INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

W

ELDOMIX ANDRZEJ KONOWALSKI

SPIS TREŚCI

1. CEL INSTRUKCJI

Celem niniejszego dokumentu jest określenie zasad właściwego zarządzania systemem Informatycznym, służącym do przetwarzania danych osobowych. Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez firmę Eldomix Andrzej Konowalski w systemach informatycznych. Zasady te stanowią ochronę danych osobowych przed udostępnieniem ich osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

2. ŹRÓDŁA WYMAGAŃ

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w firmie Eldomix Andrzej Konowalski, zwana dalej „Instrukcją" została opracowana zgodnie z wymogami § 5 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).

3. ZAKRES STOSOWANIA

Instrukcję stosuje się do danych osobowych przetwarzanych w systemach informatycznych, zapisanych w postaci elektronicznej na zewnętrznych nośnikach informacji oraz informacji dotyczących bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych. Instrukcja zawiera specyfikację podstawowych środków technicznych ochrony danych osobowych oraz elementów zarządzania systemem informatycznym.

4. DEFINICJE

Administrator danych – Eldomix Andrzej Konowalski, podmiot, który decyduje o środkach i celach przetwarzania danych osobowych.

ABI - Administrator Bezpieczeństwa Informacji osoba wyznaczona przez Dyrekcję, odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.

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 lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Osoba upoważniona – osoba posiadająca formalne upoważnienie wydane przez Administratora danych lub przez osobę wyznaczoną, uprawniona do przetwarzania danych osobowych.

Przetwarzanie danych osobowych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

System informatyczny – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Ustawa – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

Zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

5. ODPOWIEDZIALNOŚĆ

5.1. Administrator Bezpieczeństwa Informacji

Do obowiązków ABI, należy nadzorowanie przestrzegania zasad ochrony danych osobowych w systemach informatycznych. Do obowiązków należy również:

- nadzór nad stosowaniem środków ochrony w systemach informatycznych;
- nadzór nad przestrzeganiem przez administratorów i użytkowników systemu procedur bezpieczeństwa;
- uzgadnianie z właściwymi administratorami szczególnych procedur regulujących wykonywanie czynności w systemach lub aplikacjach służących do przetwarzania danych osobowych;
- zapewnienie doradztwa w zakresie przestrzegania przez pracowników firm zewnętrznych zasad ochrony danych osobowych przyjętych w firmie Eldomix Andrzej Konowalski

5.2. Administrator

Do obowiązków administratora należy bieżąca ocena ryzyka bezpieczeństwa systemów informatycznych, służących do przetwarzania danych osobowych, za które są odpowiedzialni, identyfikacja podatności na zagrożenia bezpieczeństwa przetwarzania danych osobowych oraz bezpieczne zarządzanie systemami. Do obowiązków należy również:

- zarządzanie kontrolą dostępu do systemów informatycznych
- weryfikacja zdarzeń systemowych
- zarządzanie kontami użytkowników
- wdrażanie mechanizmów bezpieczeństwa przetwarzania danych osobowych
- kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym

- regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania tych kopii zapasowych

5.3. Osoby upoważnione

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej. Do obowiązków należy również:

- współpraca przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu
- przestrzeganie opracowanych dla systemu zasad przetwarzania danych osobowych oraz procedur i instrukcji
- informowanie Administratora Bezpieczeństwa Informacji o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych
- wykonywania bez zbędnej zwłoki poleceń Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

6. ZARZĄDZANIE BEZPIECZEŃSTWEM SYSTEMÓW

6.1. Podstawowe cele zabezpieczeń danych

6.1.1. Podstawowym celem zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych jest zapewnienie jak najwyższego poziomu bezpieczeństwa tych danych, które są w nich przetwarzane.

6.1.2. W celu zachowania odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych, dostęp do systemu informatycznego przetwarzającego dane osobowe jest możliwy wyłącznie po podaniu identyfikatora odrębnego dla każdego użytkownika systemu i poufnego hasła.

6.2. Podstawowe zasady zabezpieczeń systemów

6.2.1. Należy zapewnić poufność, integralność i rozliczalność systemów informatycznych służących do przetwarzania danych osobowych.

