- **Zalogowanie** – uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
- **Odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
  - osoby, której dane dotyczą,
  - osoby, upoważnionej do przetwarzania danych,
  - przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
  - podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
  - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Wprowadzenie

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Powiatowym Centrum Integracji Społecznej w Legionowie.

Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Powiatowego Centrum Integracji Społecznej w Legionowie. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych, oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Powiatowym Centrum Integracji Społecznej w Legionowie", zwanym dalej „Polityką bezpieczeństwa", wskazujący sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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, Nr 100, poz. 1024).

1) „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:
   - stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   - stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji sieci informatycznej mogą wskazywać lub sugerować naruszenie zabezpieczeń tych danych.
2) „Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Powiatowego Centrum Integracji Społecznej w Legionowie.
3) Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych Powiatowego Centrum Integracji Społecznej w Legionowie.

ROZDZIAŁ I
ZASADY POSTĘPOWANIA PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Administrator danych osobowych, którym jest Dyrektor Powiatowego Centrum Integracji Społecznej w Legionowie (dalej PCIS), swoją decyzją wyznacza „Administratora Bezpieczeństwa Informacji" dla danych zawartych w systemach informatycznych PCIS, zwanego dalej „Administratorem Bezpieczeństwa Informacji" oraz osobę upoważnioną do zastępowania „Administratora Bezpieczeństwa Informacji".

2. Administrator danych osobowych jest zobowiązany do:
   - czuwania nad tym, by będące w jego posiadaniu dane osobowe były przetwarzane zgodnie z prawem,
   - zastosowania niezbędnych środków technicznych i organizacyjnych w celu zapewnienia ochrony przetwarzanych danych osobowych w Powiatowym Centrum Integracji Społecznej w Legionowie,
   - sprawowania kontroli nad bezpieczeństwem oraz sposobem przetwarzania danych,
   - rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiorów danych przed przystąpieniem do ich przetwarzania, prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych.

3. „Administrator Bezpieczeństwa Informacji" realizuje zadania w zakresie ochrony danych, a w szczególności:
   - ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Powiatowego Centrum Integracji Społecznej w Legionowie,
   - podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
   - niezwłocznego informowania Administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   - nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,
   - opracowania i wdrożenia programu szkolenia w zakresie zabezpieczenia systemu informatycznego,
   - prowadzenia rejestru zbiorów danych przetwarzanych przez Administratora Danych Osobowych
4. Osoba zastępująca ABI powyższe zadania realizuje tylko w przypadku nieobecności ABI.
5. Osoba zastępująca składa Administratorowi Bezpieczeństwa Informacji relację z podejmowanych działań w czasie jego zastępstwa.
6. Dyrektor Powiatowego Centrum Integracji Społecznej w Legionowie jest zobowiązany do:
   1) opracowania dla każdej osoby zatrudnionej przy przetwarzaniu danych osobowych zakresu czynności z uwzględnieniem stopnia dostępu do danych osobowych oraz przewidzenia odpowiedzialności, za naruszenie tajemnicy za danych, adekwatnej do zakresu obowiązków,
   2) sprawowanie nadzoru nad pracą podległych pracowników w zakresie wykonywania czynności służbowych w sposób zapewniający ochronę danych osobowych,

LG

7. Pracownik upoważniony przez ADO do przetwarzania danych osobowych, jest zobowiązany do:

1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
2) stosowania określonych przez administratora danych , procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
3) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą,
4) podporządkowania się poleceniom administratora bezpieczeństwa informacji oraz właściwego kierownika, w zakresie ochrony danych.

8. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez administratora danych osobowych. Wzór upoważnienia stanowi **załącznik nr 1** do niniejszego dokumentu.

9. Bezpośredni nadzór nad przetwarzaniem danych osobowych w Powiatowym Centrum Integracji Społecznej w Legionowie sprawuje Dyrektor Powiatowego Centrum Integracji Społecznej w Legionowie.

10. Pracownik, któremu administrator danych osobowych udzielił upoważnienia, o którym mowa w ust. 8 jest zobowiązany do podpisania oświadczenia. Wzór oświadczenia stanowi **załącznik nr 2** do niniejszego dokumentu.

11. W przypadku zatrudnienia nowego pracownika, zmiany stanowiska, zmiany zakresu obowiązków pracowniczych, utworzenia nowego zbioru danych osobowych, zmiany sposobu przetwarzania danych lub w innych przypadkach, które wpływają bezpośrednio na rodzaj i zakres przetwarzania danych, administrator danych osobowych wydaje lub cofa upoważnienia. Wzór pisma o cofnięciu upoważnienia stanowi **załącznik nr 3** do niniejszego dokumentu.

12. Wypowiedzenie umowy o pracę jest równoznaczne z cofnięciem upoważnienia do przetwarzania danych osobowych.

13. W obiegu wewnętrznym PCIS wprowadza się następujące zasady udostępniania danych osobowych:

1) informacje zawierające dane powszechnie dostępne może udostępnić pracownik przetwarzający dane w formie bezpośredniej lub telefonicznej, po sprawdzeniu tożsamości w procedurze "zwrotnej informacji telefonicznej",
2) zgodę na udostępnienie danych osobowych w szerszym zakresie wyraża Dyrektor.

14. W obiegu zewnętrznym zgodę na udostępnienie danych osobowych wyraża administrator danych zgodnie z powszechnie obowiązującymi przepisami.

15. Obowiązek przestrzegania tajemnicy danych osobowych spoczywa na wszystkich pracownikach, którzy mają do nich dostęp, również po ustaniu stosunku pracy.

16. ADO może przenieść obowiązek utrzymywania lub przetwarzania zbioru/zbiorów danych osobowych, na podmiot trzeci jednak musi się to odbyć za pośrednictwem stosownej umowy oraz z zachowaniem reguł bezpieczeństwa danych opisanych w niniejszym dokumencie.

L.9

17. Przetwarzanie danych osobowych sprzeczne z przepisami ustawy o ochronie danych osobowych może stanowić ciężkie naruszenie obowiązków pracowniczych.

18. Zbiory danych osobowych przetwarzane przez pracowników Powiatowego Centrum Integracji Społecznej w Legionowie nie będą udostępniane do celów komercyjnych.

ROZDZIAŁ II

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:

a) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,

b) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu informatycznego, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,

c) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:

- nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do systemu z jego wnętrza,
- pogorszenie jakości sprzętu i oprogramowania
- nieuprawniony przekaz danych
- bezpośrednie zagrożenie materialnych składników systemu.

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,

b) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie silnego pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

c) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym fakt pozostawienia serwisantów bez nadzoru,

d) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,

e) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenie systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,

f) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,

hG

g) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
h) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
i) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń np. login użytkownika i jego hasło,
j) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
k) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
l) podmieniono, lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w inny sposób niedozwolony skasowano lub skopiowano dane osobowe,
m) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowano się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych osobowych uważa się również stwierdzone nieprawidłowości w zakresie bezpieczeństwa miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

ROZDZIAŁ III

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Powiatowym Centrum Integracji Społecznej w Legionowie jest Dyrektor PCIS.
2. Administrator danych osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Powiatowego Centrum Integracji Społecznej w Legionowie, a w szczególności:
   a) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   b) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
   c) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
3. Do zastosowanych środków technicznych należy:
   a) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
   b) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt. a,
   c) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
   d) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.
4. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:
   a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,

b) przeszkolenie osób, o których mowa w pkt. a, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochrona danych osobowych,

c) kontrolowanie otwierania i zamykania pomieszczeń, w którym są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.

5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Powiatowym Centrum Integracji Społecznej w Legionowie" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

6. Wykaz pomieszczeń w których przetwarzane są dane osobowe stanowi **Załącznik** Nr **4** do niniejszego dokumentu.

7. Wykaz zbiorów przetwarzanych elektronicznie lub w inny sposób stanowi **Załącznik Nr 5 a i b** do niniejszego dokumentu.

8. Opis struktury zbiorów danych stanowi **Załącznik Nr 6** do niniejszego dokumentu.

9. Sposób przepływu danych pomiędzy systemami stanowi **Załącznik Nr 7** do niniejszego dokumentu.

10. Opis rejestracji baz danych stanowi **Załącznik Nr 8** do niniejszego dokumentu.

11. Opis zabezpieczeń systemów informatycznych stanowi **Załącznik Nr 9** do niniejszego dokumentu.

ROZDZIAŁ IV

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych osobowych lub osoba przez niego wyznaczona, którą jest „Administrator Bezpieczeństwa Informacji" sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

2. Administrator Bezpieczeństwa Informacji sporządza roczne plany kontroli zatwierdzone przez Dyrektora i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.

3. Na podstawie zgromadzonych materiałów o których mowa w pkt. 2 Administrator Bezpieczeństwa Informacji sporządza roczne sprawozdanie i przedstawia ADO.

ROZDZIAŁ V

ŚRODKI TECHNICZNE I ORGANIZACYJNE

Środki techniczne i organizacyjne

Część ta zawiera opis środków technicznych, organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Szczególny opis zawarto w „**Instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji" (rozdział VI)**

69

Środki organizacyjne

1. Dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez Administratora Danych Osobowych.
2. Każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu, przenoszeniu wszelkich danych osobowych.
3. Należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych.
4. Pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na klucz.
5. Dostęp do kluczy powinni posiadać tylko upoważnieni pracownicy.
6. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy urzędu. W wypadku, gdy jest wymagany poza godzinami pracy - możliwy jest tylko na podstawie pisemnego zezwolenia Administratora Danych Osobowych.
7. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy.
8. W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach TYLKO w obecności osób upoważnionych, i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
9. Szafy w których przechowywane są dane osobowe muszą być zamykane na klucz.
10. Klucze do tych szaf powinni posiadać tylko upoważnieni pracownicy.
11. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane.
12. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.

Środki techniczne

1. Dostęp do komputerów, na których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu.
2. Stacje komputerowe, na których przetwarzane są dane osobowe powinny mieć tak ustawione monitory, aby nie miały wglądu w dane osoby nieupoważnione.
3. Każdy plik, w którym są zawarte dane osobowe powinien być zabezpieczony hasłem, jeśli nie jest to przetwarzanie danych w systemie informatycznym.
4. W przypadku przetwarzania danych osobowych na komputerach przenośnych (notebook) należy zachować szczególną ostrożność przy ich przewożeniu.
5. Po zakończeniu pracy komputery (notebook) takie powinny być zabezpieczone w zamykanych na klucz szafach.
6. Komputerów tych nie należy wynosić poza budynek.
7. W wypadku potrzeby wyniesienia (notebook-a) wcześniej należy dane osobowe przenieść na komputer stacjonarny w miejscu pracy.
8. Nie należy udostępniać osobom nieupoważnionym tych komputerów.
9. W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności i za zgodą ABI.
10. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.
11. W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie.
12. W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
13. Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.
14. Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.

hG

15. Do zabezpieczenia sieci należy stosować:
    a) firewall,
    b) adresowanie stacji roboczych tylko adresami prywatnymi, nierutowalnymi,
    c) systemy wykrywania włamań IDS,
    d) logowanie wszelkich zdarzeń w dziennikach systemowych na serwerach,
    e) systemy antywirusowe,
    f) zabezpieczenia skrzynek poczty elektronicznej,
    g) zabezpieczenie przed dostępem na zewnątrz ze stacji roboczych do innych usług niż WWW,
    h) dostęp do poczty elektronicznej tylko na serwerach autoryzowanych przez Powiatowe Centrum Integracji Społecznej w Legionowie
    i) ustawienie odpowiednich poziomów dostępu dla odpowiednich użytkowników w systemach teleinformatycznych.

ROZDZIAŁ VI
INSTRUKCJA OKREŚLAJĄCA SPOSÓB ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM, SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH, ZE SZCZEGÓLNYM UWZGLĘDNIENIEM BEZPIECZEŃSTWA INFORMACJI

1. **Określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności.**

a. hasło nie powinno zawierać mniej niż 8 znaków,
b. hasło nie może być takie samo jak identyfikator,
c. hasło musi być zmieniane przynajmniej raz w miesiącu przez użytkownika, administratora bezpieczeństwa informacji lub automatycznie przez system,
d. użytkownikowi nie wolno zapisywać hasła na papierze,
e. użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności,
f. komputery nie pracujące w sieci muszą mieć hasło założone na BIOS,
g. w przypadku czasowego opuszczenia stanowiska pracy, użytkownik powinien wylogować się z systemu, lub po 5 minutach musi uruchomić się wygaszacz ekranu zabezpieczony hasłem,
h. za gospodarkę hasłami odpowiedzialny jest administrator bezpieczeństwa informacji,
i. hasło przy wpisywaniu nie może być wyświetlane na ekranie.

2. Określenie sposobu rejestrowania i wyrejestrowania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności.

a. administrator bezpieczeństwa informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych, zawierającą ich identyfikatory, **Załącznik Nr 12** do niniejszego dokumentu
b. rejestracji użytkowników w systemie dokonuje administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona,
c. zarejestrować można wyłącznie osoby, które administrator danych wpisał do ewidencji osób upoważnionych do przetwarzania danych,
d. wyłączenie z ewidencji osób upoważnionych do przetwarzania danych, obliguje administratora bezpieczeństwa informacji do odebrania dostępu do danych osobowych,
e. zalecane jest, aby identyfikator składał się z pierwszej litery imienia i pierwszych pięciu liter nazwiska.

3. Procedury rozpoczęcia i zakończenia pracy

LG

1. administrator bezpieczeństwa informacji danych w porozumieniu z ADO, ustala czas pracy użytkownikom systemu, na pracę poza godzinami funkcjonowania PCIS musi wyrazić zgodę na piśmie Dyrektor PCIS, w formie upoważnienia jednorazowego lub stałego,
2. administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona, nadzoruje rozpoczęcie i zakończenie pracy systemu informatycznego,
3. w pomieszczeniach gdzie przyjmowani są klienci , monitory powinny być tak ustawione, aby uniemożliwić osobie niepowołanej wgląd w dane,
4. dopuszcza się pozostawianie włączonego serwera w nocy, jeżeli pomieszczenie w którym on pracuje wyposażone jest w sprawny system powiadamiania p-poż, UPS oraz alarm anty włamaniowy.
5. kontrola wprowadzanych danych prowadzona jest na bieżąco na każdym stanowisku merytorycznym, nadzór prowadzi administrator bezpieczeństwa informacji,
6. o przekazywaniu danych osobowych innym podmiotom decyduje ADO,
7. osoby, których dane są przetwarzane powinny mieć możliwość zapoznania się z przysługującymi im prawami wynikającymi z ustawy o ochronie danych osobowych.

4. Metoda i częstotliwość tworzenia kopii awaryjnych

a. za sporządzanie i bezpieczeństwo kopii odpowiedzialny jest administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona,
b. kopii należy dokonywać poprzez przegrywanie (backup) całej bazy danych (bez kompresji),
c. w każdej chwili powinno być dostępnych jednocześnie pięć kopii: z ostatniego dnia, tygodnia, miesiąca, kwartału i roku. Kopie dzienne i tygodniowe należy zapisywać na HDD a pozostałe na CD,
d. kopie awaryjne może tworzyć jedynie administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona,
e. w czasie tworzenia kopii awaryjnej przez administratora, dostęp do bazy dla wszystkich użytkowników powinien być zablokowany,
f. dyski wymienne z kopiami bezpieczeństwa powinny być wyjęte z komputera w czasie bieżącej pracy,
g. administrator wykonuje backup lub archiwizacje systemu wykorzystując jak najlepiej swoje umiejętności.

Wprowadza się praktyczne zalecenia odnośnie do wykonania kopii bezpieczeństwa:

a. przeprowadzić składowanie informacji regularnie,
b. używać różnych typów nośników danych,
c. kopie umieszczać w różnych, oddalonych od siebie miejscach,
d. najlepiej do składowania wybrać tak nośnik, aby mógł w całości pomieścić kopie danych,
e. przed składowaniem danych sprawdzić je programem antywirusowym,
f. dokładnie opisywać składowane dane,
g. trzymać nośniki z kopiami z daleka od źródeł pola magnetycznego i miejsc nasłonecznionych,
h. sprawdzić, czy składowanie przebiegło prawidłowo,
i. upewnić się, że nośnik jest niezależny od urządzenia, tzn. że dane mogą być przywrócone nie tylko na komputerze, z którego były poprawne,
j. regularnie konserwować urządzenia do składowania.

5. Metody i częstotliwość sprawdzania obecności wirusów komputerowych oraz metody ich usuwania

a. za ochronę antywirusową odpowiedzialny jest administrator bezpieczeństwa informacji,

69

b. do ochrony antywirusowej należy stosować jednostanowiskowy program antywirusowy, zainstalowany na komputerze, gdzie odbierana jest poczta elektroniczna i sprawdzane są wszystkie dyskietki i płyty CD, przed ich uruchomieniem w sieci oraz na komputerach wolno stojących,
c. sprawdzanie dostępnymi programami antywirusowymi odbywać się powinno przynajmniej raz w miesiącu,
d. zalecane jest wykorzystanie programów pracujących w tle,
e. przy kontroli szczególną uwagę należy zwrócić na makra,
f. każdą przesyłkę otrzymaną za pomocą transmisji danych (e-mail, ftp) należy sprawdzić programem antywirusowym,
g. korzystanie z zewnętrznych nośników informacji (dyskietek, dysków wymiennych, płyt CD, Internetu, poczty elektronicznej) może mieć miejsce wyłącznie po uzyskaniu zgody administratora bezpieczeństwa informacji,
h. w przypadku wykrycia wirusa choćby na jednym komputerze, należy sprawdzić wszystkie stacje robocze w starostwie.

6. Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków

a. nie należy magazynować zbędnych plików i wydruków, kopie bezpieczeństwa po upływie okresu przechowywania muszą być skasowane, lub fizycznie zniszczone w sposób uniemożliwiający odczytanie danych,
b. za zniszczenie zbędnych wydruków i innych dokumentów zawierających dane osobowe odpowiedzialny jest administrator danych osobowych, za skasowanie danych, lub zniszczenie nośników elektronicznych, odpowiedzialny jest administrator bezpieczeństwa informacji,
c. zbędne dokumenty konwencjonalne (papierowe) powinny być zniszczone w niszczarce dokumentów lub podarte na drobne fragmenty,
d. kopie bezpieczeństwa na płytach CD powinny być przechowywane w zamkniętej metalowej szafie,
e. kopie na płytach CD nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowanych na bieżąco,
f. kopie awaryjne sprawdza się pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu – co najmniej jednorazowo po przegraniu danych,
g. wydruki należy przechowywać w pomieszczeniach, uniemożliwiających dostęp do nich przez osoby niepowołane,
h. osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera, w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, a w szczególności powinna zabezpieczyć dostęp do komputera hasłem i nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych, w szczególności komputera nie należy pozostawiać w samochodzie,
i. kopie przechowuje się co najmniej:
   - dzienne przez siedem dni,
   - tygodniowe przez kolejny tydzień,
   - miesięczne przez kolejny miesiąc,
   - kwartalne przez kolejny kwartał,
   - roczne przez cały kolejny rok od daty sporządzenia.

7. Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych

a. przeglądu i konserwacji dokonuje administrator bezpieczeństwa informacji, lub osoba przez niego

upoważniona, przynajmniej dwa razy w roku,

b. zasilacz UPS powinien zapewnić automatyczne zakończenie pracy i wyłączenie serwerów przy zaniku lub nadmiernym wahaniu napięcia – min. czas podtrzymania pracy wynosi 5 min,
c. w przypadku przekazywania komputera z dyskiem lub innym nośnikiem danych osobowych do naprawy, należy nośnik zdemontować, zabezpieczyć dostęp hasłem lub dokonać naprawy w obecności osoby upoważnionej przez administratora danych, w przypadku przekazania nośnika innemu podmiotowi należy dane nieodwracalnie skasować,
d. o wszelkich nieprawidłowościach, awariach, próbie lub naruszeniu bezpieczeństwa danych osobowych, użytkownik powinien niezwłocznie powiadomić administratora bezpieczeństwa informacji,
e. do wydzielonej sieci energetycznej zasilającej system komputerowy nie wolno podłączać żadnych innych urządzeń (czajników elektrycznych, odkurzaczy, radioodbiorników),
f. zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez pracowników urzędu.

8. Sposób postępowania w zakresie komunikacji w sieci komputerowej

System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych, lub logicznych zabezpieczeń, chroniących przed nieuprawnionym dostępem (załącznik do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 Kwietnia 2004 poz. 1024).

a. przy przydzielaniu uprawnień obowiązuje zasada „wszystko co nie jest dozwolone, jest zabronione",
b. administrator bezpieczeństwa informacji z administratorem danych określi zasoby dostępne dla każdego użytkownika,
c. użytkownicy powinni być przydzielani do odpowiedniej grupy roboczej, automatycznie w procesie logowania np. za pomocą login scriptu,
d. dostęp do serwerowi ma tylko ABI i pracownicy przez niego upoważnieni,
e. dostęp do konsoli serwera winien być zabezpieczony hasłem,
f. administrator bezpieczeństwa informacji winien monitorować pracę w sieci za pomocą dostępnego oprogramowania narzędziowego i plików .log,
g. w pomieszczeniu, gdzie ustawiony jest serwer powinien pracować tylko administrator bezpieczeństwa informacji, lub osoby przez niego upoważnione,
h. nie wolno instalować w sieci własnego oprogramowania bez zgody administratora bezpieczeństwa informacji,
i. „zwykli" użytkownicy nie powinni mieć dostępu do zasobów systemowych serwera, katalogów roboczych, danych i wolumenów z poziomu systemu operacyjnego,
j. dostęp do archiwalnych plików pocztowych należy zabezpieczyć hasłem,
k. wszystkie listy otrzymane pocztą elektroniczną należy przekazywać do rejestracji,
l. w celu zwiększenia bezpieczeństwa transmisji danych osobowych należy stosować kryptografie,
m. w czasie korzystania z Internetu za pośrednictwem linii komutowanej, końcówka powinna być fizycznie odłączona od sieci lokalnej,
n. uczestnictwo w internetowych grupach dyskusyjnych dozwolone jest jedynie za zgodą administratora bezpieczeństwa informacji,
o. komunikacja w sieci lokalnej musi umożliwiać identyfikację pracujących użytkowników.

ROZDZIAŁ VII
INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1.

Niniejsze zasady określają tryb postępowania w przypadku gdy:

a. Stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
b. Stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, mogą wskazywać na naruszenie zabezpieczeń tych danych.

2.

O naruszeniu ochrony danych osobowych mogą świadczyć w szczególności następujące symptomy:

a. Brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych.
b. Brak możliwości zalogowania się do tej aplikacji.
c. Ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika aplikacji (np. brak możliwości wykonywania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji.
d. Wygląd aplikacji inny niż normalnie.
e. Inny zakres danych niż normalnie dostępny dla użytkownika - dużo więcej lub dużo mniej danych.
f. Znaczne spowolnienie działania systemu informatycznego.
g. Pojawienie się nie standardowych komunikatów generowanych przez system informatyczny.
h. Ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe.
i. Ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii awaryjnych.
j. Włamanie lub próby włamania do szafek, w których przechowywane są w postaci elektronicznej lub papierowej - nośniki danych osobowych.
k. Zagubienie lub kradzież nośnika danych osobowych.
l. Zagubienie lub kradzież nośnika materiału krypotograficznego (karty mikroprocesorowej, dyskietki itp).
m. Kradzież sprzętu informatycznego, w którym przechowywane były dane osobowe.
n. Informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami.
o. Fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej.
p. Podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

3.

O ujawnieniu danych decyduje:

a. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nie uprawnionym tożsamości osoby, której dane dotyczą.
b. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

4.

a. Każdy pracownik PCIS biorący udział w przetwarzaniu danych osobowych w systemie

69

informatycznym jest odpowiedzialny za bezpieczeństwo tych danych. W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub. mogących spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania Administratora Bezpieczeństwa Informacji lub innej osoby wskazanej przez niego.

b. Każda osoba zatrudniona w PCIS, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób), powinna niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu danych osobowych lub Administratora Bezpieczeństwa Informacji, albo inna upoważnioną przez niego osobę.
c. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za przygotowanie i opublikowanie wykazu osób, które mogą być informowane w przypadku wystąpienia zagrożenia danych osobowych.
d. W przypadku niemożliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub osób przez niego upoważnionych, pracownik winien powiadomić bezpośredniego przełożonego.

5.

a. Informacja o pojawieniu się zagrożenia lub wystąpieniu zagrożenia danych osobowych przekazywana jest przez pracownika osobiście, telefonicznie lub pocztą elektroniczną.
b. Informacja, o której mowa w ust. 1 powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia.
c. W przypadku gdy zgłoszenie o podejrzeniu zaistnienia incydentu otrzyma osoba inna niż Administrator Bezpieczeństwa Informacji, jest ona obowiązana poinformować o tym fakcie Administratora Bezpieczeństwa Informacji.
d. Pracownik może zostać poproszony przez Administratora Bezpieczeństwa Informacji o potwierdzenie zauważonego faktu na piśmie.

6.

a. Do czasu przybycia Administratora Bezpieczeństwa Informacji lub upoważnionej przez niego osoby, zgłaszający:
    1) niezwłocznie podejmuje czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnia w działaniu również ustalenie przyczyn lub sprawców,
    2) zabezpiecza dostęp do miejsca lub urządzenia przez osoby trzecie,
    3) wstrzymuje pracę na komputerze na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane,
    4) nie zmienia położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jej okoliczności,
    5) podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
    6) podejmuje inne działania przewidziane określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
    7) wstępnie dokumentuje zaistniałe naruszenie.
b. Dokonywanie zmian w miejscu naruszenia ochrony jest dopuszczalne jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

7.

Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona, niezwłocznie po uzyskaniu sygnału o naruszeniu danych osobowych, powinien:

hq

a. Zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy PCIS.
b. Zapisać wszelkie informacje związane z danym zdarzeniem.
c. Na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia.
d. Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej.
e. Dokonać fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej.
f. Wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.
g. Dokonać zmiany hasła na konto Administratora Bezpieczeństwa Informacji i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.
h. Zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.
i. Rozważyć możliwość i potrzebę powiadomienia o zaistniałym naruszeniu Dyrektora - Administratora Danych.
j. Nawiązać bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza PCIS.
k. Zamknąć i opieczętować urządzenia, w których przechowywane są dane osobowe w formie analogowej.

8.

Administrator Bezpieczeństwa Informacji podejmuje działania zmierzające do wyjaśnienia zgłoszonego zdarzenia. W szczególności może on dokonywać, w zależności od zgłoszonego zdarzenia:

a. Wizji lokalnej w zakresie adekwatnym do rodzaju zgłoszonego zdarzenia.
b. Przeprowadzenia wywiadów z pracownikami w celu ustalenia zaistniałych faktów.
c. Przeprowadzenia analizy poprawności funkcjonowania systemu informatycznego, jeżeli zgłoszone zdarzenie było związane z nieprawidłowym jego funkcjonowaniem.
d. Przeprowadzenia analizy zapisu zdarzeń w systemie informatycznym z uwzględnieniem zapisu operacji realizowanych przez użytkowników.
e. Przeprowadzenia analizy danych przetwarzanych w systemie informatycznym, jeżeli zgłoszone zdarzenie mogło być spowodowane utratą dostępności lub integralności przetwarzanych danych.
f. Sporządzenia dokumentacji fotograficznej.
g. Zabezpieczenia danych przetwarzanych w systemie informatycznym dotkniętym incydentem, w szczególności danych konfiguracyjnych tego systemu.
h. Zebrania innych materiałów pozwalających na wyjaśnienie przyczyn zaistnienia incydentu, jego charakteru i potencjalnych skutków.

9.

Po wykonaniu czynności, o których mowa w pkt. 7 i w pkt. 8, Administrator Bezpieczeństwa Informacji jest zobowiązany do podjęcia kroków w celu:

a. Wyjaśnienia zdarzenia - w szczególności czy miało miejsce naruszenie ochrony danych osobowych.
b. Wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów - w szczególności, gdy zdarzenie było związane z celowym działaniem pracowników bądź osób trzecich.
c. Zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia.
d. Usunięcie skutków incydentu i przywrócenie pierwotnego stanu systemu informatycznego (to jest sprzed incydentu).
e. Ewentualnego ukarania sprawców incydentu.

hq

10.

Administrator Bezpieczeństwa Informacji przystępuje do usuwania skutków incydentu i przywrócenia prawidłowego przebiegu procesu przetwarzania danych osobowych. W szczególności działania związane z usuwaniem skutków incydentu mogą obejmować:

a. Przeprowadzenie naprawy sprzętu informatycznego.
b. Rekonfigurację sprzętu informatycznego.
c. Wprowadzenie poprawek do oprogramowania.
d. Rekonfigurację oprogramowania.
e. Odtworzenie danych z kopii awaryjnych.
f. Modyfikację danych w celu odtworzenia ich integralności.
g. Wycofanie z użycia materiału kryptograficznego.
h. Inne naprawy urządzeń wchodzących w skład infrastruktury informatycznej wspomagających lub zabezpieczających działanie systemu informatycznego.

11.

Administrator Bezpieczeństwa Informacji może odstąpić od usuwania skutków incydentu, jeżeli został on spowodowany działaniem celowym, a całkowite wyjaśnienie zdarzenia i wyciągnięcie konsekwencji wobec sprawców jest istotniejsze niż przerwa w działaniu systemu. Istniejący stan systemu informatycznego jest niezmieniany w celach dowodowych do czasu wyjaśnienia sprawy.

12.

