Załącznik nr 2

do zarządzenia

Wojewody Lubuskiego

z dnia .....

ZATWIERDZAM

.....

Instrukcja zarządzania systemami informatycznymi

Spis treści

I. Wstęp

Niniejszy dokument określa zasady użytkowania sprzętu komputerowego, oprogramowania, wykorzystania poczty elektronicznej i dostępu do Internetu, a także korzystania z zasobów informatycznych i zarządzania systemami informatycznymi służącymi do przetwarzania wszelkiego rodzaju danych w Lubuskim Urzędzie Wojewódzkim w Gorzowie Wlkp.

II. Definicje

Ilekroć w instrukcji zarządzania systemami informatycznymi jest mowa o:

1. **LUW** - rozumie się przez to Lubuski Urząd Wojewódzki w Gorzowie Wlkp.,
2. **Oddziale Informatyki** – rozumie się przez to Oddział Informatyki w Biurze Logistyki,
3. **administratorze bezpieczeństwa informacji (ABI)** – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,
4. **administratorze systemu informatycznego (ASI)** – rozumie się przez to osobę wyznaczoną przez Dyrektora Generalnego Lubuskiego Urzędu Wojewódzkiego, stanowisko ds. administrowania systemami informatycznymi,
5. **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
6. **identyfikatorze** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
7. **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to osobę, która upoważniona została na piśmie do przetwarzania danych osobowych przez administratora danych lub osobę wyznaczoną do wydawania odpowiedniego upoważnienia,
8. **instrukcji** – rozumie się przez to Instrukcję zarządzania systemami informatycznymi,
9. **systemie informatycznym administratora danych** – 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,

10. **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
11. **użytkowniku** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.
12. **incydent** – rozumie się przez to niepożądane zdarzenie, które niesie ze sobą szkodliwe skutki, mające negatywny wpływ na bezpieczeństwo pracy systemów informatycznych.
13. **HELPDESK –** system pomocy technicznej

III. Określenie podstawowych zasad użytkowania systemów informatycznych.

1. Uprawnienia administracyjne

1) Obsługę informatyczną pracowników LUW wykonują pracownicy Oddziału Informatyki.
2) Osoby wskazane w ust.1 mają wyłączne prawo do administrowania i zarządzania zasobami informatycznymi (serwery, komputery stacjonarne i przenośne, oprogramowanie, komputerowy sprzęt peryferyjny, urządzenia wielofunkcyjne, sieć) istniejącymi w LUW, a w szczególności do instalowania oprogramowania, dopuszczania go do eksploatacji, a także dokonywania wszelkich zmian konfiguracyjnych dotyczących zarówno sprzętu komputerowego jak i oprogramowania.

2. Podstawowe zasady dotyczące pracowników LUW

1) Wszyscy pracownicy zatrudnieni w LUW, którzy mają mieć dostęp do zasobów informatycznych LUW otrzymują identyfikator i uprawnienia do korzystania z zasobów informatycznych LUW na podstawie wypełnionego formularza znajdującego się w systemie HELPDESK, opartego na wniosku nadania uprawnień do korzystania z zasobów informatycznych LUW, którego wzór stanowi załącznik Nr 1.

2) Za nadawanie, zmianę i rejestrowanie uprawnień w systemie informatycznym jest odpowiedzialny Administrator Systemów Informatycznych administrujący tym systemem.
3) Nadanie uprawnień następuje na wniosek przełożonego danego pracownika.
4) Nadanie uprawnień do systemów przetwarzających dane osobowe może nastąpić tylko dla osób posiadających ważne upoważnienie do przetwarzania danych osobowych, nadanego zgodnie z Polityką Bezpieczeństwa Informacji.
5) Po otrzymaniu uprawnień do systemów informatycznych, odpowiedzialny pracownik w wydziale szkoli nowego pracownika z podstawowych funkcji aplikacji. Po przeszkoleniu nowy pracownik podpisuje oświadczenie odbyciu szkolenia, którego wzór stanowi załącznik Nr 2.
6) Zmiana lub odwołanie uprawnień w systemach informatycznych przetwarzających dane osobowe następuje na wniosek przełożonego, z inicjatywy Administratora Bezpieczeństwa Informacji/Administratora Systemów Informatycznych i na skutek wygaśnięcia lub odwołania upoważnienia do przetwarzania danych osobowych.
7) Czasowe zawieszenie uprawnień do przetwarzania w systemie informatycznym może nastąpić na wniosek przełożonego, z inicjatywy Administratora Bezpieczeństwa Informacji/Administratora Systemów Informatycznych gdy działania użytkownika naruszają zasady ochrony danych osobowych lub zagrażają bezpieczeństwu danych osobowych.
8) Każda stacja robocza zabezpieczona jest programem antywirusowym.
9) Zabrania się pozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych.
10) Należy umieszczać klucze do szaf w przeznaczonym do tego miejscu po zakończeniu dnia pracy.
11) Należy zamykać drzwi na klucz po zakończeniu pracy w danym dniu i złożyć klucz na portierni. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym kierownika budynku, który zgłasza firmie sprzątającej

jednorazową rezygnację z wykonania usługi sprzątania. W takim przypadku także należy zostawić klucz na portierni.

12) Należy zamykać okna w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych oraz sprzętowi komputerowemu.
13) Zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów.
14) Po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych

3. Zasady zachowania bezpieczeństwa pracy w systemach informatycznych

1) Użytkownik zobowiązany jest do zachowania w tajemnicy danych osobowych zawartych w systemach informatycznych oraz sposobu ich zabezpieczenia.
2) Użytkownik w szczególności powinien zabezpieczać dane osobowe zawarte w systemach informatycznych przed udostępnieniem osobom nieupoważnionym, kradzieżą, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3) Użytkownik w momencie otrzymania dostępu do zasobów informatycznych otrzymuje od stanowiska ds. administrowania systemów informatycznych jednorazowe hasło dostępu, które musi zmienić po pierwszym zalogowaniu do systemu.
4) Hasło dostępu powinno spełniać odpowiednie wymagania co do jego złożoności.
5) Hasło dostępu nie powinno zawierać nazwy lub części nazwy konta użytkownika.

6) Hasło powinno zawierać znaki z wymienionych kategorii: małe i duże litery bez polskich znaków, cyfry, a także zalecane są znaki specjalne (np. @, #, ! itp.).
7) Hasło powinno zawierać minimum osiem znaków;
8) Hasło dostępu logowania do systemu jest ważne przez maksymalnie 30 dni, przy czym każdy pracownik może je zmieniać samodzielnie przed upływem tego terminu.
9) W sytuacjach kiedy pracownicy korzystają z aplikacji, w których przetwarzane są dane osobowe i aplikacja nie wymusza zmiany hasła pracownik zobowiązany jest do zmiany hasła samodzielnie nie rzadziej niż co 30 dni.
10) Użytkownik zobowiązany jest do zachowania swojego hasła w tajemnicy. Niedozwolone jest przekazywanie haseł innym osobom nawet po utracie ważności hasła.
11) Hasło musi być zmienione przez użytkownika niezwłocznie w przypadku podejrzenia lub stwierdzenia jego ujawnienia.
12) W przypadku zapomnienia hasła użytkownik powinien zgłosić się ASI z prośbą o wygenerowanie nowego hasła.
13) Jeśli użytkownik wprowadzi 3-krotnie błędne hasło, wówczas jego identyfikator i hasło zostaną zablokowane. Odblokowanie następuje automatycznie po 15 minutach.
14) Użytkownik loguje się do systemu tylko i wyłącznie za pomocą swojego identyfikatora.
15) Zawieszając pracę w systemie informatycznym (w tym odchodząc od stanowiska pracy) użytkownik blokuje stację roboczą, a kontynuacja pracy możliwa jest jedynie po wprowadzeniu hasła.
16) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd w przetwarzane dane osobom postronnym.
17) Kończąc pracę użytkownik wylogowuje się ze wszystkich systemów, z których korzystał oraz wyłącza stację roboczą.
18) W przypadku nieobecności pracownika, gdy istnieje uzasadniona konieczność dostępu do jego zasobów komputerowych, na wniosek

przełożonego nieobecnego pracownika dostęp do zasobów mogą jedynie udzielić osoby wymienione w pkt 1 ppkt. 1 wyłącznie pracownikowi, który posiada formalne upoważnienie do przetwarzania tych zasobów (w tym określonych danych osobowych).

19) Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do przestrzegania swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji;
20) Osoby posiadające podpis elektroniczny zobowiązane są do przechowywania go w bezpiecznym miejscu, bez możliwości dostępu osób trzecich. Niedopuszczalne jest przechowywanie certyfikatu kwalifikowanego razem z kodem PIN.

4. Zasady postępowania ze sprzętem komputerowym oraz oprogramowaniem

1) Za powierzony pracownikowi sprzęt komputerowy i wykonywane na nim czynności odpowiada materialnie pracownik.
2) Sprzęt komputerowy i oprogramowanie w LUW można wykorzystywać tylko i wyłącznie do celów służbowych.
3) Dane w postaci elektronicznej przetwarzane w systemach LUW zapisane na nośnikach materialnych (np. dyskietkach, dyskach twardych, płytach DVD, CD itd.) są własnością LUW.
4) Niedozwolone jest korzystanie (instalowanie, kopiowanie, użytkowanie) z nielegalnego oprogramowania na służbowym sprzęcie komputerowym.
5) Za nielegalne oprogramowanie uznaje się takie, które nie zostało zatwierdzone do eksploatacji w LUW (nie spełnia warunków licencyjnych, brak oryginalnego nośnika instalacyjnego, nieudokumentowane pochodzenie).
6) Wszelkie licencje na oprogramowanie wykorzystywane w LUW przechowywane są w Oddziale Informatyki.
7) Niedozwolone jest przechowywanie na służbowym sprzęcie komputerowym prywatnych zasobów multimedialnych (np. zdjęcia, filmy, muzyka, aplikacje typu portable).

8) W przypadku wykrycia takich zasobów osoby wymienione w pkt 1 ppkt. 1 mogą je usunąć bez konieczności powiadamiania o tym fakcie użytkownika.
9) Wykorzystywanie nośników CD/DVD jest możliwe jedynie w przypadkach uzasadnionej potrzeby i wyłącznie w celach służbowych.
10) Niedozwolone są samodzielne zmiany konfiguracji komputerowych stanowisk pracy, a w szczególności:
    a) programowe (zmiana konfiguracji oprogramowania i ustawień BIOS, instalowanie niestandardowego oprogramowania na komputerach służbowych);
    b) sprzętowe (zwiększanie pamięci RAM, instalowanie dodatkowego dysku, podłączanie prywatnych urządzeń np. zewnętrznych dysków twardych czy pendrive'ów).
11) Niedozwolone jest samodzielne instalowanie oprogramowania komputerowego, a także dokonywanie jakichkolwiek zmian w konfiguracji systemowej komputerów, urządzeń sieciowych, urządzeń peryferyjnych i urządzeń wielofunkcyjnych będących na wyposażeniu pracowników.
12) Niedozwolone jest wynoszenie poza siedzibę LUW sprzętu komputerowego, za wyjątkiem komputerów przenośnych i zewnętrznych nośników informacji (typu: pendrive, płyty CD, i DVD), ani samodzielnie zmienianie miejsca użytkowania sprzętu.
13) Zgodę na wyniesienie komputerów przenośnych i zewnętrznych nośników informacji poza siedzibę LUW wydaje tylko bezpośredni przełożony.
14) W sytuacjach, kiedy pracownik w celach służbowych korzysta z komputerów przenośnych i zewnętrznych nośników poza obszarem LUW (obszar przetwarzania danych osobowych) zobligowany jest do zachowania szczególnej ostrożności podczas transportu, przechowywania i przetwarzania danych (w tym danych osobowych). Powinien stosować środki ochrony kryptograficznej, antywirusowej i zabezpieczeń zapory sieci komputerowej, z której będzie korzystał łącząc się z siecią Internet.
15) W komputerach przenośnych typu notebook musi być włączona opcja szyfrowania dysków, którą uaktywniają osoby wymienione w pkt 1 ppkt. 1. Niedozwolone jest przekazywanie haseł innym osobom.

16) Zakazuje się przechowywania w pobliżu komputera przenośnego jakichkolwiek haseł dostępowych, które w razie kradzieży mogłyby ułatwić dostęp do danych.
17) Jeżeli jest to możliwe należy zabezpieczać komputer przenośny przed kradzieżą mocując go specjalną linką zabezpieczającą (tzw. Kensington Lock), która jest w zestawie z komputerem przenośnym.
18) Wszystkie służbowe urządzenia pendrive powinny mieć uaktywnioną funkcję szyfrowania danych.
19) Dane osobowe przenoszone za pomocą zewnętrznych nośników informacji po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy i do docelowej bazy danych lub zbioru danych, powinny być z nich trwale usunięte.
20) Dane osobowe przenoszone za pomocą zewnętrznych nośników informacji, w których nie można uaktywnić funkcji szyfrowania danych (płyty CD/DVD) po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy i do docelowej bazy danych lub zbioru danych, powinny być usunięte poprzez zniszczenie samego nośnika w niszczarce.
21) Dozwolone jest tylko kopiowania jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.
22) Dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM, DVD) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym.

Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone.

23) Uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników.
24) Niedozwolone jest wynoszenie na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
25) Niedozwolone jest korzystanie z prywatnych napędów pendrive ani zewnętrznych dysków twardych.
26) Niedozwolone jest w celach prywatnych wynoszenie poza siedzibę LUW danych nagranych na płytach CD/DVD, pendrive'ach, zewnętrznych dyskach twardych czy innych nośnikach danych.
27) Niedozwolone jest pozostawianie bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych oraz w samochodach.
28) Należy dbać o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie).
29) Niedozwolone jest podłączanie do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory).

5. Wymiana danych i ich bezpieczeństwo

1) Bezpieczeństwo danych, a w szczególności ich integralność i dostępność, w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania danych w wyznaczonych zasobach serwera. Pozwala to – przynajmniej w pewnym stopniu – uniknąć wielokrotnego wprowadzania tych samych danych do systemu informatycznego administratora danych.
2) Wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach administratora bezpieczeństwa informacji oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".
3) Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora systemu w porozumieniu z administratorem bezpieczeństwa informacji. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora bezpieczeństwa

informacji lub pracowników Oddziału Informatyki oraz umożliwić im monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.

4) Administrator systemu w porozumieniu z administratorem bezpieczeństwa informacji dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.

6. Zasady korzystania Internetu

1) Internet w LUW może być wykorzystywany wyłącznie do celów służbowych.
2) Pracodawca może kontrolować wykorzystanie Internetu. Kontrolę korzystania z Internetu sprawuje Dyrektor Generalny Urzędu za pośrednictwem osób wymienionych w pkt 1 ppkt. 1.
3) Za wykorzystanie Internetu niezgodnie z przeznaczeniem pracownik podlega odpowiedzialności dyscyplinarnej lub porządkowej na podstawie odrębnych przepisów.
4) Niepożądane strony WWW są blokowane przez Oddział Informatyki. Jeżeli jest potrzeba aby pracownik Oddziału miał dostęp do zablokowanej strony jego przełożony powinien drogą elektroniczną przesłać prośbę wraz z uzasadnieniem o odblokowanie danej strony WWW do osób wymienionych w pkt 1 ppkt. 1.
5) Ograniczenia w dostępie do Internetu w porozumieniu z Oddziałem Informatyki ustala Dyrektor Generalny Urzędu. Wzór listy ograniczeń stanowi załącznik Nr 3.
6) Administrator danych wykorzystuje centralną zaporę sieciową w celu separacji lokalnej sieci od sieci publicznej.
7) Korzystanie z zasobów sieci wewnętrznej (intranet: http://intranetluw/intranet/) jest dostępne wszystkim pracownikom LUW, których komputery zostały podłączone do sieci lokalnej i został ustalony zakres uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.

8) Operacje za pośrednictwem rachunku bankowego administratora danych może wykonywać wyłącznie pracownik Oddziału Księgowości w Biurze Logistyki do tych czynności upoważniony, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

7. Zasady korzystania z poczty elektronicznej

1) Poczta elektroniczna wykorzystywana w LUW stanowi własność pracodawcy i może być wykorzystywana tylko i wyłącznie do celów służbowych.
2) Korzystanie z zewnętrznych serwerów pocztowych dozwolone jest tylko w uzasadnionych przypadkach.
9) Wykorzystanie poczty elektronicznej może podlegać kontroli. Kontrolę sprawuje Dyrektor Generalny Urzędu za pośrednictwem osób wymienionych w pkt 1 ppkt. 1.
3) Za wykorzystanie poczty elektronicznej niezgodnie z przeznaczeniem pracownik podlega odpowiedzialności dyscyplinarnej lub porządkowej na podstawie odrębnych przepisów.
4) Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed „przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie.

8. Zasady zgłaszania incydentów i naruszeń

1) Wszystkie sprawy, problemy, incydenty i uwagi dotyczące niewłaściwego działania służbowych komputerów, drukarek, urządzeń wielofunkcyjnych, sieci, dostępu do Internetu, poczty i licencjonowanego oprogramowania biurowego, a także urządzeń podtrzymujących napięcie komputera (UPS), należy zgłaszać poprzez system HELPDESK.
2) Fakt kradzieży komputera i/lub zewnętrznych nośników informacji (dysk zewnętrzny, pendrive, płyty DVD, CD) muszą być każdorazowo i niezwłocznie zgłaszane.
3) Użytkownik jest zobowiązany do natychmiastowego zgłaszania przypadków naruszenia zasad ochrony danych osobowych oraz informowania o próbach naruszenia bezpieczeństwa.

4) Zgłoszenie takie jest rejestrowane w ewidencji incydentów zagrażających bezpieczeństwu informacji, której wzór stanowi załącznik Nr 4 do Instrukcji.

9. Bezpieczeństwo danych

1) W celu zabezpieczenia danych jest tworzona cotygodniowa kopia bezpieczeństwa danych (w tym danych osobowych) ze wszystkich serwerów na macierz dyskową i/lub taśmową bibliotekę.
2) Kopie danych, w których przetwarzane są dane osobowe nagrywane są co miesiąc na nośnik optyczny, który składowany jest w sejfie poza pomieszczeniem serwerowym. Dostęp do powyższych nośników, na których zapisane są dane osobowe mają jedynie osoby wymienione w pkt 1 ppkt. 1.
3) Opis każdej kopii powinien zawierać następujące informacje:
    a) etykieta nośnika;
    b) data wykonania kopii;
    c) numer kolejny nośnika;
    d) typ kopii;
    e) nazwa jednostki organizacyjnej;
    f) zawartość kopii;
    g) identyfikator osoby wykonującej kopię;
    h) dodatkowe oznaczenia (jeśli wymagają tego odrębne procedury).
4) Wykonanie kopii bezpieczeństwa, właściwy Administrator Systemów Informatycznych odnotowuje w rejestrze kopii zapasowych, w którym zamieszcza się następujące informacje:
    a) data wykonania kopii;
    b) imię nazwisko osoby wykonującej kopie zapasową;
    c) opis kopii;
    d) etykieta nośników;
    e) typ kopii;
    f) miejsce przechowywania kopii;
    g) podpis uwagi.
5) Wzór rejestru kopii zapasowych o którym mowa stanowi załącznik Nr 5 do Instrukcji.

6) Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.
7) W przypadku korzystania z umów z firmami zewnętrznymi na serwis sprzętu komputerowego wszelkie naprawy, których realizacja będzie wymagała dostępu do danych osobowych będą realizowane w obecności pracownika LUW, a w przypadku konieczności zabrania sprzętu do serwisu dyski twarde pozostaną w LUW.
8) Firma zewnętrzna ma obowiązek zachować w poufności wszelkie materiały i/lub informacje w szczególności zaś te objęte ochroną danych osobowych ujawnione danej firmie w związku z realizacją Umowy o świadczenie usług.
9) Szczegółowe ustalenia dotyczące praw, obowiązków i zasad kontroli firm zewnętrznych (w tym dotyczących dostępu i/lub przetwarzania danych osobowych) zapisywane będą w umowach zawieranych z danymi firmami zewnętrznymi zajmującymi się serwisem sprzętu komputerowego zgodnie z Polityką Bezpieczeństwa Informacji.
10) Jakikolwiek dostęp zdalny do infrastruktury sieciowej związany z realizacją w/w umów jest zabroniony.
11) Jedynie Oddział Informatyki i osoby wskazane przez Dyrektora Generalnego mogą mieć zdalny dostęp do infrastruktury sieciowej tylko za pośrednictwem szyfrowanego połączenia.
12) Dostęp do pomieszczeń i urządzeń serwerowych mają jedynie osoby wskazane w pkt 1 ppkt. 1. Jakiekolwiek prace związane z koniecznością przebywania w pomieszczeniach serwerowych muszą być wykonywane w obecności osób wskazanych w pkt 1 ppkt. 1.
13) Kopie danych na lokalnych komputerach użytkownicy realizują samodzielnie kopiując dane na swój udział na serwerze.

10.Zasady dotyczące likwidacji sprzętu

1) W sytuacjach kiedy będzie przeprowadzana likwidacja sprzętu komputerowego w LUW osoby wymienione w pkt 1 ppkt. 1 zniszczą w sposób mechaniczny i nieodwracalny dyski twarde, dyski przenośne, pendrive'y.
2) Skasowanie danych osobowych z nośnika wycofanego z eksploatacji lub zniszczenie nośnika z danymi podlega odnotowaniu z postaci protokołu

przez osoby wymienione w pkt 1 ppkt. 1, które dokonały skasowania danych lub zniszczenia nośnika.

3) Sprzęt komputerowy i inne nośniki informacji przeznaczone do likwidacji zawierające dane osobowe są ewidencjonowane, dokładnie opisane, przechowywane w zamkniętych pomieszczeniach a dostęp do nich mają wyłącznie osoby wymienione w pkt 1 ppkt. 1.
4) Wszyscy pracownicy zobowiązani są do niszczenia płyt CD/DVD w przeznaczonych do tego niszczarkach znajdujących się w LUW.

11. Zasady udostępniania danych osobowych

1) Dla każdego systemu przetwarzającego dane osobowe (jeżeli nie ma takiej funkcjonalności w systemie) należy odnotowywać informacje o odbiorcach danych z tego systemu.
2) Odnotowanie obejmuje informacje o: nazwie podmiotu lub imieniu i nazwisku osoby, której udostępniono dane, dacie udostępnienia i zakresie udostępnionych danych.
3) Obowiązek odnotowania informacji w Rejestrze (w formie papierowej lub elektronicznej), spoczywa na użytkowniku systemu udostępniającemu dane.
4) Odnotowywanie informacji o danych osobowych przekazywanych w formie elektronicznej (e-mailowej) należy prowadzić identycznie jak rejestry pism przychodzących i wychodzących wprowadzając dodatkową kolumnę dotyczącą informacji o przekazaniu danych osobowych.
5) Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.
6) Kontrolę nad prawidłowością odnotowywania ww. informacji sprawuje Administrator Bezpieczeństwa Informacji.

12. Postanowienia końcowe

1) Wszyscy pracownicy zatrudnieni w LUW własnoręcznie podpisują Oświadczenie o zapoznaniu się z treścią niniejszej Instrukcji oraz Polityki Bezpieczeństwa Informacji, którego wzór stanowi załącznik Nr 3 do obowiązującej Polityki Bezpieczeństwa Informacji.

2) Niniejsze wytyczne wchodzą w życie z dniem podpisania i bezwzględnie obowiązują wszystkich pracowników LUW.

Instrukcja zarządzania systemami informatycznymi wchodzi w życie z dniem ..... 2014r.

Załączniki:

Załącznik Nr 1 Wzór wniosku o nadanie uprawnień dla użytkownika w systemach informatycznych.

Załącznik Nr 2 Wzór oświadczenia o przeszkoleniu z podstawowych funkcji oprogramowania.

Załącznik Nr 3 Wzór listy ograniczeń w dostępie do Internetu.

Załącznik Nr 4 Wzór ewidencji incydentów zagrażających bezpieczeństwu informacji.

Załącznik Nr 5 Wzór rejestru kopii zapasowych.