POLITYKA BEZPIECZENSTWA

INFORMACJA O DOKUMENCIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w Systemach informatycznych stosowanych w sieci wypozyczalniach Wintergroup z siedzibą w Ustroniu Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę. 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", wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych i przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych. Polityka bezpieczeństwa została opracowana na podstawie Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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).

Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:

1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

Polityka bezpieczeństwa obowiązuje wszystkich pracowników. Realizacja postanowień tego dokumentu ma zapewnić ochronę danych osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych.

Postanowienia ogólne

§ 1

1. Użyte w niniejszym dokumencie określania oznaczają:

1) **Administrator danych** – ……,(*imię i nazwisko*)
2) **Identyfikator** - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
3) **Hasło** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym;
4) **Sieć telekomunikacyjna** - sieć telekomunikacyjna w rozumieniu art. 2 pkt. 23 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)

5) **Internet** - sieć publiczna w rozumieniu art. 2 pkt. 22 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne;
6) **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
7) **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
8) **Integralności danych** - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
9) **Raport** - przygotowane przez System informatyczny zestawienia zakresu i treści przetwarzanych danych;
10) **Polityka bezpieczeństwa** – niniejszy dokument;
11) **Poufności danych** - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
12) **Uwierzytelnianie** - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
13) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
14) **Baza danych osobowych** – każdy posiadający strukturę zbiór danych o charakterze osobowym, dostępnych według określonych kryteriów,
15) **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
16) **Usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
17) **System zarządzania bazą danych** – system oprogramowania zawierający mechanizmy zapewniające spójność i bezpieczeństwo danych, sprawny dostęp do danych, środki programistyczne służące do przetwarzania danych, jednoczesny dostęp do danych dla wielu użytkowników, środki pozwalające na regulację dostępu do danych, środki pozwalające na odtworzenie zawartości bazy danych po awarii,
18) **System informatyczny** – zbiór powiązanych ze sobą elementów: serwerów z systemami operacyjnymi, systemu zarządzania bazą danych, baz danych, oprogramowania (programów użytkowych), urządzeń końcowych (komputerów, terminali, urządzeń przenośnych, drukarek) oraz urządzeń służących do komunikacji między sprzętowymi elementami systemu,

§ 2

Polityka bezpieczeństwa jest zgodna z następującymi aktami prawnymi:

1) Ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),

2) Rozporządzeniem 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. Nr 100, poz. 1024).

§ 3

1. Administrator danych realizuje zadania w zakresie ochrony danych, a w szczególności:

1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Administratora,

2) podejmowania stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych,

3) nadzoru i kontroli Systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,

4) fizycznego zabezpieczenia danych osobowych oraz obiektów, w których są gromadzone i przetwarzane.

2. Administrator danych realizuje zadania w zakresie ochrony danych osobowych, a w szczególności poprzez następujące działania:

1) prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych,

2) nadzoruje funkcjonowanie mechanizmów uwierzytelniania użytkowników w Systemie Informatycznym przetwarzającym dane osobowe oraz kontroli dostępu do danych osobowych,

3) nadzoruje wykonywanie kopii zapasowych (awaryjnych), ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,

4) nadzoruje przeglądy, konserwacje oraz uaktualnienia Systemu Informatycznego służącego do przetwarzania danych osobowych,

5) podejmuje stosowne działania zgodnie z niniejszą Polityką Bezpieczeństwa oraz Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych, w przypadku otrzymania informacji o naruszeniu zabezpieczeń Systemu informatycznego lub informacji o zmianach w sposobie działania Systemu informatycznego, programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,

6) przegląda niniejszą Politykę Bezpieczeństwa pod kątem aktualności i stosowalności nie rzadziej niż raz w roku.

Podstawowe zasady związane z przetwarzaniem danych osobowych

§ 4

1. Ochrona danych osobowych przetwarzanych w ……(*nazwa filiali*) obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych w ……(*nazwa filiali*), bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy.
2. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.
3. Zachowanie tajemnicy w zakresie danych osobowych obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu.

4. Administrator danych jest odpowiedzialny za tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji, standardów, zaleceń oraz procedur dotyczących ochrony danych osobowych w ……. (*nazwa filiali)*
5. Polecenia Administratora danych a także innych osób delegowanych i wyznaczonych do działań związanych z ochroną w zakresie ochrony informacji i bezpieczeństwa systemu informatycznego muszą być bezwzględnie wykonywane przez wszystkich pracowników i użytkowników systemu.

