ZAŁĄCZNIK NR 2 DO ZARZĄDZENIA WÓJTA GMINY GOŚCIERADÓW
NR 120/2013 Z DNIA 9 kwietnia 1013 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Niniejszy dokument zgodny jest z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. 02.101.926 z późn. zm. oraz 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.04.100.1024)

Spis treści

I. Cel instrukcji

Instrukcja określa sposób zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych, przez Administratora Danych – w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

II. Definicje

Ilekroć w instrukcji zarządzania system informatycznym jest mowa o:

1) **Administratorze Bezpieczeństwa Informacji /ABI/** – rozumie się przez to osobę, której Administrator Danych powierzył pełnienie obowiązków Administratora Bezpieczeństwa Informacji, nadzorującą stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U.02.101.926 z późn. zm) oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, a także przeprowadzająca kontrole w zakresie określonym regulacjami wewnętrznymi Administratora Danych,

2) **Administratorze Danych** – rozumie się przez to Wójta Gminy Gościeradów,

3) **Administratorze Systemu Informatycznego /ASI/**– rozumie się przez to osobę zarządzającą systemem informatycznym w którym przetwarzane są dane osobowe,

4) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

5) **identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

6) **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

7) **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,
   - podmiotu, o którym mowa w art. 31 ustawy,
   - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

8) **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Wójta na piśmie,

9) **pomieszczeniach –** rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w formie dokumentacji papierowej

10) **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

11) **przetwarzaniu danych –** rozumie się przez to 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,

12) **przetwarzającym** – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,

13) **raporcie** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

14) **rozliczalności** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

15) **rozporządzeniu** – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (DzU nr 100, poz. 1024),

16) **sieci publicznej** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (DzU nr 73, poz. 852 ze zm.),

17) **sieci telekomunikacyjnej** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne,

18) **serwisancie** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,

19) **systemie informatycznym** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną Administratora Danych,

20) **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

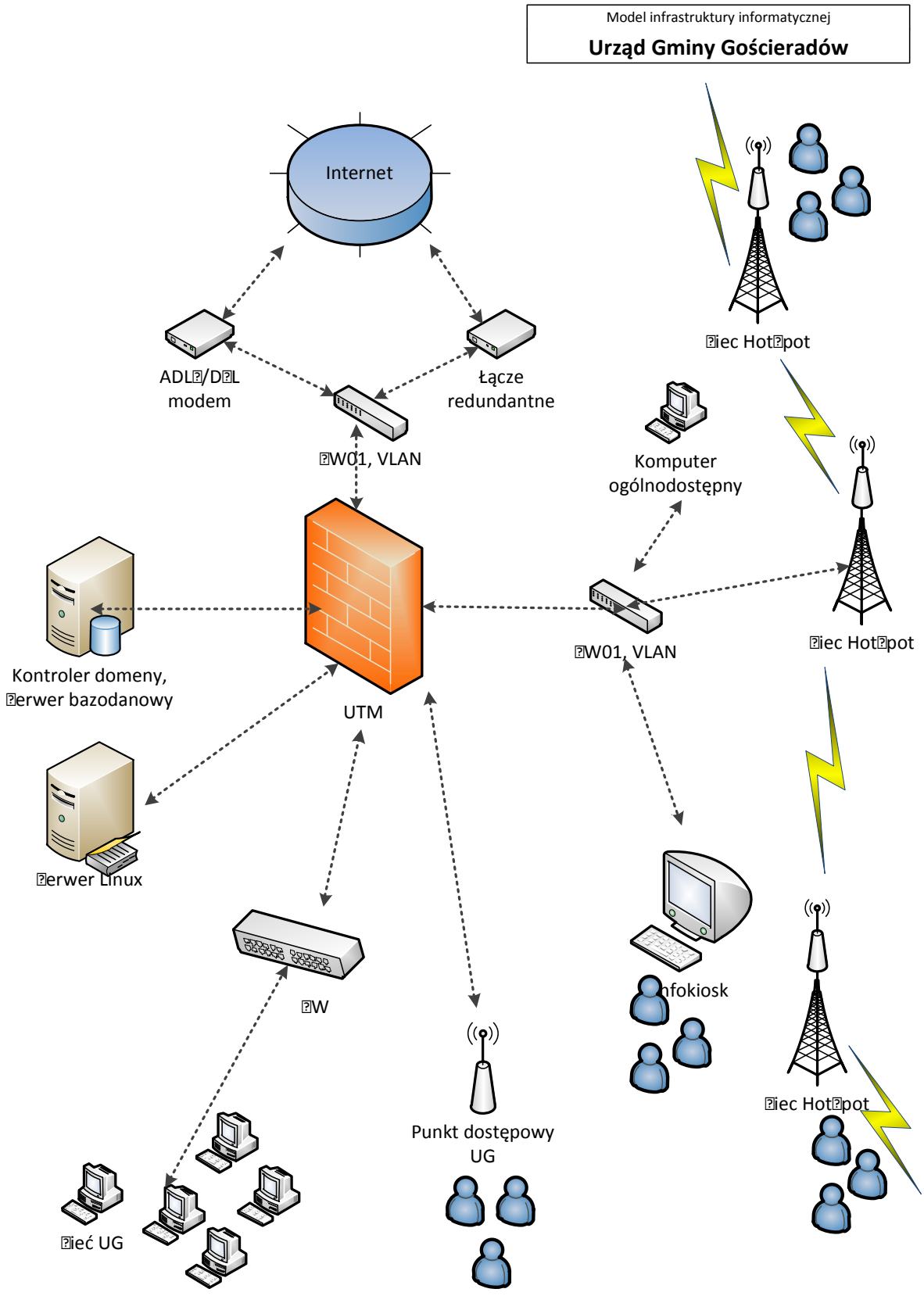
21) **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. DzU z 2002 r. nr 101, poz. 926 ze zm.),