6.2.2. Należy zapewnić aby użytkownicy systemów informatycznych służących do przetwarzania danych osobowych nie posiadali wyższych poziomów uprawnień w tych systemach niż wymagane do wykonywania powierzonych obowiązków.

6.3. Prawidłowy poziom zabezpieczeń danych

6.3.1. Prawidłowy poziom zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych zostaje zapewniony poprzez przestrzeganie następujących zasad:

- uniemożliwienie osobom postronnym uzyskiwania nieupoważnionego dostępu do systemu
- instalowanie nowego lub aktualizowanie już zainstalowanego oprogramowania wyłącznie przez uprawnionych użytkowników systemu
- niepodejmowanie przez użytkowników systemu prób testowania, modyfikacji i naruszenia zabezpieczeń systemu lub jakichkolwiek działań noszących takie znamiona.

7. BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH

7.1. Wymagania bezpieczeństwa

7.1.1. Bezpieczeństwo jest integralną częścią systemów informatycznych służących do przetwarzania danych osobowych.

7.1.2. Usługi oraz aplikacje, które nie są wykorzystywane powinny być wyłączone.

7.1.3. Wymagania bezpieczeństwa, na które mogą się również składać wymagania prawne związane z ochroną danych osobowych należy identyfikować i uzgodnić przed opracowaniem i/lub ich wdrożeniem. W szczególności wymagania muszą być zidentyfikowane dla:

- systemów operacyjnych;
- aplikacji
- baz danych
- narzędzi programowych

7.1.4. Aplikacje WWW powinny być zabezpieczone zgodnie z zaleceniami Open Web Application Security Project (OWASP).

7.1.5. Aplikacje WWW przed wdrożeniem należy poddać obiektywnemu przeglądowi bezpieczeństwa mającemu na celu zidentyfikowanie podatności na zagrożenia pochodzące z sieci Internet.

7.2. Zarządzanie systemami informatycznymi

7.2.1. Administrator systemu powinien zarządzać systemami operacyjnymi, urządzeniami sieciowymi korzystając z kont dodatkowych o mniejszych uprawnieniach niż konta główne. Konta główne powinny służyć wyłącznie do zakładania i usuwania kont dodatkowych.

7.2.2. Administrator powinien odnotowywać w prowadzonych rejestrach systemów wszystkie ważne zdarzenia związane z zarządzanym systemem, w szczególności:

- zmiany, np. instalacja nowego oprogramowania;
- okresowe testy i konserwacje;

- incydenty bezpieczeństwa (awarie sprzętu, błędy oprogramowania, naruszenia bezpieczeństwa, zdarzenia losowe, ataki szkodliwego oprogramowania) i sposób ich obsługi;
- fakty zaistnienia kontroli.

7.3. Dokumentacja systemów

7.3.1. Należy prowadzić dokumentację eksploatowanych systemów informatycznych w celu zapewnienia oczekiwanej funkcjonalności, jakości, dostępności i bezpieczeństwa systemów.

7.3.2. Dokumentacja systemów powinna być aktualizowana na bieżąco a dostęp do niej ograniczony dla uprawnionych osób na zasadzie wiedzy koniecznej.

7.4. Sposób realizacji wymogów § 7 ust. 1 pkt 4

7.4.1. Dla każdego systemu służącego do przetwarzania danych osobowych, z którego udostępniane są dane osobowe odbiorcom danych, należy zapewnić odnotowanie komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione, chyba, że dane pochodzą z jawnego zbioru danych osobowych.

7.4.2. Należy zapewnić dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym sporządzenie zestawień z zakresu i treści przetwarzanych na jej temat danych osobowych

7.4.3. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach, wymagania, o których mowa w § 7 ust. 1 pkt 4 Rozporządzenia, mogą być realizowane w jednej z nich lub w odrębnej aplikacji przeznaczonej do tego celu.

7.4.4. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w aplikacjach ewidencjonujących osoby fizyczne.

7.5. Szkolenia

Użytkownicy systemu podlegają szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (np. wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

8. KONTROLA DOSTĘPU

8.1. Kontrola dostępu do danych

8.1.1. Należy zapobiegać nieautoryzowanemu i nieuprawnionemu dostępowi do systemów informatycznych służących do przetwarzania danych osobowych.