§ 5

1. Przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych. Wykaz pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych stanowi **Załącznik nr 1** do niniejszej polityki.
2. W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych), jednak wymaga to zgody indywidualnej Administratora danych. Szczegółowe zasady przetwarzania danych osobowych na komputerach przenośnych określa **Załącznik nr 2** do niniejszej Polityki.
3. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe oraz do pomieszczeń, w których znajdują się serwery baz danych lub przechowywane są kopie zapasowe mogą mieć wyłącznie osoby, które posiadają do tego upoważnienie nadane przez Administratora danych.
4. Przetwarzać dane osobowe może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych.

§ 6

1. Aktualny wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych znajduje się w **Załączniku 3** do niniejszej Polityki.
2. Załącznik ten powinien być aktualizowany po wprowadzeniu do przetwarzania nowych zbiorów danych osobowych lub nowych programów, które je obsługują.

§ 7

1. Aktualny opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi znajduje się w **Załączniku 4** do niniejszej Polityki.
2. W przypadku istnienia więcej niż jednego zbioru danych dla każdego zbioru powinien zostać sporządzony odrębny załącznik do niniejszego dokumentu opatrzony odpowiednio numerem 3a, 3b itd.
3. Każdy załącznik powinien być aktualizowany po wprowadzeniu istotnych zmian w strukturze bazy danych, którą opisuje. W przypadku systemów, które są rozbudowywane wprowadzone zmiany

Opis zdarzeń naruszających ochronę danych osobowych

§ 8

1. Podział zagrożeń:

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

2) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania) - może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

3) Zagrożenia zamierzone - świadome i celowe działania powodujące 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,
- nieuprawnione przekazanie danych,
- bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).

2. Naruszenie lub podejrzenie naruszenia Systemu informatycznego, w którym przetwarzane są dane osobowe następuje w sytuacji:

1) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.,

2) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

3) awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,

4) pojawienia się odpowiedniego komunikatu alarmowego,

5) podejrzenia nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,

6) naruszenia lub próby naruszenia integralności systemu lub bazy danych w tym systemie,

7) pracy w systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych - np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,

8) ujawnienia nieautoryzowanych kont dostępu do systemu,

9) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych np.

- niezabezpieczone pomieszczenia,
- nienadzorowane, otwarte szafy, biurka, regały,
- niezabezpieczone urządzenia archiwizujące,
- pozostawianie danych w nieodpowiednich miejscach – kosze, stoły itp.

Zabezpieczenie danych osobowych

§ 9

Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych, a w szczególności:

1) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
2) zapobieganie przed pobraniem danych przez osobę nieuprawnioną,
3) zapobieganie zmianie, utracie, uszkodzeniu lub zniszczeniu danych,
4) zapewnianie przetwarzanie danych zgodnie z obowiązującymi przepisami prawa.

§ 10

1. Zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe:
   1) wszystkie pomieszczenia, w których przetwarza się dane osobowe, są zamykane na klucz oraz dodatkowo zabezpieczone alarmem……
   2) w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy, dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (na zewnętrznych nośnikach np. typu pendirve, płyta CD/DVD, dysk zewnętrzny, itp.) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe – w szafach metalowych lub pancernych. Klucze od szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych,
   3) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach,
   4) pomieszczenia, w którym zlokalizowane są zbiory danych osobowych, jest nadzorowany *przez pracowników ochrony fizycznej oraz posiada instalację alarmową*.
2. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych następuje poprzez:
   1) podłączenie urządzenia końcowego (komputera, terminala, drukarki) do Sieci informatycznej dokonywane jest przez Administratora danych,
   2) udostępnianie użytkownikowi zasobów sieci (programów i baz danych), następuje na podstawie upoważnienia do przetwarzania danych osobowych,
   3) identyfikacja użytkownika w systemie następuje poprzez zastosowanie pojedynczego uwierzytelnienia (*ustalić z informatykiem)*,
   4) przydzielenie indywidualnego identyfikatora każdemu użytkownikowi Systemu Informatycznego i rejestrowanie przez system czasu logowania użytkownika i rodzaju wprowadzonych przez niego danych,
   5) udostępnianie kluczy od centrum przetwarzania danych (serwerowni) tylko upoważnionym pracownikom,
   6) przechowywanie kopii zapasowych w zamykanej szafie metalowej, ognioodopornej umiejscowionej w odrębnym pomieszczeniu,
   7) stosowanie programu antywirusowego z zaporą antywłamaniową na komputerach ze środowiskiem operacyjnym MS Windows,

