# INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

# BAZA MONITORUJĄCA

Spis treści

[INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM 1](#_Toc375072411)

[BAZA MONITORUJĄCA 1](#_Toc375072412)

[1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności: 3](#_Toc375072413)

[2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem 4](#_Toc375072414)

[3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu 4](#_Toc375072415)

[4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania 5](#_Toc375072416)

[5. Sposób, miejsce i okres przechowywania: 5](#_Toc375072417)

[a) elektronicznych nośników informacji zawierających dane osobowe, 5](#_Toc375072418)

[b) kopii zapasowych, o których mowa w pkt. 4, 5](#_Toc375072419)

[6. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia 6](#_Toc375072420)

[7. Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia 6](#_Toc375072421)

[8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych. 6](#_Toc375072422)

Niniejsza instrukcji określa sposób zarządzania systemem informatycznym – BAZA monitorująca, zwanym dalej systemem, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

Instrukcja stanowi wykonanie obowiązku, o którym mowa w § 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 informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 ze zm.).

System BAZA monitorująca jest używany do monitoringu działań konsorcjum organizacji pozarządowych.

Instrukcja niniejsza została zatwierdzona przez Administratora Danych Osobowych i przyjęta do stosowania jako obowiązujący dokument dnia ……………………..

Zawarte w instrukcji procedury powinny być przekazane osobom odpowiedzialnym w jednostce za ich realizację stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności. Np. zasady i procedury nadawania uprawnień do przetwarzania danych osobowych, czy też sposób prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych powinny być przekazane osobom zarządzającym organizacją przetwarzania danych, zaś sposób rozpoczęcia i zakończenia pracy, sposób użytkowania systemu, czy też zasady zmiany haseł - wszystkim osobom będącym jego użytkownikami. Zasady ochrony antywirusowej, a także procedury wykonywania kopii zapasowych – osobom zajmującym się techniczną eksploatacją i utrzymaniem ciągłości pracy systemu.

## Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności:

1. Osobą odpowiedzialną za nadawanie uprawnień, rejestrowanie i wyrejestrowywanie użytkowników, realizację uprawnień i ustalonych procedur w systemie informatycznym jest Administrator Bezpieczeństwa Informacji ( w skrócie ABI).
2. Użytkownikiem systemu informatycznego (osoba upoważniona) może być:
3. Osoba, której jednym z zadań jest przetwarzanie danych osobowych, która posiada upoważnienie do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład,
4. Pracownik innego podmiotu lub przedsiębiorca będący osobą fizyczną prowadzący działalność na podstawie wpisu do ewidencji działalności gospodarczej, którzy świadczą na podstawie stosowanych umów usługi związane z ich pracą w systemie informatycznym (serwis, zlecenie przetwarzania danych osobowych itp.).
5. Uzyskanie uprawnień następuje na kilku poziomach:
6. Wniosku przesłanego w formie pisemnej lub mailowej o nadanie uprawnień przez bezpośredniego przełożonego Użytkownika do ABI
7. Nadaniu pisemnego upoważnienia do przetwarzania danych osobowych
8. Podpisaniu przez użytkownika oświadczenia o przetwarzaniu danych osobowych
9. Zarejestrowania w sieci komputerowej (założenie konta)
10. Nadanie określonych uprawnień do systemów aplikacyjnych
11. Uprawnienia są nadawane lub blokowane przez ABI na pisemną (mailową) prośbę bezpośredniego przełożonego Użytkownika zatwierdzoną przez Administratora Danych Osobowych.
12. Określając przeznaczenie uprawnienia należy wskazać tylko taki zakres funkcji systemu informatycznego, z jakiego Użytkownik będzie faktycznie korzystać. Wskazanie zakresu szerszego niż praktycznie wykorzystywany może być potraktowane jako podanie nieprawdziwych danych.
13. Administrator Danych Osobowych, analizuje prośbę o nadanie dostępu, m.in. pod kątem zgodności z wymogami ustaw o ochronie danych osobowych i ostatecznie ją zatwierdza.
14. Po spełnieniu wyżej wymienionych warunków ABI tworzy login i hasło nowemu użytkownikowi, a także rejestruje go w systemie, login i hasło są przekazywane użytkownikowi w formie ustnej.
15. W przypadku stwierdzenia niewłaściwego, niezgodnego z treścią wniosku wykorzystania dostępu Administrator Bezpieczeństwa Informacji oraz Administrator Danych Osobowych są uprawnieni do zablokowania dostępu tego Użytkownika do funkcji i zasobów systemu informatycznego.
16. W przypadku ustania umowy z Użytkownikiem ABI bezzwłocznie usuwa lub blokuje konta tego Użytkownika.
17. Zasady administrowania systemem w przypadkach awaryjnych:
18. W przypadku nieobecności ABI, przekazuje on swoje obowiązki ADO lub innej osobie, która podpisuje należyte oświadczenie
19. W innych przypadkach awaryjnych, nastąpi zebranie przedstawicieli wszystkich Administratorów Danych Osobowych i zostanie ustalona oraz spisana procedura postępowania w danym przypadku
20. Użytkownikami uprzywilejowanymi, czyli osobami posiadającymi uprawnienia na poziomie administratorów systemów informatycznych mogą być tylko ABI lub ADO. Osoby te muszą zmienić hasło w ciągu pięciu dni od nadania.

## Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Użytkownicy systemu informatycznego są zobowiązani chronić przed nieuprawnionym wykorzystaniem wszelkie znane im lub będące w ich posiadaniu dane umożliwiające dostęp do zasobów systemu informatycznego. Oznacza to m.in. zakaz ujawniania komukolwiek haseł umożliwiających dostęp do kont lub innych zasobów.
2. Każdorazowe uwierzytelnianie użytkownika w systemie następuje po podaniu identyfikatora i hasła.
3. Używanie haseł jest obowiązkowe dla każdego użytkownika, posiadającego identyfikator w systemie.
4. Obowiązują następujące zasady korzystania z haseł:
5. Zabrania się ujawniania haseł innym osobom,
6. Zabrania się zapisywania haseł lub takiego z nimi postępowania, które umożliwia lub ułatwia dostęp do haseł innych osób,
7. Minimalna długość hasła powinna wynosić 8 znaków,
8. Hasło powinno składać się z małych i dużych liter, cyfr lub znaku nie będącego literą ani cyfrą,
9. Posługiwanie się danymi identyfikującymi lub uwierzytelniającymi należącymi do innego użytkownika w celu dostępu do zasobów systemu informatycznego na jego konto lub podejmowania jakichkolwiek innych działań w jego imieniu jest nielegalne, również za zgodą właściwego użytkownika. Nielegalne jest też korzystanie z plików lub innych zasobów innego użytkownika bez jego zgody, nawet jeśli nie są one należycie chronione.
10. Użytkownicy systemu informatycznego korzystający także z innych systemów informatycznych nie mogą posługiwać się przy tym takimi samymi lub tymi samymi informacjami uwierzytelniającymi jak stosowane w celu dostępu do zasobów systemu informatycznego. Jeśli użytkownik systemu informatycznego posiadał wcześniej konto w innym systemie, to nie wolno mu użyć w systemie informatycznym takiej samej nazwy hasła.
11. Użytkownik otrzymuje hasło w formie ustnej, system wymusza zmianę hasła co 30 dni, Użytkownik natychmiast po otrzymaniu musi je zmienić.
12. Hasło w systemie informatycznym jest przechowywane w postaci zaszyfrowanej.
13. Awaryjne użycie haseł użytkowników uprzywilejowanych jest każdorazowo odnotowywane przez ABI. Ich hasła są przechowywane w specjalnej zamkniętej kopercie, w szafce zamykanej na klucz, z dostępem tylko przez tych użytkowników.

## Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

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. W przypadku naruszenia ochrony danych osobowych, czy też niemożności zalogowania się na swoje konto Użytkownik niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji lub Administratora Danych Osobowych.
2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
3. włączenia komputera,
4. sprawdzenia aktualności programu antywirusowego na tym komputerze,
5. upewnienia się, że sposób korzystania z tego urządzenia nie umożliwia wglądu w wyświetlane dane osobom trzecim i nieuprawnionym (oznacza to m.in. zakaz stosowania podczas zalogowania do systemu udostępnionego pulpitu, umiejscowienie ekranu w sposób uniemożliwiający dostęp do wyświetlanych treści osobom trzecim)
6. uwierzytelnienia się („zalogowania” w systemie) za pomocą identyfikatora i hasła.
7. Niedopuszczalne jest uwierzytelnianie się na hasło i identyfikator innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.
8. Zakończenie pracy użytkownika w systemie następuje po „wylogowaniu się” z systemu. Operacja wyrejestrowania się z systemu informatycznego po zakończeniu pracy w tym systemie jest obowiązkowa. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności dyskietki, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych.
9. W przypadku dłuższego opuszczenia stanowiska pracy, użytkownik zobowiązany jest „wylogować się” lub zaktywizować wygaszacz ekranu z opcją ponownego „logowania” się do systemu.
10. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania („logowaniu się” w systemie), użytkownik niezwłocznie powiadamia o nich ABI.
11. Wszelkie wydruki z systemu informatycznego powinny być zabezpieczone i nie mogą być przekazywane osobom trzecim nie posiadającym do tego uprawnienia
12. System automatycznie wylogowuje Użytkownika po dłuższym braku aktywności