22) **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

23) **użytkowniku** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło,

24) **zbiorze danych –** rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnym według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

III. Model infrastruktury IT



Centralnym elementem sieci jest urządzenie UTM. Zastosowano je aby zapewnić bezpieczeństwo zgromadzonej w Urzędzie informacji. Wymogi ustawy o ochronie danych osobowych wymuszają odseparowanie następujących segmentów sieci:

- serwer (każdy serwer musi być w samodzielnym segmencie),
- sieć LAN Urzędu,
- bezprzewodowy punkt dostępowy do sieci LAN Urzędu dla pracowników Urzędu
- punkty dostępowe dla mieszkańców (HotSpot, Infokiosk)

Zgodnie z wymogami ustawy urządzenie UTM monitoruje i zabezpiecza komunikację pomiędzy siecią wewnętrzną (serwerami, siecią lokalną Urzędu, bezprzewodowymi punktami dostępowymi, punktami dostępowymi dla mieszkańców) a siecią publiczną WAN – Internetem.

Ponadto wydzielenie segmentów sieci umożliwia monitorowanie i zabezpieczenie komunikacji pomiędzy nimi. Konsekwencją tego jest bezpieczeństwo serwerów (na których przetwarzane są dane osobowe) oraz sieci lokalnej Urzędu. Takie mechanizmy są jednym z głównych wymogów ustawy o ochronie danych osobowych. To rozwiązanie oddziela chronione zasoby od segmentów sieci ogólnodostępnych dla mieszkańców (HotSpot, Infokiosk).

Urządzenie UTM będzie zapewniało dodatkową autoryzację dostępu do zasobów za pomocą bezpiecznych mechanizmów szyfrowania.

Aby zapewnić stabilną pracę Urzędu w sieci Internet UTM ma możliwość zaimplementowania mechanizmów zarządzania pasem QoS. Bardzo przydatne jest to do właściwego działania telefonii VoIP a wręcz obowiązkowe przy stosowaniu ogólnodostępnych punktów dostępowych do sieci Internet.

Sieć informatyczna przetwarzająca dane osobowe to oprócz serwera także jednostki centralne do niego podłączone.

Zarządzanie nimi możliwe jest poprzez wdrożenie usług katalogowych. Wszystkie komputery są wyposażone w systemy operacyjne klasy professional (Windows 7 Professional). Umożliwia on podpięcie do serwera Active Directory i centralnego zarządzania uprawnieniami użytkowników oraz komputerami podpiętymi do sieci lokalnej Urzędu.

IV. Poziom bezpieczeństwa

W związku z tym, że system informatyczny przetwarzający dane osobowe jest podpięty do publicznej sieci telekomunikacyjnej (Internet), wymagana jest ochrona na poziomie wysokim zgodnie z § 6 rozporządzenia. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

V. Nadawanie i rejestrowanie (wyrejestrowywanie) uprawnień do przetwarzania

Nadawanie i rejestrowanie uprawnień

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez Administratora Systemu Informatycznego.
2. Rejestracja użytkownika, o której mowa w pkt 1, polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

3. Administrator Systemu Informatycznego albo upoważniony pracownik, o którym mowa w pkt 2, odnotowuje informację o identyfikatorze, który został nadany użytkownikowi.

Wyrejestrowywanie uprawnień

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu Informatycznego.
2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.
3. Wyrejestrowanie następuje poprzez:
   - zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   - usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
4. Czasowe wyrejestrowanie użytkownika z systemu informatycznego musi nastąpić w razie:
   - nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
   - zawieszenia w pełnieniu obowiązków służbowych.
5. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
   - wypowiedzenie umowy o pracy,
   - wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.
6. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

VI. Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

Identyfikator

1. Identyfikator składa się z pierwszej litery imienia oraz nazwiska. W identyfikatorze pomija się polskie znaki diakrytyczne. W przypadku dublowania się identyfikatorów zostanie on rozszerzony o kolejne litery imienia.
2. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Systemu Informatycznego, za zgodą Administratora Bezpieczeństwa Informacji, nadaje inny identyfikator, odstępując od zasady określonej w pkt 1.

Hasło użytkownika

1. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem. Powyższe obostrzenie sprawdzane są przez system informatyczny Administratora Danych.
2. System informatyczny wymusza automatycznie zmianę hasła co 30 dni; Administrator Bezpieczeństwa Informacji może, w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez użytkownika.
3. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.

Hasło administratora

Hasło administratora systemu przechowywane jest w zamkniętej kopercie w miejscu, do którego ma dostęp wyłącznie Administrator Bezpieczeństwa Informacji lub osoba ją formalnie zastępująca.

VII. Procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu

Tryb pracy na poszczególnych stacjach roboczych

1. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia w listwie podtrzymującej napięcie, włączeniu zasilacza awaryjnego (UPS) i komputera, a następnie wprowadzeniu indywidualnego, znanego tylko użytkownikowi, hasła i identyfikatora.
2. Logowanie do stacji roboczych realizowane jest za pomocą usług katalogowych (Active Directory). Konsekwencją przyjętej koncepcji jest pełna kontrola nad użytkownikami i dostępem do zasobów sieci z poziomu konta administratora domeny serwera usług katalogowych.
3. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika albo Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego.
4. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać pogląd), wydruki leżące na biurkach oraz w otwartych szafach.
5. Monitory komputerów wyposażone są we włączające się po 10 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.
6. W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest aktywizować wygaszacz ekranu lub w inny sposób zablokować stację roboczą.
7. Obowiązuje zakaz robienia kopii całych zbiorów danych; całe zbiory danych mogą być kopiowane tylko przez Administratora Systemu Informatycznego lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.
8. Obowiązuje zakaz wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
9. Przetwarzając dane osobowe, należy odpowiednio często robić kopie robocze danych, na których się właśnie pracuje, tak by zapobiec ich utracie.
10. Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych tego dnia przetwarzanych w odpowiednie zabezpieczone obszary, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w zasilaczu awaryjnym (UPS) i listwie.
11. Przed opuszczeniem pokoju należy:
    - zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
    - schować do zamykanych na klucz szaf wszelkie akta zawierające dane osobowe,
    - umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
    - zamknąć okna.
12. Opuszczając pokój, należy zamknąć za sobą drzwi na klucz

Tryb pracy na komputerach przenośnych

1. O ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji, dotyczące pracy na komputerach stacjonarnych.
2. Użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas ich transportu.
3. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.

4. Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika.
5. Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż raz na 30 dni.
6. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem Administratora Systemu Informatycznego, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to Administratorowi Systemu Informatycznego.
7. Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację sugeruje automatycznie system.

Tryb kończenia pracy na serwerze

Serwer przeznaczony jest do pracy ciągłej. Każdorazowe wyłącznie serwera powinno zostać przeprowadzone przez ASI z odnotowaniem przyczyny tej operacji w logach serwera oraz dzienniku systemu informatycznego.

VIII. Procedury tworzenia kopii zapasowych

8. W systemie informatycznym wykorzystującym technologię klient - serwer kopie zapasowe wykonuje się po stronie serwera .Kopie wykonywane są na napędzie taśmowym DAT.
9. Dostęp do kopii bezpieczeństwa mają tylko Administrator Bezpieczeństwa Informacji oraz Administrator Systemu Informatycznego.
10. Kopie tworzy się na oddzielnych nośnikach informatycznych.