8.1.2. Wszelkie czynności mogące powodować nieuprawniony dostęp do systemów informatycznych są zabronione.

8.1.3. Dane osobowe przechowywane na urządzeniach mobilnych takich jak np. komputerach przenośnych, urządzeniach PDA, telefonach komórkowych są zabezpieczone w sposób zapewniający poufność tym danym.

8.1.4. Serwery oraz stacje robocze są tak skonfigurowane, aby w przypadku nieaktywności użytkownika przez zdefiniowany okres (zalecane 10 minut) uruchamiał się wygaszasz ekranu odblokowywany hasłem.

8.2. Zarządzanie dostępem użytkowników

8.2.1. Dostęp do systemów informatycznych służących do przetwarzania danych osobowych, posiadają tylko i wyłącznie autoryzowani użytkownicy, na podstawie formalnych procedur przyznawania praw dostępu.

8.2.2. Należy zapewnić niezwłoczne odebranie i zablokowanie praw dostępu użytkownikom, którzy nie są już pracownikami lub którzy zakończyli świadczenie usług na podstawie umów, zamówień lub porozumień.

8.2.3. Systemy informatyczne powinny zapewniać blokowanie użytkowników po określonej liczbie nieudanych prób uwierzytelniania (maksymalnie 5 prób).

8.3. Identyfikacja użytkowników

8.3.1. Każdy użytkownik posiada unikalny identyfikator wyłącznie do swojego użytku.

8.3.2. Wydanie innym użytkownikom wykorzystanych wcześniej identyfikatorów jest zabronione.

8.3.3. Konta funkcyjne lub serwisowe należy oznaczyć i zapewnić ich łatwą identyfikację oraz powinny wygasać po określonym czasie.

8.3.4. Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych należy chronić hasłem lub innym bezpiecznym sposobem uwierzytelniania.

8.4. Zarządzanie hasłami

8.4.1. Przydzielanie haseł powinno być kontrolowane za pośrednictwem formalnego procesu zarządzania.

8.4.2. Hasła powinny być dobrej jakości:

- długości co najmniej 8 znaków;
- które są łatwe do zapamiętania, a trudne do odgadnięcia;
- nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.)

8.5. Zmiana haseł

8.5.1. Hasła są regularnie zmieniane, okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła) oraz/lub w przypadku ujawnienia lub podejrzenia ujawnienia hasła.

8.5.2. System operacyjny w firmie Eldomix Andrzej Konowalski nie zapewnia automatycznego wymuszania zmiany haseł, w związku z tym użytkownik zobligował się do samodzielnej zmiany haseł, zgodnie z zasadami przyjętymi dla danego systemu informatycznego.

8.5.4. Hasła należy niezwłocznie zmieniać w przypadkach, gdy cokolwiek mogłoby wskazywać na możliwość naruszenia bezpieczeństwa systemu informatycznego lub hasła.

8.5.5. Należy zapewnić aby wszelkie urządzenia sprzętowe lub programowe, które na początku posiadały hasło domyślne, miały zmienione hasło zgodnie z przyjętymi wymogami dotyczącymi formułowania haseł.

8.6. Zabezpieczenie haseł

8.6.1. Hasła nie powinny być przechowywane w systemach, aplikacjach, bazach danych, skryptach i plikach konfiguracyjnych w postaci jawnej, bez zapewnienia im poufności.
8.6.2. Hasła nie powinny być przesyłane za pomocną narzędzi i usług teleinformatycznych w postaci jawnej, bez zapewnienia im poufności.
8.6.3. Należy stosować bezpieczną procedurę przekazywania haseł użytkownikom np. nieprzesyłanie przez sieć haseł (np. w niechronionych wiadomościach poczty elektronicznej).
8.6.4. Czynności związane z przechwytywaniem lub odgadywaniem haseł innych użytkowników są zabronione.
8.6.5. Hasła należy utrzymywać w tajemnicy również po upływie ich ważności.

8.7. Przegląd oraz weryfikacja kont i uprawnień

8.7.1. Przegląd kont należy przeprowadzać regularnie, co najmniej raz na rok
8.7.2. Należy zapewnić niezwłoczne blokowanie zbędnych kont użytkowników oraz uprawnień.
8.7.3. Konto użytkownika należy zablokować po upływie zdefiniowanego okresu bezczynności (zalecane 60 dni od daty ostatniego użycia).