Przy usuwaniu skutków incydentu z wykorzystaniem odtwarzania danych z kopii awaryjnych Administrator Bezpieczeństwa Informacji obowiązany jest upewnić się, że odtworzone dane zostały zapisane przed wystąpieniem incydentu - w szczególności dotyczy to przypadków odtwarzania systemu po infekcji wirusowej.

13.

a. W sytuacjach wyjątkowych wszystkie powyżej opisane działania związane z usuwaniem skutków incydentu i wyjaśnianiem jego przyczyn mogą być realizowane przez osoby upoważnione przez Administratora Bezpieczeństwa Informacji.
b. Administrator Bezpieczeństwa Informacji odpowiada za sporządzenie listy pracowników mających prawo do podejmowania odpowiednich kroków w razie wystąpienia incydentu w sytuacji, gdy nie mogą one być wykonane osobiście przez niego.

14.

a. Administrator Bezpieczeństwa Informacji określa, na podstawie przeprowadzonych wyjaśnień, przyczyny zaistnienia incydentu.
b. Jeżeli incydent był spowodowany celowym działaniem, Administrator Bezpieczeństwa Informacji jest zobowiązany do pisemnego powiadomienia Dyrektora PCIS - Administratora Danych.
c. Dyrektor - Administrator Danych, biorąc pod uwagę charakter zdarzenia, może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.

15.

Zgodę na uruchomienie komputerów i innych urządzeń lub dokonanie zmian w miejscu naruszenia ochrony wyraża Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

h9

16.

a. System informatyczny, którego prawidłowe działanie zostało odtworzone, powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu. W czasie jej trwania użytkowanie systemu informatycznego powinno być ograniczone do niezbędnego minimum.

b. Okres kwarantanny, o którym mowa w ust.1 , jest uzależniony charakterem incydentu i specyfiką systemu informatycznego - jest on każdorazowo określany przez Administratora Bezpieczeństwa Informacji.

17.

a. Administrator Bezpieczeństwa Informacji dokumentuje w raporcie każdy zaistniały przypadek naruszenia ochrony danych osobowych.

b. Dokumentacja, o której mowa w ust. 17.a, obejmuje następujące informacje:

1) imię i nazwisko osoby zgłaszającej incydent,
2) imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
3) datę i godzinę przyjęcia zgłoszenia incydentu,
4) określenie czasu i miejsca incydentu,
5) opis zgłoszonego incydentu oraz okoliczności towarzyszące,
6) przyczyny wystąpienia naruszenia,
7) opis podjętych działań naprawczych,
8) wyniki przeprowadzonego badania wyjaśniającego,
9) ocenę skuteczności przeprowadzonego postępowania naprawczego,
10) podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości naruszenia ochrony danych osobowych.

c. Wzór raportu, o którym mowa w ust.17.a, określa **Załącznik Nr 10** do Polityki Bezpieczeństwa

18.

Administrator Bezpieczeństwa Informacji w oparciu o posiadaną dokumentację, odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:

a. Określenia skuteczności podejmowanych działań wyjaśniających i naprawczych.

b. Określenia wymagań działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów.

c. Określenia potrzeb w zakresie szkoleń użytkowników systemu informatycznego przetwarzającego dane osobowe.

ROZDZIAŁ VIII

POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

hg

2. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego **Załącznik nr 11** do niniejszego dokumentu.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa.
4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002r. Nr 101, poz. 926 ze zm.) oraz możliwość wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U.2016 poz. 922), rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004, Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. 2004, Nr 100, poz. 1023).
6. Niniejsza „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Powiatowym Centrum Integracji Społecznej w Legionowie" wchodzi w życie z dniem jej podpisania przez Dyrektora.

ROZDZIAŁ IX

ZAŁĄCZNIKI

DYREKTOR
Powiatowego Centrum Integracji Społecznej
w Legionowie
Dorota Wróbel-Górecka

Załącznik Nr 1

(WZÓR)

....., dnia .....

.....

(pieczątka)

UPOWAŻNIENIE nr .....

z dnia .....

Na podstawie art. 37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (*Dz. U. 2016, poz. 922*) upoważniam Panią/a ..... zatrudnioną/ego w Powiatowym Centrum Integracji Społecznej w Legionowie, na stanowisku ..... do przetwarzania danych osobowych.

Zadania i czynności do wykonania:

1. Ochrona danych osobowych w systemie informatycznym i ręcznym, a w szczególności przeciwdziałanie dostępowi osób niepowołanych oraz przeciwdziałanie w przypadku wykrycia naruszeń zabezpieczeń systemu zgodnie z ustawą o ochronie danych osobowych (*Dz. U. 2016, poz. 922*).
2. Przestrzeganie zasad określonych w instrukcji określającej sposób zarządzania systemem informatycznym i ręcznym.
3. Przestrzeganie zasad określonych w instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych.
4. Przestrzeganie zachowania w tajemnicy danych osobowych uzyskanych w okresie zatrudnienia w związku z upoważnieniem do przetwarzania danych osobowych, także po ustaniu stosunku pracy.
5. W szczególności przetwarzanie danych osobowych w następujących zbiorach danych (*numer i nazwa*):..... ....

Data i podpis Administratora Danych Osobowych *Data i podpis pracownika*

Załącznik Nr 2

Oświadczenie pracownika

.....

(imię i nazwisko)

.....

(Wydział)

.....

(stanowisko)

OŚWIADCZENIE

Oświadczam, że zapoznałem(łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. 2016, poz. 922) oraz Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemu informatyczne, służące do przetwarzania danych osobowych (Dz. U. 2004, Nr 100, poz. 1024) i zobowiązuję się do ich przestrzegania.

Oświadczam ponadto, że zapoznałem(łam) się z Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych oraz Instrukcją przetwarzania danych osobowych w Powiatowym Centrum Integracji Społecznej w Legionowie.

Świadomy(a) odpowiedzialności porządkowej i karnej oświadczam, że znane mi dane osobowe będę przetwarzać zgodnie z prawem, i nie dopuszczę do bezprawnego naruszenia tajemnicy również w sytuacji, gdy ustanie moje zatrudnienie w:

Powiatowym Centrum Integracji Społecznej w Legionowie

ul. gen. Władysława Sikorskiego 11

05 – 119 Legionowo

Otrzymałem(łam) dnia:

.....