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

1. Kopie zapasowe są tworzone, przechowywane i wykorzystywane z uwzględnieniem następujących zasad:
2. kopie awaryjne konfiguracji systemu należy wykonywać na nośniku magnetycznym lub optycznym przy pomocy programów standardowych średnio raz w miesiącu,
3. kopie awaryjne konfiguracji usług należy wykonywać po każdej zmianie konfiguracji usługi, np. po utworzeniu, rekonfiguracji lub usunięciu konta użytkownika czy też utworzeniu, rekonfiguracji lub usunięciu katalogu grupowego lub informacyjnego. Należy w tym celu skopiować na nośnik zawartość katalogów,
4. nośniki z kopiami archiwalnymi i awaryjnymi są przechowywane w zamykanej szafie, do której dostęp posiadają tylko osoby uprawione do przetwarzania danych osobowych, a gdy tracą już swoją przydatność są trwale pozbawione zapisu danych i/ lub niszczone w sposób uniemożliwiający odczytanie danych,
5. za tworzenie i przechowywanie kopii awaryjnych odpowiada ABI,
6. Użytkownicy systemu informatycznego powinni sami dbać o wykonywanie i przechowywanie kopii archiwalnych, stosownie do własnych potrzeb,
7. kopie są okresowo, przynajmniej raz w miesiącu, sprawdzane w środowisku testowym pod kątem ich przydatności do odtwarzania danych, a jeżeli ustanie ich użyteczność są niezwłocznie usuwane.

## 5. Sposób, miejsce i okres przechowywania:

## a) elektronicznych nośników informacji zawierających dane osobowe,

## b) kopii zapasowych, o których mowa w pkt. 4,

1. Wydruki i dokumenty papierowe zawierające dane osobowe przechowywane są wyłącznie w odrębnych zamykanych szafach, w pomieszczeniach przeznaczonych do przechowywania danych osobowych, do których dostęp mają tylko osoby upoważnione do przetwarzania danych osobowych.
2. Osoba upoważniona do przetwarzania danych osobowych sporządzająca wydruk zawierający dane osobowe ma obowiązek na bieżąco sprawdzać przydatność wydruku w wykonywanej pracy, a w przypadku jego nieprzydatności – niezwłocznie zniszczyć wydruk w niszczarce.
3. Elektroniczne nośniki informacji z danymi osobowymi są oznaczane i przechowywane w zamykanych szafach lub sejfach do których dostęp mają wyłącznie upoważnieni pracownicy.
4. Fizyczna likwidacja zniszczonych lub niepotrzebnych elektronicznych nośników informacji z danymi osobowymi odbywa się komisyjnie w sposób uniemożliwiający odczyt danych osobowych.
5. 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.

## Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia

1. Sprawdzanie obecności szkodliwego oprogramowania dokonywane jest poprzez zainstalowanie programu, który skanuje automatycznie, bez udziału użytkownika, na obecność szkodliwego oprogramowania wszystkie pliki. Program jest zainstalowany na wszystkich serwerach i stacjach roboczych.
2. Po każdej naprawie, konserwacji komputera należy dokonać sprawdzenia pod kątem występowania szkodliwego oprogramowania.
3. Elektroniczne nośniki informacji pochodzenia zewnętrznego podlegają sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich. Dane uzyskiwane drogą teletransmisji należy umieszczać – przed otwarciem – w katalogu przejściowym, który podlega sprawdzeniu.
4. W celu ochrony przed przedostaniem się szkodliwego oprogramowania na komputerach, z których obsługiwany jest system powinna być zainstalowana zapora FIREWALL. Dodatkowo, ze względu na niebezpieczeństwo przedostania się szkodliwego oprogramowania z sieci Internet, system będzie obsługiwany jedynie w sieciach wewnętrznych, zabezpieczonych hasłem.
5. Program antywirusowy zainstalowany na stacji, z której będzie obsługiwany system, powinien być aktualizowany średnio raz w tygodniu. Osobą odpowiedzialną za zarządzanie tym systemem jest ABI.
6. W przypadku, gdy w przypadku, gdy oprogramowanie zabezpieczające wskazuje zaistnienie zagrożenia Użytkownik powinien niezwłocznie usunąć niebezpieczne pliki, ponownie przeskanować komputer, a także zawiadomić ABI o zaistniałym fakcie.

## Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia

1. System odnotowuje informacje o udostępnieniach danych Użytkownikom – zapisując wszystkie wykonywane czynności, m.in. komu, kiedy i w jakim zakresie dane raporty zostały wygenerowane.

## Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Przegląd i konserwacja zbiorów danych dokonywane są nie rzadziej niż raz w miesiącu, poprzez:
2. badanie spójności bazy danych,
3. uruchamianie zapytań do bazy danych w celu analizy danych,
4. przegląd wydruków po wyznaczonych procesach,
5. sprawdzanie zgodności danych z dokumentami,
6. analiza zgłaszanych uwag Użytkowników.
7. Przeglądu i konserwacji dokonuje wyznaczony pracownik w porozumieniu z Administratorem Bezpieczeństwa Informacji lub Administrator Danych Osobowych.
8. W przypadku zlecenia czynności, o których mowa wyżej, podmiotowi zewnętrznemu, wszelkie prace powinny odbywać się pod nadzorem Administratora Systemu Informacji na postawie sporządzonej uprzednio umowy.
9. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy, należy pozbawiać wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie, bądź też naprawiać je pod nadzorem osoby upoważnionej przez Administratora Danych Osobowych.

*Każdy Użytkownik systemu informatycznego jest zobowiązany zapoznać się z treścią niniejszej Instrukcji i przestrzegać jej.*