8.8. Odpowiedzialność użytkowników

8.8.1. Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu przetwarzającego dane osobowe, musi być poprzedzone złożeniem przez użytkownika oświadczenia o zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczania oraz przetwarzaniu danych osobowych zgodnie z przepisami, a także uzyskaniem formalnego upoważnienia do przetwarzania danych osobowych.
8.8.2. Użytkownicy powinni zapobiegać nieuprawnionemu dostępowi, naruszeniu bezpieczeństwa, kradzieży lub systemów informatycznych służących do przetwarzania danych osobowych.
8.8.3. Użytkownicy powinni być świadomi swojej odpowiedzialności za utrzymanie skutecznej kontroli dostępu, szczególnie w odniesieniu do haseł i zabezpieczenia swojego sprzętu.

9. ROZPOCZĘCIE, ZAWIESZENIE I ZAKOŃCZENIE PRACY

9.1. Przed przystąpieniem do pracy z systemem informatycznym, użytkownik systemu zobowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
9.2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest powiadomić o tym fakcie ABI.
9.3. Kończąc pracę, użytkownik systemu obowiązany jest do wylogowania się z systemu informatycznego i zabezpieczenia stanowiska pracy, w szczególności wszelkiej dokumentacji, wydruków oraz elektronicznych nośników informacji, na których znajdują się dane osobowe i umieszczenia ich w zamykanych szafkach.
9.4. Stacje robocze powinny być tak skonfigurowane, aby w przypadku nieobecności użytkownika systemu dłużej niż 10 minut uruchamiał się wygaszasz ekranu

odblokowywany hasłem. Alternatywnie może obowiązywać wymaganie wylogowywania się z systemu lub blokowania stacji roboczej w przypadku chwilowego opuszczenia stanowiska pracy.

10. BEZPIECZEŃSTWO DANYCH

10.1. Poufność

10.1.1. Dane osobowe zapisane w postaci elektronicznej należy przetwarzać wyłącznie na urządzeniach służbowych zabezpieczonych zgodnie z obowiązującymi procedurami.
10.1.2. Należy zapewnić aby wszelkie informacje o systemach informatycznych służących do przetwarzania danych osobowych, których ujawnienie może powodować utratę bezpieczeństwa tego systemu lub danych w nim przetwarzanych nie były ujawniane użytkownikom ani żadnej innej nieuprawnionej osobie za wyjątkiem informacji niezbędnych do prawidłowego korzystania z tych systemów.
10.1.3. Użytkownicy systemów informatycznych służących do przetwarzania danych osobowych nie powinni ujawniać informacji o charakterze, funkcjonalności, zastosowanych środkach kontrolnych, sposobie ich obsługi oraz lokalizacji wykorzystywanych systemów osobom, które nie są uprawnione do otrzymania tego typu informacji.
10.1.4. Dane osobowe powinny być przetwarzane przy użyciu systemów informatycznych zgodnie z zasadą wiedzy koniecznej.

10.2. Kopie zapasowe

10.2.1. Należy utrzymywać dostępność i integralności systemów informatycznych, służących do przetwarzania danych osobowych oraz danych przetwarzanych w tych systemach poprzez wykonywanie kopii zapasowych.
10.2.2. Sposób i zakres (tj. pełna lub różnicowa kopia zapasowa) oraz częstotliwość tworzenia kopii zapasowych powinien odzwierciedlać wymagania biznesowe, wymagania bezpieczeństwa, wymagania prawne oraz stopień krytyczności informacji.
10.2.3. Kopie zapasowe zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania powinny być wykonywane na bieżąco przez Administratora systemu lub inną wyznaczoną do tego celu osobę.
10.2.4. Administrator systemu odpowiedzialny za tworzenie kopii zapasowych zobowiązany jest przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odtworzenia danych zapisanych na tych kopiach pod kątem ewentualnej przydatności w sytuacji awarii systemu.
10.2.5. Kopie zapasowe powinny być tworzone w bezpiecznym systemie archiwizacji, który powinien zapewniać ograniczony dostęp fizyczny do nośników oraz przyznanie uprawnień dostępu tylko wyznaczonym imiennie administratorom systemu.