(podpis pracownika)

....., dnia .....

beg

Załącznik Nr 3

(WZÓR)

Wycofanie upoważnienia

Na podstawie art. 37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016, poz. 922)

w związku z:

.....

.....

.....

cofam upoważnienie

Pana/Pani.....
zatrudnionego/ zatrudnionej w.....
.....
na stanowisku.....

.....

do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych.

Legionowo, dnia.....

b9

Załącznik Nr 4

(WZÓR)

Wykaz budynków, pomieszczeń lub części pomieszczeń w których przetwarzane są dane

Lp.	Nr pokoju	Nazwa biura	Określenie części pomieszczenia, w którym przetwarza się, lub archiwizuje dane
Budynek SPP „Nadzieja" w Legionowie, ul. Marszałka Józefa Piłsudskiego 3			
1	1	Biuro Projektu / Biuro Powiatowego Centrum Integracji Społecznej w Legionowie	Przenośny nośnik informacji (dane w wersji elektronicznej) / szafa zamykana na klucz (dane w wersji papierowej)

Załącznik Nr 5 z dnia 01.06.2017
a)

(WZÓR)

Wykaz zbiorów przetwarzanych elektronicznie

Lp.	Nazwa zbioru	Program zastosowany do przetwarzania	Pomieszczenie, w którym przetwarza się dane	Nazwa urządzenia, w którym znajdują się dane osobowe	Osoby przetwarzające dane
1	Zbiór uczestników Powiatowego Centrum Integracji Społecznej w Legionowie	Excel	Biuro PCIS	Komputer przenośny, laptop	Aleksandra Muskała Ewa Ferenc Marek Markowski Anna Elert-Markowska Małgorzata Więch Daniel Twardo Anna Wojtas Agnieszka Kalinowska

hO

Załącznik Nr 5 z dnia 01.06.2017

b)

(WZÓR)

Wykaz zbiorów przetwarzanych w inny sposób niż elektronicznie

Lp.	Nazwa zbioru	Cel przetwarzania danych	Osoby przetwarzające dane	Rodzaj danych	Pomieszczenie, w którym przetwarza się dane
1	Zbiór uczestników Powiatowego Centrum Integracji Społecznej w Legionowie	Dokumentacja uczestnika	Ewa Ferenc Aleksandra Muskała Małgorzata Więch Agnieszka Kalinowska	Dane wynikające ze stosowania ustawy o zatrudnieniu socjalnym	Biuro PCIS
2	Zbiór uczestników Powiatowego Centrum Integracji Społecznej w Legionowie	Dokumentacja związana z wykonywaną pracą (listy obecności, wnioski urlopowe itd.)	Marek Markowski Ewa Ferenc Daniel Twardo Anna Wojtas	Dane osobowe związane z ewidencją pracy	Warsztaty zawodowe PCIS

Załącznik Nr 6

Opis struktury zbiorów danych

Zgodnie z § 4 pkt 3 rozporządzenia 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 informacyjne służące do przetwarzania danych osobowych (Dz. U. 2004 Nr 100, poz. 1024), dla każdego zidentyfikowanego zbioru danych powinien być wskazany opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze. Opisy poszczególnych pól informacyjnych w strukturze zbioru danych powinny jednoznacznie wskazywać jakie kategorie danych są w nich przechowywane.

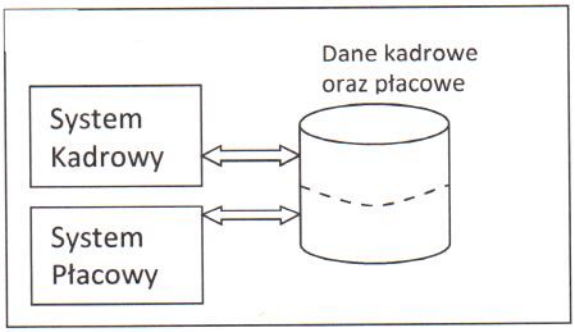
Opis struktury zbioru danych powinien znajdować się w dokumentacji technicznej eksploatowanych systemów. Dokumentacja może być załączona w formie elektronicznej lub papierowej.

Załącznik Nr 7

Sposób przepływu danych pomiędzy systemami

1. W Powiatowym Centrum Integracji Społecznej w Legionowie nie istnieją żadne relacje pomiędzy różnymi systemami informatycznymi.

2. W przypadku zmiany stanu opisanego w punkcie 1 należy przedstawić w tym załączniku sposób współpracy pomiędzy różnymi systemami informatycznymi oraz relacje, jakie istnieją pomiędzy danymi zgromadzonymi w zbiorach do przetwarzania, których systemy te są wykorzystywane. Przedstawiając przepływ danych można posłużyć się np. schematami, jak na rys. 1, które wskazują, z jakimi zbiorami dany system lub moduł systemu współpracuje, czy przepływ informacji pomiędzy zbiorem danych a systemem informatycznym jest jednokierunkowy, np. informacje pobierane są tylko do odczytu, czy dwukierunkowy (do odczytu i do zapisu). W sposobie przepływu danych pomiędzy poszczególnymi systemami należy zamieścić również informacje o danych, które przenoszone są pomiędzy systemami w sposób manualny (przy wykorzystaniu zewnętrznych nośników danych), lub półautomatycznie – za pomocą teletransmisji (przy wykorzystaniu specjalnych funkcji eksportu/importu danych), wykonywanych w określonych odstępach czasu.



Przykładowy przepływ danych między systemami

Załącznik Nr 8

Opis rejestracji baz danych

W przypadku konieczności przetwarzania danych w nowej bazie danych, wymagana jest konsultacja z Administratorem Bezpieczeństwa Informacji (ABI). W przypadku konieczności rejestracji bazy danych w Generalnym Inspektoracie Danych Osobowych, rejestracja następuje na wniosek Dyrektora PCIS.