Częstotliwość wykonywania kopii

Kopie zapasowe tworzy się:

1. raz w tygodniu – po zakończeniu pracy - zarówno danych, jak i aplikacji, w tym także systemu operacyjnego.
2. raz w miesiącu – na koniec miesiąca kopię zarówno danych, jak i aplikacji, w tym także systemu operacyjnego.
3. raz w roku – na koniec roku kopię zarówno danych, jak i aplikacji, w tym także systemu operacyjnego.

Każdorazowo wykonana kopia jest odnotowywana w dzienniku wykonywanych kopii zabezpieczających.

Testowanie kopii

W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa należy co najmniej raz w tygodniu poddać testowi cyklicznie wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.

Przechowywanie kopii

1. Kopie zabezpieczające przechowuje się w zamykanej szafie metalowej. Dostęp do kopii posiada wyłącznie Administrator Bezpieczeństwa Informacji oraz Administrator Systemu.
2. Zabrania się przechowywania kopii zabezpieczających w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

Likwidacja nośników zawierających kopie

1. Nośniki zawierające nieaktualne kopie danych, będące poza wykazem cyklicznych kopii, likwiduje się czyniąc o tym stosowny zapis w dzienniku kopii zabezpieczających. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym

zniszczeniu w taki sposób, by nie można było odczytać ich zawartości. Nośniki wielorazowego użytku, takie jak dyski twarde, dyskietki, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.

2. Nośniki wielorazowego użytku nienadające się do ponownego użycia należy zniszczyć fizycznie i zniszczenie odnotować w dzienniku kopii zabezpieczających.

Przechowywanie elektronicznych nośników informacji zawierających dane osobowe

1. Zbiory danych przechowywane są na 2 jednostkach obsługujących system informatyczny Administratora Danych. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich miejscach na tych jednostkach, przydzielonych każdemu użytkownikowi przez Administratora Systemu Informatycznego.
2. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.
3. Na nośnikach, o których mowa w pkt 2, dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.
4. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.
5. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

IX. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez Administratora Systemu Informatycznego.
2. Oprogramowanie, o którym mowa w pkt 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi. Ponadto oprogramowania to jest zarządzane i monitorowane centralnie przez ASI z poziomu konsoli zarządzającej celem zapewnienia jeszcze większego poziomu bezpieczeństwa. ASI może wymusić skanowanie antywirusowe, zdalny audyt sprzętu i oprogramowania w sytuacji gdy uzna to za stosowne z punktu widzenia bezpieczeństwa systemu lub potrzeb administracyjnych.
3. Niezależnie od ciągłego nadzoru, o którym mowa w pkt 2, Administrator Systemu Informatycznego nie rzadziej niż raz na tydzień przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
4. Do obowiązków Administratora Systemu Informatycznego należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.
5. Użytkownik jest obowiązany zawiadomić Administratora Systemu Informatycznego o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
6. Dostęp do Internetu możliwy jest na stacjach roboczych, chronionych urządzeniem sprzętowym UTM.
7. Urządzenie UTM zabezpiecza, monitoruje i loguje komunikację pomiędzy siecią wewnętrzną jednostki a publiczną siecią telekomunikacyjną. Logi ze styku sieci przesyłane są na zewnętrzny serwer gdzie są monitorowane przez wykwalifikowany personel.
8. Urządzenie UTM zabezpiecza, monitoruje i loguje komunikację z serwerem na którym znajduje

się baza danych osobowych. Logi te są przesyłane na zewnętrzny serwer gdzie są monitorowane przez wykwalifikowany personel.

9. Urządzenie UTM chroni system informatyczny przetwarzający dane osobowe poprzez:
   a. wysokiej klasy stateful inspection firewall (zapora ogniowa),
      Zapora ogniowa, zwana również firewall to urządzenie służące od ochrony przed nieuprawnionym dostępem do sieci dzięki filtrowaniu przychodzących i wychodzących z sieci połączeń. Firewall wykrywa nieprawidłowe połączenia i je blokuje. Dzięki temu intruz z zewnątrz nie może uzyskać dostępu do zasobów chronionych przez zaporę.
   b. wykrywanie i blokowanie ataków z ochroną proaktywną IPS (Intrusion Prevention System).
      Intrusion Prevention System dokonuje pełnej analizy ruchu od warstwy 3 do 7 modelu ISO/OSI. Dzięki temu jest w stanie wykryć czy przesyłany pakiet danych powinien zostać przepuszczony, czy też należy go zablokować, ze względu na zagrożenie dla sieci
   c. możliwość budowania szyfrowanych kanałów VPN do ewentualnego zdalnego dostępu do systemu przetwarzającego dane osobowe,
   d. autoryzację użytkowników w celu zdefiniowania dodatkowych polityk bezpieczeństwa,
   e. zaimplementowany skaner antywirusowy dla protokołów POP3, SMTP, HTTP, FTP,
   f. ochronę przed spamem (technika heurystyczna oraz DNS Blacklisting),
   g. filtrowania URL,
   h. zarządzanie pasem – QoS (Quality of Service).

X. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych

System informatyczny Administratora Danych umożliwia automatycznie:

1) przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu,
2) sygnalizację wygaśnięcia czasu obowiązywania hasła dostępu do stacji roboczej (dotyczy to także komputerów przenośnych),
3) sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zawierającego:
   - datę pierwszego wprowadzenia danych do systemu Administratora Danych,
   - identyfikator użytkownika wprowadzającego te dane,

Odnotowanie informacji, o których mowa w pkt 3), następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

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

1. Przeglądu i konserwacji systemu dokonuje Administrator Systemu Informatycznego doraźnie.
2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) Administrator Systemu Informatycznego dokonuje nie rzadziej niż raz na miesiąc.
3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale Administratora Systemu Informatycznego nie rzadziej niż raz na miesiąc.
4. Zapisy logów systemowych powinny być przeglądane przez Administratora Systemu Informatycznego codziennie oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.
5. Kontrole i testy przeprowadzane przez Administratora Bezpieczeństwa Informacji powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.

XII. Naprawy urządzeń komputerowych z chronionymi danymi osobowymi

1. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora Danych przeprowadzane są – o ile to możliwe – przez Administratora Systemu Informatycznego.
2. Naprawy i zmiany w systemie informatycznym Administratora Danych przeprowadzane przez serwisanta prowadzone są pod nadzorem Administratora Systemu Informatycznego w siedzibie Administratora Danych (jeśli to możliwe) lub poza siedzibą Administratora Danych, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych lub jak to ma miejsce w przypadku komputerów bazodanowych (serwerów) bez podania kluczy zabezpieczających, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.

XIII. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

1. Użytkownik zobowiązany jest zawiadomić Administratora Systemu Informatycznego o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:
   - naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),
   - częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
   - braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów,
   - wykryciu wirusa komputerowego,
   - zauważeniu elektronicznych śladów próby włamania do systemu informatycznego,
   - znacznym spowolnieniu działania systemu informatycznego,
   - podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
   - zmianie położenia sprzętu komputerowego,
   - zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.
2. Do czasu przybycia na miejsce Administratora Systemu Informatycznego należy:
   - nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby przez niego wskazanej.
   - o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców,
   - rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   - zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   - zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
   - przygotować opis incydentu,
3. Administrator Systemu Informatycznego przyjmujący zawiadomienie jest obowiązany niezwłocznie poinformować Administratora Bezpieczeństwa Informacji o naruszeniu lub

podejrzeniu naruszenia bezpieczeństwa systemu.

4. Administrator Bezpieczeństwa Informacji po otrzymaniu zawiadomienia, o którym mowa w pkt 1, powinien niezwłocznie:
   a) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
   b) podjąć działania chroniące system przed ponownym naruszeniem,
   c) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić notatkę służbową dotyczącą naruszenia bezpieczeństwa systemu informatycznego Administratora Danych, a następnie niezwłocznie przekazać jego kopię Administratorowi Danych.
5. Administrator Bezpieczeństwa Informacji w uzgodnieniu z Administratorem Systemu Informatycznego może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.
6. W razie odtwarzania danych z kopii zapasowych Administrator Systemu Informatycznego obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej).
7. Administrator Danych po zapoznaniu się z raportem, o którym mowa w pkt 4 lit. c, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego Administratora Danych bądź zastosowaniu środków ochrony fizycznej.
8. Administrator Systemu Informatycznego jest zobowiązany do informowania Administratora Bezpieczeństwa Informacji i Administratora Danych o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.
9. Administrator Systemu Informatycznego składa raz na dwa lata Administratorowi Danych kompleksową analizę zarządzania systemem informatycznym.

XIV. Postanowienia końcowe

1. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
3. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 kodeksu pracy.
4. Niniejsza instrukcja wchodzi w życie 9 kwietnia 2013 r.