10.3. Okres przechowywania kopi zapasowych

10.3.1. Okres przechowywania kopi zapasowych zawierających dane osobowe ustalony jest przez osobę kierującą komórką organizacyjną, w której te dane są przetwarzane i przekazany do Administratora systemu odpowiedzialnego za wykonywanie kopii zapasowych.
10.3.2. Kopie zapasowe zawierające dane osobowe, dla których cel przetwarzania ustał powinny być pozbawiane zapisu tych danych a w przypadku gdy nie jest to możliwe, należy je zniszczyć w sposób uniemożliwiający odczytanie/odzyskanie danych osobowych.

10.4. Zabezpieczenie kopi zapasowych

10.4.1. Kopie zapasowe są odpowiednio zabezpieczone przed nieuprawnionym dostępem, nadużyciem lub uszkodzeniem.

10.4.2. Dostęp do kopii zapasowych jest zgodny z nadanymi i autoryzowanymi uprawnieniami.

10.4.3. Procedury niszczenia kopii zapasowych są zgodne z obowiązującymi regulacjami i przepisami prawa.

10.4.4. Kopie zapasowe są własnością firmy Eldomix Andrzej Konowalski, a ich nieuprawnione użycie jest zabronione.

10.5. Zasady postępowania z komputerami przenośnymi

10.6.1. Osoba używająca komputer przenośny zawierający dane osobowe zobowiązana jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.

10.6.2. Osoba używająca komputer przenośny zawierający dane osobowe w szczególności powinna:

- stosować ochronę kryptograficzną wobec danych osobowych przetwarzanych na komputerze przenośnym;
- zabezpieczyć dostęp do komputera na poziomie biosu i systemu operacyjnego - identyfikator i hasło
- nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych
- nie wykorzystywać komputera przenośnego do przetwarzania danych osobowych w obszarach użyteczności publicznej
- zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych.

10.6.3. W przypadku podłączania komputera przenośnego do sieci publicznej poza siecią Administratora danych należy zastosować firewall zainstalowany bezpośrednio na tym komputerze oraz system antywirusowy.

10.6.4. Użytkownik powinien zachować wyjątkową ostrożność podczas korzystania z zasobów sieci publicznej.

11. ZARZĄDZANIE BEZPIECZEŃSTWEM SIECI

11.1. Podstawowe zasady

11.1.1. Infrastruktura sieciowa jest właściwie chroniona, adekwatnie do zagrożeń mogących powodować utratę bezpieczeństwa przetwarzania danych osobowych.

11.1.2. Dane osobowe przesyłane poprzez publiczną sieć telekomunikacyjną są zabezpieczone środkami kryptograficznej ochrony.

11.1.3. Administrator systemu, chroni system przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, poprzez kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;

11.1.4. Wewnętrzna adresacja IP, konfiguracja oraz informacja o systemach powiązanych nie jest ujawniana osobom nieuprawnionym, bez akceptacji ze strony uprawnionej do tego celu osoby.

11.1.5. Podłączanie do infrastruktury sieciowej nieautoryzowanych urządzeń takich jak modemy, urządzenia sieciowe, w tym urządzenia sieci bezprzewodowych jest zabronione.

11.1.6. Podłączanie we własnym zakresie stacji roboczych do publicznej sieci telekomunikacyjnej poprzez nieautoryzowane urządzenia sieciowe, będąc jednocześnie podłączymy do infrastruktury lokalnej LAN jest zarobione.
11.1.7. Zastosowano specjalne zabezpieczenia (np. kryptograficzne środki ochrony) w celu ochrony integralności i poufności danych przesyłanych przez sieci bezprzewodowe.

11.2. Polityka dotycząca korzystania z usług sieciowych
11.2.1. Użytkownikom należy zapewnić dostęp tylko do tych usług infrastruktury teleinformatycznej (np. dostęp do Internetu, zdalny dostęp, poczta elektroniczna), do których zostali autoryzowani.
11.2.2. Osoby nie będące pracownikami, nie posiadają nieautoryzowanego i niekontrolowanego dostępu do infrastruktury teleinformatycznej.
11.2.3. Niezabezpieczone usługi infrastruktury teleinformatycznej, pozwalające przesyłać hasła w postaci niezabezpieczonej np. telnet lub ftp, nie są wykorzystywane i są zablokowane.