W Powiatowym Centrum Integracji Społecznej w Legionowie prowadzone są dokumentacje opisujące bazy danych osobowych przetwarzanych w PCIS. Dokumentacja winna zawierać:

c. nazwę bazy,
d. imię i nazwisko osoby tworzącej,
e. datę utworzenia,
f. ewentualną datę zakończenia przetwarzania danych,
g. podstawę prawną przetwarzania,
h. cel przetwarzania,
i. listę osób przetwarzających dane,
j. zakres danych osobowych zawartych w bazie,
k. przewidywany czas użytkowania bazy (stały, okresowy, jednorazowy),
l. informacje o ewentualnym przekazywaniu danych (komu, kiedy, w jakim celu, podstawa prawna, jaki zakres przekazania danych),
m. dodatkowe ważne informacje (zmiany osób uprawnionych itp.).

Załącznik Nr 9

Opis zabezpieczeń systemów informatycznych

W celu ochrony przed utratą danych w Powiatowym Centrum Integracji Społecznej w Legionowie stosowane są następujące zabezpieczenia:

a) odrębne zasilanie sprzętu komputerowego,

b) ochrona serwerów przed zanikiem (wahaniami) zasilania poprzez stosowanie zasilaczy zapasowych UPS,

c) ochrona newralgicznych elementów sieciowych (switch'y) przed zanikiem zasilania,

d) ochrona przed utratą zgromadzonych danych przez robienie codziennych kopii zapasowych na taśmach magnetycznych, z których w przypadku awarii odtwarzane są dane i system operacyjny,

e) ochrona przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych (mirroring),

Uszkodzenie jakiegokolwiek z dysków zestawu nie spowoduje utraty danych, a nawet zatrzymania pracy systemu (zastosowanie elementów hotswap i hotspare).

Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Powiatowego Centrum Integracji Społecznej w Legionowie:

a) wszystkie gniazdka lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenie (zkrosowanie) danego użytkownika do szkieletu sieci komputerowej dokonuje Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona,

b) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa z wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie mają być udostępnione,

c) w systemie informatycznym Powiatowego Centrum Integracji Społecznej w Legionowie zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do komputera Powiatowym Centrum Integracji Społecznej w Legionowie podając login oraz hasło, drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika oraz hasło. Dostęp do wybranej bazy danych uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego.

Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Powiatowym Centrum Integracji Społecznej w Legionowie poprzez Internet.

W zakresie dostępu do sieci wewnętrznej Powiatowym Centrum Integracji Społecznej w Legionowie z rozległej sieci Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz.
Zastosowano firewall na routerze, który ma za zadanie uwierzytelnianie źródła przychodzących pakietów oraz ich filtrowanie w oparciu o adres IP i inne parametry. Zablokowano wszystkie nieużywane porty celem zmniejszenia potencjalnych luk, które mogą być wykorzystane przez osobę próbującą uzyskać nieautoryzowany dostęp do sieci wewnętrznej. Ruch pakietów, oraz otwarte porty zostały określone przez Administratora Bezpieczeństwa.

Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez router. dostęp do sieci zewnętrznej jest ustalony indywidualnie na wniosek pisemny, lub ustny użytkownika.
Oprócz filtra pakietów (firewall) zastosowano system wykrywający obecność wirusów w poczcie elektronicznej.
W efekcie zapewnione jest:

- zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wszystkich zbędnych portów,
- objęcie ochroną antywirusową wszystkich danych ściąganych z sieci Internet na stacjach lokalnych,
- zapisywanie do logów połączeń użytkowników z siecią Internet.

49

Załącznik Nr 10

Wzór raportu z naruszenia zasad bezpieczeństwa systemu informatycznego w Powiatowym Centrum Integracji Społecznej w Legionowie

Wzór

Raport nr ...../.....
z naruszenia bezpieczeństwa systemu informatycznego w Powiatowym Centrum Integracji Społecznej w Legionowie

1. Data:..... Godzina:.....
(dd.mm.rrrr) (00:00)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię i Nazwisko, stanowisko służbowe, nazwa użytkownika jeśli występuje)

3. Osoba przyjmująca zgłoszenie o zaistniałym zdarzeniu:

.....
(Imię i Nazwisko, stanowisko służbowe, nazwa użytkownika jeśli występuje)

4. Lokalizacja zdarzenia:

.....
(np. nr pokoju; nazwa pomieszczenia)

5. Rodzaj naruszenia bezpieczeństwa, oraz okoliczności towarzyszące:

.....

.....

.....

6. Podjęte działania:

.....

.....

7. Przyczyny wystąpienia zdarzenia:

.....

.....

8. Postępowanie wyjaśniające:

.....

.....

9. Ocena skuteczności przeprowadzonego postępowania naprawczego:

.....

.....

10. Podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości podobnym naruszeniom ochrony danych osobowych:

.....

.....

.....

data, podpis Administratora Bezpieczeństwa Informacji

Załącznik Nr 11 z dnia 01.06.2017

(WZÓR)

Wzór wykazu osób które zapoznały się z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Powiatowym Centrum Integracji Społecznej w Legionowie

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Powiatowym Centrum Integracji Społecznej w Legionowie", przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.

Przyjąłem/am/ do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

Nr Upoważnienia	Nazwisko i Imię	Data nadania	Podpis upoważnionego	Data odebrania	Podpis odbierającego
052014	Marek Markowski	01.09.2014			
022015	Ewa Ferenc	01.07.2015			
012015	Aleksandara Muskała	16.03.2015			
012016	Anna Elert-Markowska	03.08.2016			
032016	Małgorzata Więch	24.10.2016			
072017	Daniel Twardo	11.05.2017			
052017	Anna Wojtas	01.06.2017			
062017	Agnieszka Kalinowska	01.06.2017			

LG

POŚWIADCZENIE ZAPOZNANIA SIĘ Z DOKUMENTEM

Nazwa dokumentu: **Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych, wprowadzona Zarządzeniem Dyrektora Powiatowego Centrum Integracji Społecznej w Legionowie z dnia 01.06.2017 r.**

Zapoznałem/am się z treścią dokumentu i przyjmuję do stosowania

Lp.	NAZWISKO I IMIĘ PRACOWNIKA	STANOWISKO	DATA I PODPIS
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			