Polityka bezpieczeństwa teleinformatycznego

Uniwersytet Przyrodniczy w Lublinie

SPIS TREŚCI

ROZDZIAŁ I - Postanowienia ogólne

§ 1

Niniejsza polityka bezpieczeństwa teleinformatycznego normuje zagadnienia związane z bezpieczeństwem danych komputerowych gromadzonych, przetwarzanych, transmitowanych lub przechowywanych w jednostkach organizacyjnych Uczelni.

W szczególności określa sposób zabezpieczenia systemów komputerowych przed dostępem do nich osób nieupoważnionych, a także tryb tworzenia kopii bezpieczeństwa i archiwalnych.

§ 2

Przez użyte w Instrukcji określenia należy rozumieć:

1. Administrator systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;

2. Autoryzacja – nadanie uprawnienia na dostęp do konkretnych informacji lub zasobów .

3. Baza danych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze rekordów lub obiektów, w których są zapisane dane jednostkowych obiektów.;

4. Bomba logiczna - nazwa kodu zawartego w legalnym programie, mającego się uaktywnić w określonych warunkach np. pojawienie się konkretnego użytkownika, obecność pewnego pliku na dysku lub data oraz wpływającego destrukcyjnie na działanie systemu informatycznego.

5. Certyfikat klucza – sekwencja danych opatrzona przez Ośrodek Certyfikacji podpisami cyfrowymi, która zawiera co najmniej : nazwę Ośrodka Certyfikacji, identyfikator użytkownika, klucz publiczny użytkownika, określenie okresu ważności oraz numer seryjny.

6. Firewall (ściana ognia) - urządzenie (lub grupa urządzeń), którego głównym zadaniem jest zabezpieczenie sieci wewnętrznej przed nieuprawnionym dostępem z zewnątrz, jak również zapewnienie kontrolowanego dostępu użytkowników wewnętrznych do sieci rozległej;

7. Hasło - słowo złożone z liter, cyfr lub innych znaków, które musi podać użytkownik aby mógł korzystać z dostępu do zastrzeżonych zasobów np. sieci komputerowej, bazy danych, komputera. Hasło jest jednym ze sposobów ochrony danych przed osobami nieupoważnionymi;

8. Inspektor bezpieczeństwa systemów informatycznych – odpowiedzialny za opracowanie polityki bezpieczeństwa systemów informatycznych oraz organizację ich zabezpieczenia, a także posiadający uprawnienia kontrolne w zakresie przestrzegania przez pracowników uczelni procedur związanych z bezpieczeństwem systemów informatycznych;

9. Jednostki organizacyjne – funkcjonujące na uczelni wszystkie komórki organizacyjne

10. Kierownik – kierownik, dyrektor albo inna osoba pełniąca funkcje kierownicze jednostki organizacyjnej uczelni;

11. Klucz publiczny – parametr przekształcenia matematycznego, który może zostać podany do publicznej wiadomości używany do weryfikacji podpisów cyfrowych utworzonych z użyciem odpowiadającego mu klucza prywatnego . Klucze publiczne są również używane do szyfrowania wiadomości lub plików które mogą zostać później odszyfrowane z udziałem odpowiadających im kluczy prywatnych.

12. Koń trojański – program, który udaje pracę innego legalnego programu, a w międzyczasie wykonuje szereg niepożądanych czynności (np. fałszywy program „login" kradnie hasło użytkownika);

13. Kopie archiwalne – kopie plików danych lub plików oprogramowania tworzone na nośniku wymiennym lub dysku twardym komputera, przeznaczone do ich trwałego przechowywania, jak również do odtworzenia danych w przypadku ich utraty lub uszkodzenia;

14. Kopie bezpieczeństwa – kopie plików danych lub plików programowania tworzone na nośniku wymiennym lub dysku twardym komputera w celu ich odtworzenia w przypadku utraty lub uszkodzenia danych;

15. Nośnik komputerowy (wymienny) – nośnik służący do zapisu informacji, np. dyskietka, taśma, płyta CD, wymienny dysk twardy, pendrive;

16. Plik - ciąg bajtów posiadający swoją nazwę odróżniającą ją od innych plików i parametry: rozmiar, datę powstania lub datę ostatniej modyfikacji itp.;

17. Pliki logów - pliki tekstowe (dzienniki) zawierające informacje o czasie i rodzajach zdarzeń występujących w systemie informatycznym;

18. Polityka bezpieczeństwa – zespół procedur dotyczących ochrony informacji w uczelni,

19. Program komputerowy – zbiór instrukcji, które po umieszczeniu na rozpoznawalnym przez urządzenie nośniku i automatycznym przetłumaczeniu na język zrozumiały dla tego urządzenia powoduje, że osiąga on zdolność do wykonywania danej czynności lub też wykonuje daną czynność;

20. Serwer - wyróżniony specjalistyczny komputer świadczący usługi na rzecz mających z nim łączność innych komputerów np. przechowujący pliki, pośredniczący w przekazywaniu poczty itp.;

21. Sieć komputerowa - połączenie komputerów umożliwiające im dzielenie się swoimi zasobami takimi jak: pamięć dyskowa, programy, urządzenia peryferyjne;

22. Sieć publiczna – sieć komputerowa nie uczelniana, np. Internet;

23. Służby informatyczne - pracownicy ośrodka informatyki odpowiedzialni za należyte funkcjonowanie systemów informatycznych;

24. System autentyfikacji użytkownika – proces weryfikacji dostępu użytkownika do systemu informatycznego opierający się na identyfikatorach lub hasłach;

25. System informatyczny (system) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

26. Teletransmisja danych - przesyłanie danych przy pomocy dostępnych łączy;

27. Uczelnia – Uniwersytet Przyrodniczy w Lublinie

28. Uczelniana sieć komputerowa – własna lub dzierżawiona sieć komputerowa wraz z wszelkimi zasobami teleinformatycznymi będącymi własnością Uczelni;

29. Urządzenie mechaniczne uniemożliwiające swobodne przenoszenie sprzętu – urządzenie uniemożliwiające przenoszenie sprzętu poza obszar pomieszczenia służbowego użytkownika bez zgody dysponenta bądź pokonania zastosowanych zabezpieczeń mechanicznych;

30. Uwierzytelnianie – proces potwierdzenia tożsamości osoby, urządzenia lub integracji danych.

31. Użytkownik – pracownik posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych, użytkownik z uprawnieniami na poziomie administratora staje się administratorem systemu;

32. W szczególności bezpieczeństwa systemów informatycznych, obejmujących m.in. dane, sprzęt komputerowy, oprogramowanie, metody ochrony, plany awaryjne, zarządzanie systemem informatycznym.

33. Ważne dane - dane wymagające szczególnej ochrony ze względu na interes Uczelni oraz objęte tajemnicą na podstawie odrębnych przepisów;

34. Wirus - program, który uaktywniony w pamięci operacyjnej, powoduje wadliwe działanie, zniszczenie lub modyfikację systemu operacyjnego, programu komputerowego lub danych;

§ 3

1. Za stan bezpieczeństwa danych komputerowych, zainstalowanego oprogramowania oraz sprzętu komputerowego odpowiedzialni są: władze Uczelni oraz kierownicy jednostek organizacyjnych Uczelni. Za zabezpieczenie danych komputerowych, oprogramowania i sprzętu komputerowego poszczególnych stanowisk odpowiedzialni są ich użytkownicy.

2. Wszyscy użytkownicy systemu informatycznego zobowiązani są do zapoznania się z przepisami normującymi kwestie związane z bezpieczeństwem systemów teleinformatycznych w Uczelni oraz złożenia u bezpośredniego przełożonego stosownego oświadczenia.

3. Wzór „Oświadczenia" określa Załącznik nr 1.

ROZDZIAŁ II - Zdarzenia zagrażające bezpieczeństwu danych i praca w trybie awaryjnym

§ 4

1. Do zdarzeń zagrażających bezpieczeństwu danych należą:

a) próby naruszenia ochrony danych:
   - z zewnątrz: włamania do systemu, podsłuch, kradzież danych,
   - z wewnątrz: nieumyślna lub celowa modyfikacja danych, kradzież danych, zniszczenie danych,

b) programy destrukcyjne tj. wirusy, konie trojańskie, bomby logiczne,
c) awarie sprzętu lub uszkodzenie oprogramowania,
d) zabór sprzętu lub nośników z ważnymi danymi,
e) inne skutkujące utratą danych.

1. W przypadku stwierdzenia naruszenia ochrony informacji, w szczególności zaistnienia zdarzenia, o którym mowa w ust. 1, pracownik Uczelni zobowiązany jest natychmiast powiadomić o zaistniałym zdarzeniu bezpośredniego przełożonego, administratora danego systemu oraz administratora bezpieczeństwa teleinformatycznego.

2. Osoby, wymienione w ust. 2, podejmują działania w celu:

   a) określenia miejsca, sytuacji i czasu w jakim stwierdzono naruszenie bezpieczeństwa,
   b) określenia symptomów naruszenia bezpieczeństwa,
   c) określenia wszelkich informacji mogących wskazać na przyczynę naruszenia,
   d) oszacowania strat w systemie,
   e) naprawy uszkodzeń, w szczególności odtworzenia danych.

3. W celu odtworzenia danych należy wykorzystywać kopie bezpieczeństwa oraz archiwalne, których procedury tworzenia zawarte zostały w § 28-31.

4. Każde zdarzenie zagrażające bezpieczeństwu danych lub każde zdarzenie, które spowodowało naruszenie ochrony danych, winno zostać pisemnie udokumentowane przez administratora systemu poprzez sporządzenie przez niego stosownej notatki.

ROZDZIAŁ III - Zabezpieczenie systemu informatycznego przed zjawiskami fizycznymi

§ 6

1. Pomieszczenia, w których eksploatowane są urządzenia komputerowe, oraz pomieszczenia,
   w których przechowywane są nośniki danych, powinny być:

a) wolne od zagrożeń związanych ze zjawiskami fizycznymi typu:

   - wyładowania elektrostatyczne i atmosferyczne (np. elektryzujące się wykładziny, sąsiedztwo urządzeń odgromowych),

   - silne działanie pól elektromagnetycznych (np. bliskie sąsiedztwo stacji transformatorowych i urządzeń rozdzielczych wysokiego napięcia, pól magnetycznych pochodzących od urządzeń z silnikami elektrycznymi wysokiej mocy lub od transformatorów zasilania budynków itp.),

b) zabezpieczone systemem ochrony p.poż.

c) zabezpieczone przed zalaniem

2. Serwerownia powinny mieć zapewnione stałe utrzymywanie temperatury, wilgotności i innych parametrów określonych przez producenta sprzętu komputerowego. Zabezpieczenie przed zanikiem prądu ma być zapewnione poprzez zastosowanie awaryjnych zasilaczy bezprzerwowych oraz agregat prądotwórczy.

3. Szafy, w których przechowywane są nośniki magnetyczne, powinny zapewniać ochronę przed czynnikami zewnętrznymi mogącymi doprowadzić do utraty danych.

ROZDZIAŁ IV - Fizyczne zabezpieczenie systemu informatycznego przed osobami nieupoważnionymi

§ 7

1. Serwery, profesjonalne stacje robocze, urządzenia teletransmisyjne, szafy teletechniczne, wyłączniki zasilania elektrycznego, szafy z nośnikami magnetycznymi zawierające kopie danych powinny być usytuowane w pomieszczeniu uniemożliwiającym dostęp do nich osób nieupoważnionych.

2. Dostęp do pomieszczeń, o których mowa w ust. 1, winien być ściśle kontrolowany poprzez zainstalowane systemy alarmowe oraz kontrolę dostępu do pomieszczeń.

3. Zaleca się dodatkowe zabezpieczenie serwerów oraz komputerów, w których zapisane są ważne dane, poprzez zastosowanie urządzeń mechanicznych uniemożliwiających swobodne przemieszczanie oraz utrudniających ich ewentualny zabór.

§ 8

1. Lokalizacja urządzeń komputerowych (komputerów typu PC, terminali, drukarek) w pomieszczeniach użytkowanych przez administracje uczelni powinna uniemożliwiać osobom postronnym dostęp do nich, a także wgląd do danych wyświetlanych na monitorach komputerowych.

2. Ograniczenie dostępu nie dotyczy urządzeń przeznaczonych do samoobsługi użytkowników, np. infokiosków, terminali informacyjnych.

3. W przypadku oddalenia się pracownika od stanowiska pracy należy pozostawić system w takim stanie (zablokować konsolę), aby osoby nieupoważnione nie miały do niego dostępu.

§ 9

1. Wszelkie prace konserwacyjne i naprawcze urządzeń komputerowych oraz uaktualnienia systemu informatycznego, wykonywane przez firmę zewnętrzną, powinny odbywać się na zasadach określonych w szczegółowej umowie pomiędzy Uczelnią a tymże podmiotem, z uwzględnieniem klauzuli dotyczącej ochrony przez Zleceniobiorcę wszelkich informacji, do których ma dostęp w czasie wykonywania usługi.

2. Prace, o których mowa w ust. 2, winny zostać odnotowane w rejestrze wykonanych usług/napraw prowadzonym przez Ośrodek informatyki.

3. W przypadku naprawy sprzętu komputerowego w serwisie zewnętrznym ważne dane należy zabezpieczyć (zarchiwizować) oraz o ile to możliwe usunąć z nośników informacji.

4. Zlecone ośrodkowi informatyki naprawy lub modernizacje sprzętu techniki komputerowej upoważniają pracowników ośrodka do zdjęcia zabezpieczeń, i ustawienia haseł tymczasowych po wykonaniu usługi.

§ 10

1. Wszyscy użytkownicy z jednostek administracyjnych Uczelni zobowiązani są do przekazywania uszkodzonych nośników komputerowych, zawierających ważne dane, do służb informatycznych.

2. Przekazanie winno zostać potwierdzone protokołem przekazania i odbioru.

3. Uszkodzone nośniki komputerowe, zawierające ważne dane, powinny być fizycznie niszczone przy udziale komisji powołanej przez kierownika ośrodka informatyki. Z wykonanych czynności komisja sporządza protokół.

4. Do czasu zniszczenia nośniki komputerowe powinny być zabezpieczone przed dostępem osób nieupoważnionych.

§ 11

1. Za bezpieczeństwo komputerów przenośnych odpowiedzialni są ich użytkownicy.

2. Komputery, o których mowa w ust. 1, po zakończonej pracy winny być przechowywane w warunkach zapewniających ich bezpieczeństwo. Dopuszcza się zabezpieczenie ich poprzez użycie urządzeń mechanicznych uniemożliwiających swobodne przemieszczanie sprzętu oraz utrudniających ewentualny zabór.

3. Wynoszenie komputera przenośnego przez pracownika nie będącego jego bezpośrednim użytkownikiem (nie będącego odpowiedzialnym za komputer) dozwolone jest po uzyskaniu zgody bezpośredniego przełożonego osoby odpowiedzialnej za komputer oraz zaewidencjonowaniu faktu jego pobrania zgodnie z książką komputera przenośnego – załącznik nr 2.

ROZDZIAŁ V - Kontrola dostępu do systemów informatycznych

§ 12

1. Dostęp do systemu informatycznego mogą posiadać:

   a) pracownicy – w zależności od wykonywanych czynności służbowych,
   b) wykonawcy usług oraz dostawcy sprzętu lub oprogramowania – w zakresie koniecznym do realizowania danej usługi lub wykonania określonych czynności w systemie za zgodą ośrodka informatyki
   c) inni użytkownicy – w zakresie ustalonym w stosowniej umowie.

2. Osoby, o których mowa w ust. 1, mogą posiadać w systemie własne konto, dostęp do którego winien być możliwy jedynie po podaniu właściwego identyfikatora i hasła.

3. Właściciel konta odpowiedzialny jest za wszelkie działania wykonane z użyciem jego identyfikatora.

4. Pracownicy dostawców sprzętu i oprogramowania wykonują usługę tylko za zgodą administratorów systemu. Jeśli rodzaj wykonywanych czynności (np. uaktualnienie, poprawienie błędnej lub wadliwie działającej konfiguracji oprogramowania czy sprzętu) wymusza pracę na kontach administracyjnych – usługa winna być nadzorowana przez administratora systemu.

§ 13

1. Zabronione jest:

   a) udostepnianie identyfikatorów, haseł postronnym osobom
   b) łamanie haseł,
   c) dokonywanie włamań na konta innych użytkowników,
   d) nieprawne uzyskiwanie dostępu do kont administracyjnych,
   e) zakłócanie działania usług,
   f) omijanie i badania zabezpieczeń (nie dotyczy audytu lub testowania),
   g) rozprowadzanie wirusów, robaków i koni trojańskich oraz niechcianej poczty (spam),
   h) praca na koncie innego użytkownika, za wyjątkiem sytuacji określonej w § 12 ust. 4,
   i) podejmowanie innych działań mogących być zagrożeniem dla systemu.

2. Wykonywanie zabronionych czynności, o których mowa w ust. 1 pkt. a - i, stanowi ciężkie naruszenie obowiązków pracowniczych.

3. Zabronione jest użytkowanie sprzętu komputerowego przez osoby nie posiadające uprawnień do pracy w systemie informatycznym.

4. Wykorzystywanie służbowego sprzętu komputerowego i oprogramowania do celów prywatnych możliwe jest po uzyskaniu przez pracownika pisemnej zgody kierownika właściwej jednostki organizacyjnej Uczelni.

§ 14

1. Rejestracja użytkowników w systemie informatycznym (nie związanym z przetwarzaniem danych osobowych), nadawanie lub modyfikacja uprawnień oraz wyrejestrowywanie użytkowników z systemu odbywa się zgodnie z poniższymi procedurami:

   a) Kierownik jednostki organizacyjnej Uczelni składa u administratora danego systemu zlecenie zarejestrowania użytkownika w systemie.

   b) Wzór „Zlecenia zarejestrowania, modyfikacji uprawnień, wyrejestrowania użytkownika" określa Załącznik nr 4.;

   c) Administrator systemu po otrzymaniu zlecenia, o którym mowa powyżej, rejestruje użytkownika w systemie nadając mu identyfikator oraz wnioskowane uprawnienia.;

   d) W przypadku zmiany przez użytkownika uprawnień do obsługi danego systemu, administrator systemu niezwłocznie modyfikuje uprawnienia na podstawie zlecenia, o którym mowa w pkt. 1, otrzymanego od kierownika właściwej jednostki organizacyjnej Uczelni.;

   e) W przypadku utraty przez użytkownika uprawnień do obsługi danego systemu informatycznego (np. rozwiązanie stosunku pracy, nie obsługiwanie systemu z powodu zmiany stanowiska pracy) kierownik właściwej jednostki organizacyjnej Uczelni niezwłocznie występuje do administratora systemu z wnioskiem o wyrejestrowanie użytkownika z systemu, usunięcie użytkownika (zablokowanie dostępu do systemu), przekazując mu zlecenie.;

   f) Administrator systemu, po otrzymaniu zlecenia, niezwłocznie wyrejestrowuje lub usuwa użytkownika z systemu (blokuje jego dostęp do systemu).

2. Procedury związane z rejestracją użytkowników do systemu informatycznego, służącego do przetwarzania danych osobowych, oraz nadawanie lub modyfikacja uprawnień w tymże systemie, zawarte zostały w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

§ 15

1. Wszystkie systemy informatyczne muszą mieć uaktywnione posiadane mechanizmy kontroli dostępu.
2. Każdy użytkownik systemu informatycznego musi posiadać jawny identyfikator i wprowadzone przez siebie poufne hasło (hasła) autoryzujące jego osobę.
3. Komputery stacjonarne i przenośne powinny mieć uaktywnione posiadane mechanizmy kontroli dostępu do zasobów komputera.
4. Hasłami winny być również zabezpieczone udostępniane w wewnętrznej sieci Uczelnianej zasoby zawierające ważne dane.
5. W celach bezpieczeństwa zaleca się:

   a) wprowadzenie haseł na pliki zawierające ważne dane,
   b) uaktywnienie wygaszaczy ekranów oraz wprowadzenie haseł na nich.

§ 16

1. Hasła, o których mowa w § 15 ust. 2, 3 i 4, oraz hasła służące do administrowania systemami i programami nie powinny być krótsze niż 6 znaków. W systemach, które na to zezwalają, zaleca się stosowanie dużych i małych liter, cyfr oraz innych znaków.

2. O długości haseł, o których mowa w § 15 ust. 5, decyduje użytkownik.

3. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom lub umieszczanie w miejscu łatwo widocznym i dostępnym.

4. W przypadku prac serwisowych serwisant z ramienia OIUP upoważniony jest do zresetowania hasła

§ 17

1. Hasła służące do administrowania systemami i programami powinny być spisane oraz umieszczone w zamkniętych kopertach, oddzielnych dla każdego systemu lub programu, w miejscu uniemożliwiającym dostęp do nich osób nieupoważnionych, chroniącym przed utratą lub zniszczeniem oraz gwarantującym ich odczytanie upoważnionemu użytkownikowi, a także kierownikowi właściwej jednostki organizacyjnej Uczelni w przypadkach nadzwyczajnych.

2. Zarejestrowane hasła, o których mowa w ust. 1, powinny posiadać adnotację o dacie ich wprowadzenia oraz być przechowywane przez okres 5 lat.

3. Hasła, o których mowa w § 15 ust. 3, winny zostać zabezpieczone zgodnie z procedurą określoną w ust. 1.

§ 18

1. Hasła, o których mowa w § 15 ust. 2, należy zmieniać raz na sześć miesięcy , niezwłocznie w przypadku stwierdzenia ich ujawnienia lub podejrzenia o ujawnienie osobie nieuprawnionej.

2. Hasła służące do administrowania systemami i programami powinny być zmieniane co najmniej raz na trzy miesiące, niezwłocznie w przypadku stwierdzenia ich ujawnienia lub podejrzenia o ujawnienie osobie nieuprawnionej.

3. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, o których mowa w ust. 2.
4. Hasła, o których mowa w § 15 ust. 3, powinny być zmieniane co najmniej raz na sześć miesięcy, jak również w przypadku stwierdzenia ich ujawnienia lub podejrzenia o ujawnienie osobie nieuprawnionej.
5. Hasła, o których mowa w § 15 ust. 4 i 5, powinny być zmieniane w przypadku stwierdzenia ich ujawnienia lub podejrzenia o ujawnienie osobie nieuprawnionej.

6. Hasła zachowują swoją poufność również po ustaniu ich czasu trwania.

§ 19

1. W systemach obsługujących transmisję ważnych danych wykorzystywane są klucze kryptograficzne służące do zabezpieczenia danych.
2. Za generowanie, przechowywanie i bezpieczną dystrybucję kluczy kryptograficznych odpowiada osoba upoważniona pisemnie przez władze Uczelni.
3. Przekazywanie kluczy użytkownikom powinno odbywać się w sposób protokolarny, o ile nie następuje w drodze teletransmisji.
4. Obowiązkiem użytkownika jest zabezpieczenie kluczy (prywatnych) przed dostępem osób nieupoważnionych.
5. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia o jego ujawnienie należy powiadomić bezpośredniego przełożonego lub osobę wymienioną w ust. 2.

6. Ważne informacje, do których nie stosuje się kluczy kryptograficznych, należy przesyłać w postaci niejawnej.

ROZDZIAŁ VI - Komputerowa sieć publiczna a sieć Uczelniana

§ 20

1. Komputerowa sieć Uczelniana powinna być odseparowana od sieci publicznej za pomocą systemów typu firewall.

2. Korzystanie z usług Uczelnianych poprzez sieć publiczną winno mieć miejsce po zastosowaniu przez właściwą jednostkę organizacyjną koniecznych systemów zabezpieczeń, w szczególności firewall-i oraz systemu autentyfikacji użytkownika i szyfrowania danych- VPN.

§ 21

1. Zabrania się wykonywania połączeń modemowych z systemów (serwerów, stacji zarządzających, konsol, komputerów) funkcjonujących w wewnętrznej sieci administracyjnej do publicznej sieci Internet, z wyjątkiem połączeń rezerwowych (awaryjnych) na wydzielonych i zabezpieczonych stanowiskach.

2. Zdalny dostęp do serwerów w celach administracyjnych powinien być realizowany z użyciem narzędzi zapewniających bezpieczną komunikację – szyfrowania danych i certyfiaktów.

§ 22

1. Dopuszcza się obieg dokumentów elektronicznych pomiędzy jednostkami organizacyjnymi Uczelni.

2. Do przesyłania dokumentów elektronicznych pomiędzy jednostkami organizacyjnymi Uczelni należy stosować Uczelnianą pocztę elektroniczną lub inne lokalne rozwiązania technologiczne.

3. Ważne dane powinny być przesyłane w formie niejawnej i umożliwiającej ich uwierzytelnienie.

§ 23

4. Dostęp do wszystkich usług internetowych np.: stron www, ftp, grup dyskusyjnych etc. dla pracowników Uczelni z wewnątrz komputerowej sieci Uczelnianej możliwy jest po zarejestrowaniu i zweryfikowaniu służbowego komputera poprzez wypełnienie formularza elektronicznego na stronie spis.up.lublin.pl

5. Za techniczne umożliwienie użytkownikom korzystania z zasobów internetowych, o których mowa w ust. 1, odpowiedzialny jest ośrodek informatyki.

ROZDZIAŁ VII - Przesyłanie danych do podmiotów zewnętrznych

§ 24

1. Do przesyłania ważnych danych do podmiotów zewnętrznych mogą być uzyte systemy informatyczne, które uzyskały pozytywną opinię administratora bezpieczeństwa informacji oraz administratora systemu informatycznego Uczelni oraz zostały przetestowane zgodnie z procedurami określonymi w § 27.

2. Systemy informatyczne służące do przesłania danych oraz generowania plików przeznaczonych do wysłania do podmiotów zewnętrznych winny posiadać uaktywnione mechanizmy kontroli dostępu.

3. Ważne dane należy przesyłać w formie niejawnej i umożliwiającej ich uwierzytelnienie.

4. Za przesyłanie danych, określonych w ust. 3, odpowiedzialny jest pracownik wyznaczony przez kierownika danej jednostki organizacyjnej Uczelni.

5. Każde wysłanie danych winno zostać potwierdzone w systemie lub też pisemnie przez upoważnioną osobę na wydruku przesłanych danych.

§ 25

Kwestie związane z wykorzystywaniem systemów informatycznych Uczelni do przekazywania danych do podmiotów zewnętrznych podlegają szczegółowym uregulowaniom w zawieranych obustronnie umowach, których procedury i klauzule dotyczące bezpieczeństwa systemów informatycznych winny być zgodne z uregulowaniami niniejszej Polityki i skonsultowane z ośrodkiem informatyki.

ROZDZIAŁ VIII - Zabezpieczenie oprogramowania i archiwizacja danych

§ 26

1. Oprogramowanie stosowane w Uczelni musi pochodzić wyłącznie ze źródeł legalnych posiadać łatwo dostępną informację o identyfikatorze wersji i numerze licencji.

2. Wykorzystywane na Uczelni oprogramowanie powinno być ewidencjonowane w formie rejestru oprogramowania (załącznik nr 4). Wykaz poszczególnych licencji powinien znajdować się u Kierownika jednostki organizacyjnej

3. Zabronione jest instalowanie oprogramowania nielegalnego oraz niezwiązanego merytorycznie z wykonywaną pracą a w szczególności oprogramowania, którego eksploatacja jest sprzeczna z Ustawą o prawach autorskich i prawach pokrewnych.

4. Instalacja oprogramowania, o którym mowa w ust. 2, stanowi ciężkie naruszenie obowiązków pracowniczych.

5. Dopuszcza się, po uzyskaniu zgody bezpośredniego przełożonego, instalowanie:

   a) w celach służbowych oprogramowania darmowego (freewar-owego),
   b) w celach służbowych – testowych oprogramowania tzw. sharewar-owego, na wydzielonym stanowisku komputerowym ze wszystkimi obostrzeniami umowy licencyjnej oprogramowania (EULA)

§ 27

1. Umowy dotyczące świadczenia usług teleinformatycznych, zakupu lub modernizacji urządzeń komputerowych, systemów informatycznych i oprogramowania powinny zawierać niezbędne wymagania dotyczące bezpieczeństwa informacji lub odniesienia do odpowiednich dokumentów regulujących te kwestie w Uczelni oraz zakresy odpowiedzialności stron umowy w tym względzie.

2. W celu ograniczenia ryzyka niewydolności funkcjonalnej systemów informatycznych należy prognozować przyszłe wymagania dotyczące pojemności zasobów dyskowych, mocy obliczeniowej procesorów, przepustowości sieci itd. Wymagania te powinny być określone i udokumentowane przed zaakceptowaniem i wdrożeniem nowych i modernizowanych systemów.

3. Przed dokonaniem odbioru nowych lub modernizowanych systemów informatycznych istotnych z punktu widzenia działalności Uczelni należy ustalić kryteria ich odbioru oraz przeprowadzić testy sprawdzające.

4. Kryteria odbioru systemu informatycznego powinny uwzględniać następujące elementy:

a) wymagania dotyczące wydajności i pojemności,
b) wymagania dotyczące wdrożonych zabezpieczeń,
c) przygotowania procedur zarządzania incydentami zagrażającymi bezpieczeństwu informacji przetwarzanej i gromadzonej w systemie,
d) szkolenie w obsłudze i użytkowaniu,
e) optymalne warunki gwarancji i serwisu
f) potwierdzenie, że instalacja nowego systemu nie będzie wpływała niekorzystnie na istniejące systemy.

5. Testowanie istotnego oprogramowania z punktu widzenia działalności Uczelni należy przeprowadzać w wydzielonym środowisku testowym.

6. Testowanie przeprowadzają: pracownicy służb informatycznych, wyznaczeni przez władze Uczelni, oraz osoby merytorycznie odpowiedzialne za funkcjonowanie systemu, wyznaczone przez władze administracji Uczelni.

7. Zmiany w istotnych, z punktu widzenia funkcjonowania Uczelni, programach eksploatowanych w Uczelni podlegają takim samym rygorom jak włączenie do eksploatacji nowego oprogramowania.

§ 28

1. Bazy danych, oprogramowanie oraz konfiguracja systemów operacyjnych w jednostkach organizacyjnych Uczelni powinny być zabezpieczone w postaci kopii bezpieczeństwa lub archiwalnych oraz posiadać oryginalne nośniki instalacyjne.

2. Procedury związane z tworzeniem kopii bezpieczeństwa i archiwalnych dotyczących systemów, w których przetwarzane są dane osobowe, zawarte zostały w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" oraz „Polityce bezpieczeństwa przetwarzania i ochrony danych osobowych".

3. W przypadku systemów, innych niż określone w ust. 2, należy wykonywać następujące kopie bezpieczeństwa:

a) przed dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania,
b) przed dokonaniem zmian w programach (np. zmiana wersji),
c) po każdej istotnej zmianie danych w bazie danych.

4. Oprócz kopii, o których mowa w ust. 3, należy wykonywać kopie archiwalne:

a) miesięczne – na koniec danego miesiąca,
b) roczne – na koniec danego roku.

5. Za wykonanie i zabezpieczenie kopii, określonych w ust. 3 i 4, odpowiedzialny jest administrator danego systemu, który fakt sporządzenia kopii odnotowuje w „Dzienniku administratora systemu".

§ 29

1. Kopie bezpieczeństwa i archiwalne należy:

a) Wykonać w co najmniej dwóch egzemplarzach każda, przy czym przynajmniej jedną na nośniku wymiennym,
b) przechowywać w dwóch różnych urządzeniach i miejscach innych niż te, w którym eksploatowane zbiory przechowywane są na bieżąco.

§ 30

1. Kopie bezpieczeństwa należy przechowywać do momentu wykonania następnej kopii bezpieczeństwa.

2. Kopie archiwalne miesięczne należy przechowywać przez okres 1 roku, a kopie roczne przez okres 5 lat, licząc od pierwszego dnia roku następującego po roku, za który wykonana jest kopia.

§ 31

Nośniki komputerowe, na których znajdują się kopie bezpieczeństwa i archiwalne, powinny być oznaczone w sposób trwały, jednoznaczny i czytelny i zaewidencjonowane w „Rejestrze nośników komputerowych zawierających ważne dane" stanowiącym Załącznik nr 4 do „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

§ 32

Kopie archiwalne należy:
1. okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania,
2. bezzwłocznie usuwać po ustaniu ich użyteczności.

§ 33

1. W jednostkach organizacyjnych Uczelni ważne dane przychodzące pocztą elektroniczną winny być zabezpieczone na nośniku wymiennym lub lokalnym dysku twardym komputera.

2. O trybie archiwizowania danych decyduje administrator systemu informatycznego odpowiedzialny za obsługę poczty elektronicznej.

3. Okres przechowywania kopii, określonych w ust. 1, powinien wynikać z rodzaju zarchiwizowanych danych oraz być zgodny z przepisami wewnętrznymi Uczelni dotyczącymi archiwizowania.

§ 34

1. W celach bezpieczeństwa należy archiwizować istotne dane zapisane na dyskach twardych komputerów poszczególnych użytkowników, w szczególności dane z komputerów przenośnych.

2. O trybie archiwizowania danych, o których mowa w ust. 1, decyduje użytkownik. Przekazanie do pracy komputera używanego powinno nastąpić po usunięciu zbędnych danych
i oprogramowania przez służby informatyczne w porozumieniu z poprzednim użytkownikiem.

3. Oprogramowanie oraz bazy danych, które przestały być wykorzystywane w Uczelni należy usunąć z urządzeń komputerowych po dokonaniu ich uprzedniej archiwizacji

ROZDZIAŁ IX - Ochrona danych przed wirusami i programami szpiegowskimi

§ 35

1. Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

   a) załączniki do poczty elektronicznej,
   b) przeglądane strony internetowe,
   c) pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

2. W celu zapewnienia ochrony antywirusowej administrator systemu informatycznego lub użytkownik, jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:

   a) rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
   b) antywirusowy skaner ruchu internetowego powinien być stale włączony,
   c) monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office powinien być stale włączony,
   d) skaner poczty elektronicznej powinien być stale włączony.

ROZDZIAŁ X - Administrator systemu

§ 36

1. Administratora systemu informatycznego wyznacza lub upoważnia kierownik jednostki organizacyjnej.

2. W Uczelni prowadzone są rejestry administratorów w jednostce organizacyjnej Uczelni:

3. Rejestr, o którym mowa w ust. 2 winien zawierać:

   a) imię i nazwisko administratora,
   b) nazwę systemu informatycznego, którym administruje osoba określona w pkt. a),
   c) nr. telefonu administratora,
   d) daty wpisania i wykreślenia z rejestru.

4. Administratorem systemu może zostać osoba posiadająca odpowiednie kwalifikacje potwierdzone ukończonymi szkoleniami lub doświadczeniem zawodowym.

5. Podstawowym obowiązkiem administratora systemu jest:

   a) zapewnienie ciągłości pracy systemu,
   b) zarządzanie pracą systemu informatycznego, jego zasobami i użytkownikami,

c) czuwanie nad bezpieczeństwem zasobów systemu,

d) konsultacje i zgłaszanie uwag o zauważonych anomaliach do ośrodka informatyki.

6. Administrator systemu powinien być dostępny dla użytkowników w godzinach swojej pracy.

ROZDZIAŁ XI - Kontrola wewnętrzna

§ 37

1. Do kontroli stanu bezpieczeństwa systemu informatycznego w komórkach organizacyjnych Uczelni upoważnieni są:

a) władze Uczelni,

b) administrator bezpieczeństwa informacji,

c) upoważnieni przez władze Uczelni pracownicy kontroli wewnętrznej.

2. Raz w roku administrator bezpieczeństwa informacji przedstawia władzom Uczelni sprawozdanie z wyników kontroli stanu zabezpieczenia systemów informatycznych w Uczelni.

ROZDZIAŁ XII - Postanowienia końcowe

§ 38

Zobowiązuje się wszystkich pracowników Uczelni do bezwzględnego przestrzegania ustaleń niniejszej instrukcji.

ROZDZIAŁ XIII - Załączniki

.....
(nazwisko i imię)
.....
(nazwa jednostki organizacyjnej)
.....
(nazwa komórki organizacyjnej)

OŚWIADCZENIE

Niniejszym oświadczam, że:
1) **zapoznałam(-em) się z obowiązującymi w Uczelni przepisami dotyczącymi bezpieczeństwa systemów teleinformatycznych,**
2) **zobowiązuję się do ich przestrzegania.**

.....
.....
(miejscowość, data) **(czytelny podpis)**

KSIĄŻKA KOMPUTERA PRZENOŚNEGO

.....

(nr inwentarzowy)

L.p.	Data		Imię i Nazwisko Pobierającego (zwracającego)	Podpis Pobierającego (zwracającego)	Podpis przekazującego (odbierającego)	Podpis przełożonego	Uwagi
	Pobrania komputera	zwrotu					

ZLECENIE

zarejestrowania użytkownika, modyfikacji uprawnień, wyrejestrowania użytkownika

Proszę o ..... użytkownika
(zarejestrowanie, modyfikację uprawnień,
wyrejestrowanie)
Pani/Pana .....,
(nazwisko i imię)
pracownika .....,
(nazwa jednostki organizacyjnej uczelni)
w systemie informatycznym: .....
(nazwa systemu lub programu)
.....
oraz
- nadanie uprawnień w zakresie: .....
  .....
- anulowanie uprawnień w zakresie: .....
  .....

.....
(miejscowość, data)

.....
(pieczęć i podpis
kierownika jednostki org.)

REJESTR OPROGRAMOWANIA

.....

L.p.	Nazwa oprogramowania łącznie z nr wersji	Nr licencji/ilość	Data instalacji	Nazwa jednostki org.	Podpis Użytkownika	Uwagi