11.3. Bezpieczeństwo sieci bezprzewodowych
11.3.1. Sieci bezprzewodowe podłączone do infrastruktury teleinformatycznej są autoryzowane, udokumentowane, monitorowane oraz odpowiednio zabezpieczone.
11.3.2. Wszystkie urządzenia sieci bezprzewodowych, do których podłączane są systemy informatyczne, powinny być zatwierdzone przez ABI poprzez bezpieczne protokoły szyfrowania i uwierzytelniania.
11.3.3. Wszystkie urządzenia sieci bezprzewodowych podłączone do infrastruktury informatycznej, powinny wykorzystywać bezpieczne protokoły komunikacyjne z zaawansowaną funkcją szyfrowania (AES) o długości klucza co najmniej 128 bitów.

11.4. Polityka dotycząca korzystania z Internetu
11.4.1. Wykonywane połączenia do Internetu są monitorowane i rejestrowane.
11.4.2. Systemy monitorowania połączeń do Internetu rejestrowują źródłowy adres IP, datę i godzinę połączenia, wykorzystywany protokół, docelową witrynę lub urządzenie (adres IP) oraz nazwę użytkownika nawiązującego połączenie.
11.4.3. Dostęp do Internetu jest zabezpieczony, poprzez zastosowanie narzędzi służących do blokowania stron internetowych lub usług zawierających niepożądane treści lub zawartość, np. takie jak: materiały o charakterze pornograficznym, nielegalnym, obraźliwym, szkodliwe oprogramowanie oraz usługi udostępniania plików.
11.4.4. Wszystkie pliki ściągnięte z Internetu sprawdzane są przez system antywirusowy.
11.4.5. Użytkownicy zostali uświadamiani o zagrożeniach występujących podczas korzystania z Internetu.
11.4.6. Użytkownicy nie powinny instalować żadnego oprogramowania ściągniętego z Internetu bez upewniania się czy został on ściągnięty z zaufanej strony oraz czy nie zagraża bezpieczeństwu systemów informatycznych.

11.5. Polityka dotycząca korzystania z poczty elektronicznej
11.5.1. Użytkownicy zostali poinformowani, że poczta elektroniczna nie może być wykorzystywana do przesyłania informacji zawierających treści obraźliwe, szkodliwe, nielegalne, pornograficzne, dotyczących przekonań politycznych i uprzedzeń rasowych.
11.5.2. Wykorzystywanie prywatnych skrzynek pocztowych, znajdujących się poza domeną pocztową firmy Eldomix Andrzej Konowalsk, do przesyłania informacji

służbowych jest niedozwolone, chyba że zastosowano właściwe zabezpieczenia uzgodnione wcześniej z ABI.
11.5.3. Przychodzące i wychodzące wiadomości poczty elektronicznej należy sprawdzać na wypadek występowania wirusów i kodów złośliwych a potencjalne niebezpieczne załączniki należy blokować.
11.5.4. Wiadomości poczty elektronicznej otrzymane z nieznanych i podejrzanych źródeł nie powinny być otwierane i przekazywane dalej.
11.5.5. Wewnętrzne adresy poczty elektronicznej nie powinny być udostępniane i ujawniane osobom nieuprawnionym.
11.5.6. Wewnętrzna lista adresowa powinna być zabezpieczona przed nieautoryzowanym dostępem i modyfikacją.

12. SZKODLIWE OPROGRAMOWANIE

12.1. Podstawowe zasady
12.1.1. Systemy informatyczne należy chronić przed szkodliwym oprogramowaniem (np. wirusy, trojany, bomby logiczne, robaki) poprzez stosowanie odpowiednich środków technicznych i organizacyjnych.
12.1.2. Oprogramowanie antywirusowe należy aktywować na wszystkich serwerach, stacjach roboczych oraz na stacjach roboczych i serwerach połączonych za pomocą zdalnego dostępu.
12.1.3. Zastosowane zabezpieczenia ochrony antywirusowej powinny być adekwatne dla danego zasobu teleinformatycznego lub usługi.
12.1.4. Oprogramowanie antywirusowe powinno być zainstalowane tak aby użytkownik systemu nie był w stanie wyłączyć lub pominąć etapu skanowania.
12.1.5. Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
12.1.6. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instalują wyznaczone osoby niezwłocznie po ich otrzymaniu lub ściągnięciu, uprzednio weryfikując pochodzenie oprogramowania.

12.2. Aktualizacja
12.2.1. Aktualizacja oprogramowania antywirusowego powinna być przetestowana i zgodna z wymaganiami procesu zarządzania zmianą.
12.2.2. Aktualizacja sygnatur szkodliwego oprogramowania powinna być prowadzona automatycznie. Jeżeli automatyczna dystrybucja nowych sygnatur szkodliwego oprogramowania nie jest możliwa, powinna być prowadzona manualnie, co najmniej raz na tydzień.

13. PRZEGLĄD I MONITOROWANIE SYSTEMÓW

13.1. Przeglądy systemów
13.1.1. Przeglądy, naprawy i konserwacje systemu informatycznego, które będą przeprowadzane w miejscu użytkowania tego systemu wymagają obecności Administratora systemu lub innej wyznaczonej osoby.
13.1.2. W przypadku gdy konieczne jest dokonanie przeglądu, naprawy lub konserwacji systemu informatycznego poza miejscem jego użytkowania, z urządzenia należy wymontować element, na którym zapisane są dane osobowe, o ile jest to możliwe. W

przeciwnym wypadku należy zawrzeć z podmiotem dokonującym naprawy umowę powierzenia w rozumieniu art. 31 ustawy o ochronie danych osobowych.
13.1.3. Osoby nie będące pracownikami, które prowadzą prace serwisowe na rzecz Administratora danych przed rozpoczęciem prac, powinny być poddane weryfikacji tożsamości przez Administratora systemu lub inną wyznaczoną do tego celu osobę.
13.1.4. Przegląd programów i narzędzi programowych powinien być przeprowadzany w przypadku zmiany wersji oprogramowania aplikacji, zmiany wersji oprogramowania bazy danych lub wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.

13.2. Dziennik zdarzeń
13.2.1. Mechanizmy monitorowania i tworzenia dzienników zdarzeń powinny być stosowane w celu umożliwienia rejestracji działań związanych z bezpieczeństwem przetwarzania danych osobowych.
13.2.2. Dziennik zdarzeń powinien odzwierciedlać wymagania biznesowe oraz wymagania bezpieczeństwa przetwarzania danych osobowych. Jako domyślnie dziennik audytu powinien być przechowywany przez min. 6 miesięcy.
13.2.3. Dziennik zdarzeń powinien zawierać w szczególności:
- identyfikator użytkownika, który wygenerował zdarzenie;
- datę, czas i szczegóły ważnych zdarzeń, np. rozpoczęcia i zakończenia pracy w systemie;
- pliki lub obiekty powiązane z wygenerowanym zdarzeniem;
- adres IP źródłowy i docelowy;
- zmiany konfiguracji systemu;
- informację o zdarzeniu.

13.2.4. Zarejestrowane zdarzenia powinny być analizowane w celu identyfikacji problemów związanych z przetwarzaniem danych osobowych oceny skuteczności zaimplementowanych mechanizmów kontrolnych.
13.2.5. Dziennik zdarzeń należy zabezpieczyć przed modyfikacją oraz nieuprawnionym dostępem.
13.2.6. Zapisy w dziennikach zdarzeń należy regularnie przeglądać. Podczas przeglądu należy weryfikować ich integralność.
13.2.7. Dzienniki zdarzeń powinny bazować na poprawnym mechanizmie synchronizacji czasu.

14. POSTANOWIENIA KOŃCOWE
14.1.1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Instrukcji może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
14.1.2. W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz.U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.
14.1.3. Użytkownicy systemu zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji, w wypadku odrębnych od zawartych w niniejszej Instrukcji uregulowań występujących w innych procedurach obowiązujących w firmie Eldomix Andrzej Konowalski użytkownicy systemu mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych przetwarzanych w systemie informatycznym.