8) zabezpieczenie hasłami kont na komputerach, używanie kont z ograniczonymi uprawnieniami do ciągłej pracy,
9) ustawienie monitorów stanowisk przetwarzania danych osobowych w sposób uniemożliwiający wgląd w dane osobom nieupoważnionym.

3. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych poprzez Internet:

1) logiczne oddzielenie Sieci informatycznej (lokalnej), uniemożliwiające uzyskanie połączenia z bazą danych spoza Systemu Informatycznego, jak również uzyskanie dostępu z Systemu do sieci rozległej Internet,
2) zastosowanie dwustopniowego zabezpieczenia Sieci lokalnej:
   1.a) pierwszy stopień ochrony stanowią listy dostępu ACL (Acces Control List) na głównym routerze uniemożliwiające nawiązanie połączenia z jakimkolwiek niewskazanym jawnie komputerem w sieci,
   1.b) drugi stopień ochrony stanowi lokalna brama sieciowa z zainstalowanym systemem typu firewall z funkcją analizy charakteru ruchu sieciowego, uniemożliwiającym nawiązanie połączenia do chronionych komputerów i blokującym ruch o charakterystyce niepożądanej lub mogącej zostać uznanej za szkodliwą. (do weryfikacji z Informatykiem)

4. Zabezpieczenia przed utratą danych osobowych w wyniku awarii:

1) odrębne zasilanie sprzętu komputerowego,
2) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,
3) ochrona przed utratą zgromadzonych danych poprzez cykliczne wykonywanie kopii zapasowych, z których w przypadku awarii odtwarzane są dane i system operacyjny,
4) ochrona przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych, (do weryfikacji z Informatykiem)
5) zapewnienie właściwej temperatury i wilgotności powietrza dla pracy sprzętu komputerowego, poprzez zastosowanie klimatyzatorów,
6) zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w serwerowni gaśnic, okresowo kontrolowanych przez specjalistę,
7) zwiększenie niezawodności serwerów i urządzeń sieciowych poprzez logiczne rozmieszczenie ich w szafach serwerowych.

Kontrola przestrzegania zasad zabezpieczenia danych osobowych

§ 11

1. Administrator danych sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikający z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
2. Administrator danych przeprowadza kontrole roczne oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.

Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 12

1. W przypadku stwierdzenia naruszenia:
   1) zabezpieczenia systemu informatycznego,
   2) technicznego stanu urządzeń,
   3) zawartości zbioru danych osobowych,
   4) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   5) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, kradzież itp.)

każda osoba jest zobowiązana do niezwłocznego powiadomienia o tym fakcie Administratora danych i bezpośredniego przełożonego.

2. Po wykonaniu czynności określonych w pkt. 1 należy:

1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,
4) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego lub aplikacji użytkowej,
5) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
6) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Danych lub osoby upoważnionej.

3. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Danych lub osoba go zastępująca:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy,
   2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   3) jeżeli zachodzi taka potrzeba zleca usuniecie występujących naruszeń, oraz powiadamia odpowiednie instytucje, w tym organy ścigania.

4. Administrator Danych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego **Załącznik nr 5**.

5. Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez zespół powołany przez Administratora danych.

6. Analiza, o której mowa w pkt. 5, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Postanowienia końcowe

§ 14

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, możliwe jest zastosowanie środków dyscyplinarnych.
2. Administrator danych 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 6** do niniejszej Polityki.

SPIS ZAŁĄCZNIKÓW

Załącznik nr 8 Obowiązki pracownicze osób zatrudnionych przy przetwarzaniu danych osobowych wynikające z potrzeby zapewnienia ochrony danych osobowych

Załącznik nr 9 Instrukcja zarządzania systemem Informatycznym służącym do przetwarzania danych osobowych – do weryfikacji z informatykiem

Załącznik nr 10 Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych