Załącznik nr 1
do Zarządzenia Rektora nr ….. z dnia ……..

POLITYKA BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW IT

UNIWERSYTETU PRZYRODNICZEGO WE WROCŁAWIU

Spis treści

Rozdział 1. Słownik

§ 1

1. Definicje używane w niniejszej polityce mają następujące znaczenie:

Administrator Danych (AD) - oznacza Uniwersytet Przyrodniczy we Wrocławiu, reprezentowany przez Rektora, który ustala cele i środki przetwarzania danych osobowych.
Administrator Systemów Informatycznych (ASI) – pracownik administrujący określonym systemem IT i zasobem IT. Rolą ASI jest zapewnienie efektywnego zarządzania operacyjnego danego systemu IT i sprawnej jego pracy. Do typowych zadań administratora należy nadzorowanie pracy powierzonych systemów IT, zarządzanie kontami i uprawnieniami użytkowników (na poziomie systemowym), konfiguracja zasobu, instalowanie i aktualizacja oprogramowania, nadzorowanie, wykrywanie i eliminowanie błędów oraz nieprawidłowości, asystowanie i współpraca z zewnętrznymi specjalistami przy pracach instalacyjnych, konfiguracyjnych i naprawczych, a także zapewnienie aktualności dokumentacji takiego zasobu obejmującego również dokumentację zmian mających bezpośredni wpływ na jego funkcjonalność. ASI odpowiada za właściwą i aktualną informację o systemach.
Autoryzacja – proces weryfikacji przyznanego dostępu do systemu i zasobu IT. Celem autoryzacji jest kontrola dostępu, która potwierdza, czy dany użytkownik jest uprawniony do korzystania z żądanego systemu IT.
Bezpieczeństwo informacji – ogół działań podejmowanych w celu zapewnienia poufności, dostępności i integralności i niezaprzeczalności operacji przetwarzanych informacji.
Bezpieczeństwo IT – stan, w którym Zasoby IT i przetwarzane za ich pośrednictwem informacje oraz wspierane procesy wymagające ochrony są właściwie zabezpieczone poprzez zapewnienie atrybutów bezpieczeństwa tj. dostępności, poufności, integralności oraz technologii funkcjonujących w środowisku ładu informatycznego.
Centrum Sieci Komputerowych (CSK) - pozawydziałowa jednostka Uniwersytetu Przyrodniczego we Wrocławiu, której głównym zadaniem jest zapewnienie osobom korzystającym z uczelnianej sieci komputerowej i telefonicznej dostępu do zasobów sieciowych oraz administrowanie uczelnianymi systemami IT.
Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
Dostawca IT – każda firma zewnętrzna, która na podstawie zawartej umowy dostarcza określoną usługę IT – produkt, wsparcie, oprogramowanie, licencje, dostęp do chmury obliczeniowej, baz danych itd.
Dostępność informacji – właściwość, określająca możliwość wykorzystania informacji przez użytkownika na żądanie, w określonym czasie.
Granulacja ról i uprawnień – działanie, które pozwala na dzielenie i określanie uprawnień dla zasobów i użytkowników.
Informacje chronione – wszystkie nieujawnione do wiadomości publicznej informacje o charakterze technicznym, technologicznym, handlowym, kadrowym, finansowym, organizacyjnym, strategicznym lub inne informacje posiadające wartość dla Uczelni, w szczególności mogą to być dane osobowe pracowników, doktorantów i studentów oraz kontrahentów.

Integralność informacji – właściwość zapewniająca, że informacja nie została zmieniona lub zniszczona w sposób nieautoryzowany.

IT (*ang. Information Technology*) – całokształt zagadnień, metod, środków i działań związanych z przetwarzaniem informacji. Stanowi połączenie zastosowań informatyki i telekomunikacji, obejmuje również sprzęt komputerowy oraz oprogramowanie, a także narzędzia i inne technologie związane z przetwarzaniem, przesyłaniem, przechowywaniem, zabezpieczaniem i prezentowaniem informacji.

Inspektor Ochrony Danych (IOD) – oznacza rolę w organizacji AD, odpowiedzialną za operacyjne i wykonawcze wsparcie i realizację obowiązków AD wynikających z RODO. Szczegółowy opis zakresu obowiązków roli IOD znajduje się w dokumencie „Polityki Ochrony Danych Osobowych".

Jednostka organizacyjna - jednostki, o których mowa w § 8 Regulaminu organizacyjnego UPWr. t.j. Wydziały, Jednostki organizacyjne wchodzące w skład wydziałów, jednostki ogólnouczelniane, międzywydziałowe i pozawydziałowe oraz wspólne, a także jednostki administracyjne i samodzielne stanowiska.

Klasa bezpieczeństwa zasobu IT - dla każdego Zasobu IT wyznaczony ASI przeprowadza ocenę krytyczności i klasyfikuje Zasób IT, definiując poziom ochrony (wysoki, średni, niski) oraz kryteria ich oceny.

Naruszenie bezpieczeństwa IT – pojedyncze zdarzenie lub seria zdarzeń niepożądanych albo niespodziewanych, związanych z bezpieczeństwem informacji i Zasobów IT, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu Zasobów IT i informacji w nich przetwarzanej.

Podatność – właściwość Zasobu IT natury architektonicznej, konfiguracyjnej i konstrukcji samego oprogramowania lub sprzętu, na które mogą oddziaływać zagrożenia, z negatywnym skutkiem, a tym samym sprowadzać na środowisko IT, ryzyko naruszenia bezpieczeństwa IT (bądź ryzyka naruszenia prywatności podmiotu w przypadku przetwarzania danych osobowych) i informacji w takim środowisku przetwarzanych.

Polityka Bezpieczeństwa Informacji i Systemów IT – w skrócie PBIiST,

Poufność informacji – właściwość zapewniająca, że informacja nie jest udostępniana nieupoważnionym osobom, podmiotom lub w celu niezgodnym z przeznaczeniem.

Przełączniki sieciowe – urządzenia łączące segmenty sieci komputerowej ich zadaniem jest przekazywanie ramki między segmentami sieci z doborem portu przełącznika, na który jest przekazywana.

Przetwarzanie informacji – operacje wykonywane w stosunku do informacji (zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie) również w systemach informatycznych.

Retencja danych - zatrzymywanie przez administratorów informacji o tym, kto, z kim i kiedy łączył się (lub próbował to zrobić) za pomocą środków komunikacji elektronicznej.

Sieć - zbiór komputerów i innych urządzeń połączonych z sobą kanałami komunikacyjnymi. Umożliwia ona wzajemne przekazywanie informacji oraz udostępnianie zasobów własnych między podłączonymi do niej urządzeniami.

System IT (system teleinformatyczny) – zespół współpracujących urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie

danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego.

Utwardzanie – proces polegający na usunięciu zbędnego oprogramowania, zlikwidowaniu niepotrzebnych nazw użytkowników i niewykorzystywanych loginów, wyłączeniu niepotrzebnych usług oraz systematycznych aktualizacjach oprogramowania w serwerach oraz serwerach wirtualnych.

Urządzenie końcowe – komputery stacjonarne oraz mobilne, serwery, drukarki sieciowe, dyski i inne urządzenia wykonujące usługi bezpośrednio dla użytkownika.

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika.

Użytkownik – Pracownik, który w ramach obowiązków służbowych wykorzystuje powierzony Zasób IT.

Zasoby IT – każde urządzenie i oprogramowanie stanowiące element (poprzez możliwość fizycznego i logicznego połączenia) środowiska teleinformatycznego zapewniające prawidłową pracę operacyjną Uczelni. Są to w szczególności – systemy informatyczne, bazy danych, urządzenia sieciowe, firewalle, laptopy, stacje robocze, tablety, telefony komórkowe, oprogramowanie aplikacyjne, biurowe, serwery.

Zarządzanie bezpieczeństwem IT – ogół działań, podejmowanych w celu zapewnienia organizacyjnej, technicznej i proceduralnej ochrony informacji i Zasobów IT, za pośrednictwem których przetwarzane są informacje i wspierane procesy.

Złośliwe oprogramowanie - ogół programów mających szkodliwe działanie w stosunku do systemu komputerowego lub jego użytkownika.

Rozdział 2. Cel i zakres opracowania

§ 2

1. Celem opracowania i utrzymania aktualnej PBIiSIT w Uczelni jest:
   1.1. zapewnienie bezpieczeństwa zasobów IT,
   1.2. zapewnienie dostępu do zasobów IT oraz przetwarzanej informacji w sposób monitorowany i ograniczony dla tych pracowników, którzy ich potrzebują do realizacji celów związanych z wykonywanymi obowiązkami, zgodnie z zasadą „wiedzy koniecznej”,
   1.3. zapewnienie rozliczalności aktywności Użytkowników,
   1.4. zapewnienie optymalnych pod względem kosztowym warunków do eksploatacji i rozwoju zasobów IT, zgodnie z zasadami bezpieczeństwa określonymi w ”Instrukcji Bezpieczeństwa IT”,
   1.5. zapewnienie prawidłowej i bezpiecznej eksploatacji poszczególnych zasobów IT,
   1.6. doskonalenie zasad zarządzania bezpieczeństwem zasobów IT.

Rozdział 3. Klasyfikacja bezpieczeństwa zasobów IT

§ 3

1. Dla każdego zasobu oraz systemu IT lub grupy zasobów IT przetwarzających informacje, Administrator Systemów Informatycznych przeprowadza ocenę krytyczności i przydziela klasę

bezpieczeństwa zasobowi IT, które zatwierdza właściwy kompetencyjnie Prorektor. Ocena taka definiuje oczekiwany poziom ochrony.

2. CSK odpowiada za przechowywanie, aktualizację i zarządzanie dostępem do kodu źródłowego zasobu IT.
3. W celu rozeznania poziomu bezpieczeństwa zasobów IT minimum raz na rok przeprowadza się analizę ryzyka. Proces przeprowadzania analizy ryzyka został szczegółowo opisany w Metodyce szacowania ryzyka dla systemów IT.

Rozdział 4. Bezpieczeństwo komunikacji sieciowej

§ 4

1. Centrum Sieci Komputerowych odpowiada za wdrożenie wymaganych mechanizmów zabezpieczeń kontroli ruchu sieciowego i transmisji danych w Uczelni.
2. Przy planowaniu i wdrażaniu sieci komputerowych należy wziąć pod uwagę następujące aspekty, mające wpływ na politykę kontroli ruchu sieciowego i kontrolę logiczną przepływów informacyjnych:
   2.1. podsieci (segmenty) z narzędziami i zasobami IT służącymi do celów stricte IT – tj. administrowania zasobami, monitorowanie zasobów itd. powinny być wydzielone,
   2.2. podsieci (segmenty) przeznaczone na zasoby IT dla celów testowych i developerskich powinny być wydzielone.
3. Wszelkie zmiany realizowane w środowiskach sieci Uczelni i jej urządzeniach sieciowych wraz z Usługami IT wspierającymi właściwą eksploatację takich sieci, podlegają obowiązującym zasadom opisanym w **§** 9 niniejszej polityki.
4. Ruch w sieci jest kontrolowany za pomocą urządzeń sieciowych w taki sposób, aby odrębne funkcjonalnie segmenty sieci były odseparowane od siebie co najmniej logicznie.
5. Przełączniki sieciowe realizujące zaplanowane funkcje transmisji i kontroli ruchu sieciowego nie powinny mieć pozostawionej bez żadnych zmian, domyślnej konfiguracji producenta.
6. Zasoby IT działające w ramach infrastruktury niebędącej własnością Uczelni lub pozostającej poza jej bezpośrednim utrzymaniem muszą spełniać wymagania bezpieczeństwa wynikające z klasyfikacji informacji przetwarzanych w tych zasobach IT.
7. Do zarządzania Zasobami IT spoza infrastruktury informatycznej Uczelni wykorzystywane powinny być połączenia zapewniające szyfrowanie komunikacji (np. SSH, TLS, VPN).
8. W przypadku zasobów IT, których dostępność wymagana jest tylko w określonym czasie, należy wprowadzić ograniczenia połączeń poza zdefiniowanym okresem.
9. Wysyłanie informacji chronionych poza sieć wewnętrzną wymaga stosowania mechanizmu szyfrowania np. poprzez SSH.
10. Zasób IT powinien zapewniać mechanizmy szyfrowania informacji chronionych przesyłanych przez sieci publiczne, za co odpowiada ASI danego zasobu IT.

Rozdział 5. Kontrola dostępu

§ 5

1. Zasady kontroli dostępu do zasobów IT muszą uwzględniać:
   1.1. Zasadę wiedzy koniecznej, tzn. konieczność nadania uprawnień/upoważnień wynikających wprost z rzeczywistych potrzeb związanych z wypełnianiem obowiązków służbowych.
   1.2. Zasadę minimalnych uprawnień, tzn. potrzebę przydzielenia tylko tych uprawnień, które są wymagane do wypełniania obowiązków służbowych.
   1.3. Zasadę rozdziału uprawnień, tzn. konieczność rozdzielenia uprawnień użytkowników w taki sposób, by każdy z nich realizował – z zachowaniem zasad opisanych w pkt. 1.1 – w miarę możliwości tylko jedną z poniższych funkcji:
   1.3.1. Funkcje zarządcze;
   1.3.2. Funkcje nadzorcze i kontrolne;
   1.3.3. Funkcje administracyjne;
   1.3.4. Funkcje operatorskie;
   1.3.5. Funkcje rozwojowe.
   1.4. Wszystkie ograniczenia prawne.
   1.5. Weryfikację nadanego już upoważnienia przez AD do przetwarzania danych osobowych w Uniwersytecie Przyrodniczym we Wrocławiu.
2. Autoryzacja musi się odbywać każdorazowo przed próbą uzyskania dostępu do systemu IT.
3. Dla każdego systemu IT należy określić szczegółowy zakres i okres retencji danych generowanych przez mechanizm rozliczalności (dalej: logów). Dane generowane przez mechanizm rozliczalności (tzw. logi) muszą zawierać co najmniej:
   3.1. identyfikatory użytkowników uzyskujących dostęp do informacji,
   3.2. daty i czasy dostępu do informacji, z uwzględnieniem strefy czasowej,
   3.3. szczegóły działania w odniesieniu do informacji (np. parametry wywołania, rodzaj operacji, status wykonania, komunikat błędów itp.).
4. Zasady kontroli dostępu do systemów IT, w których przetwarzane są informacje chronione, muszą dodatkowo uwzględniać:
   4.1. Unikanie nadmiernej liczby użytkowników posiadających, co najmniej jedno z podanych niżej praw dostępu:
   4.1.1.prawo umożliwiające nieograniczony dostęp do systemów IT (tzw. prawa administratora);
   4.1.2. prawo umożliwiające zmianę przywilejów innych użytkowników;
   4.1.3. prawo umożliwiające zmianę logów systemu, wykraczające poza prawo zmiany tych logów na skutek bezpośredniego i zamierzonego przez twórców systemu wykonywania normalnych funkcji.
   4.2. Każdy system IT powinien posiadać co najmniej jednego użytkownika posiadającego prawa dostępu wystarczające do sprawnego usuwania awarii, przy czym:
   4.2.1. identyfikator i hasło tego użytkownika mogą być wykorzystywane jedynie podczas awarii, a nie w toku normalnego funkcjonowania i powinny być przypisane wyłącznie do jednej osoby fizycznej;
   4.2.2. identyfikator oraz hasło użytkownika muszą być przechowywane w bezpieczny sposób; miejsce i sposób przechowywania określa Dyrektor CSK;

4.2.3. po usunięciu awarii osoba, która użyła identyfikatora powinna niezwłocznie zmienić hasło oraz je zabezpieczyć.

5. Zarządzanie uprawnieniami i kontrolą dostępu jest zgodne z Procedurą zarządzania dostępami i upoważnieniami do przetwarzania danych osobowych w Uniwersytecie Przyrodniczym we Wrocławiu oraz dodatkowo należy brać pod uwagę:

5.1. Wszystkie systemy IT, tam gdzie jest to technicznie możliwe, muszą posiadać mechanizmy zapewniające przestrzeganie niżej podanych zasad tworzenia i posługiwania się hasłami:

5.1.1. hasła muszą mieć długość co najmniej 8 znaków;

5.1.2. hasła muszą składać się z przynajmniej: jednej dużej, jednej małej litery, jednej cyfry i jednego znaku specjalnego;

5.1.3. hasło nie może być łatwe do odgadnięcia oraz być hasłem słownikowym;

5.1.4. hasło nie może być przechowywane (np. w plikach programów, skryptów, schematów baz danych, w dokumentacji etc.) w formie jawnej.

6. W przypadku wystąpienia trzech następujących po sobie prób nieudanego użycia hasła, tam gdzie jest to technicznie możliwe, konieczne jest zablokowanie użytkownika na ustalony czas.

7. W przypadku użytkowników systemów IT, konta mogą zostać zablokowane na podstawie:

7.1. karty obiegowej zwolnienia pracownika,

7.2. informacji z Działu Kadr i Płac o zwolnieniu pracownika ze świadczenia obowiązku pracy,

7.3. w przypadku naruszenia bezpieczeństwa systemu.

Rozdział 6. Zabezpieczanie urządzeń końcowych

§ 6

1. Za zabezpieczanie urządzeń końcowych, w tym nośników wymiennych, odpowiada osoba kierująca jednostką organizacyjną, w ramach której urządzenie końcowe jest eksploatowane. W razie potrzeby proces ten odbywa się przy pomocy pracowników CSK.
2. Zabezpieczenia, o których mowa w ust. 6.1., obejmują:
   2.1. konfigurację urządzeń - w razie potrzeby proces ten odbywa się przy pomocy pracowników CSK.
   2.2. implementację oprogramowania i narzędzi sprawdzających, szyfrujących i ochronę przed złośliwym oprogramowaniem - w razie potrzeby proces ten odbywa się przy pomocy pracowników CSK.
   2.3. prowadzenie rejestrów urządzeń.
3. Konfiguracja urządzeń końcowych powinna zostać ustawiona na podstawie zaleceń producentów wykorzystywanego oprogramowania oraz ogólnie uznanych za poprawne, zasad i standardów bezpieczeństwa. W szczególności powinna obejmować:
   3.1. instalację wyłącznie niezbędnych pakietów oprogramowania oraz usunięcie zbędnych,
   3.2. aktualizację zainstalowanego oprogramowania zgodnie z zaleceniami ich producentów,
   3.3. wdrożenie zasad kontroli dostępu,
   3.4. instalację i uruchamianie wyłącznie niezbędnych usług i procesów oraz wyłączenie zbędnych,
   3.5. zmianę domyślnych ustawień konfiguracyjnych.

4. Urządzenia końcowe powinny być tak skonfigurowane by zapewnić bieżącą aktualizację oprogramowania i instalację poprawek, zarówno systemowych jak i bezpieczeństwa.
5. Ochronie antywirusowej podlegają wszystkie urządzenia końcowe, na których taka ochrona jest technologicznie możliwa i nie wpłynie ona znacząco na ich funkcjonalność, wydajność lub dostępność.
6. Ustawienia ochrony antywirusowej muszą zapewniać następujący minimalny zakres funkcjonalności:
    6.1. mechanizmy ochrony antywirusowej blokują aktywność złośliwego oprogramowania (wirusów),
    6.2. konfiguracja ochrony zapewnia codzienną automatyczną aktualizację baz sygnatur,
    6.3. działanie ochrony przez cały czas (tzn. realizacja tzw. ochrony w czasie rzeczywistym).
7. Urządzenia nieprzyłączone do sieci z dostępem do Internetu muszą być aktualizowane ręcznie. Za ich cykliczną aktualizację odpowiada właściwy ASI zasobu IT. Aktualizacje takie muszą się odbywać nie rzadziej niż raz w miesiącu.
8. Użytkownik powiadomiony o aktywności złośliwego oprogramowania musi niezwłocznie zgłosić takie zdarzenie zgodnie z obowiązującą w Uczelni Procedurą zarządzania incydentami z zakresu bezpieczeństwa informacji w Uniwersytecie Przyrodniczym we Wrocławiu.
9. Urządzenia końcowe powinny podlegać ochronie przed zagrożeniami (w tym złośliwym oprogramowaniem i spamem), polegającej na wykorzystaniu mechanizmów do identyfikacji oraz blokowania zagrożeń.

Rozdział 7. Urządzenia mobilne

§ 7

1. Kierownicy jednostek organizacyjnych Uczelni zobowiązani są do opracowania i aktualizacji wykazu pracowników, którzy otrzymali urządzenia mobilne (np. laptop, telefony komórkowe) do realizacji zadań służbowych poza siedzibą Uczelni.
2. Mechanizmy ochrony urządzeń mobilnych implementowane są zgodnie z zakresem przedstawionym dla urządzeń końcowych, tam gdzie jest to możliwe. Dotyczy to w szczególności aspektów kontroli dostępu poprzez zapewnienie silnych metod uwierzytelniania i haseł dostępowych do urządzeń mobilnych.
3. Urządzenia mobilne powinny mieć możliwość ograniczenia zdalnego dostępu do danych (poczty elektronicznej, przechowywanych dokumentów itp.). Służy do tego wykorzystanie haseł o wymaganych parametrach określonych w § 5 ust. 5, automatycznego blokowania urządzenia po określonym czasie bezczynności, określenia maksymalnej liczby prób wprowadzenia wadliwego hasła oraz okresu ważności hasła.
4. Procedura niszczenia musi zagwarantować uniemożliwienie odczytania zawartości nośnika, na którym przetwarzane były informacje chronione.
5. Naprawa przez dostawców IT urządzenia zawierającego informacje chronione może odbywać się po wcześniejszym usunięciu z niego wszystkich informacji chronionych zawartych na dysku, w sposób gwarantujący uniemożliwienie ich odczytania. W przypadku braku możliwości usunięcia danych z nośnika, zostaje on fizycznie zniszczony.
6. Wsparcie w zakresie realizacji zapisów pkt. 2-5, na wniosek kierownika jednostki organizacyjnej Uczelni lub użytkownika wykonuje CSK.

Rozdział 8. Usługi chmurowe

§ 8

1. Zasoby IT funkcjonujące poza infrastrukturą Uczelni lub w tzw. chmurze publicznej mogą przetwarzać informacje chronione pod warunkiem przeprowadzenia oceny ryzyka przez ASI związanego z takim przetwarzaniem.
2. Zakres dla usług chmurowych powinien uwzględniać następujące aspekty bezpieczeństwa informacji (aczkolwiek nie ograniczając się do niżej przedstawionego zakresu):
   2.1. umożliwienie wglądu w bezpieczeństwo infrastruktury dostawcy takich usług,
   2.2. mechanizmy detekcji i usuwania zagrożeń,
   2.3. szyfrowanie danych,
   2.4. zapewnienie odpowiedniej granulacji ról i uprawnień,
   2.5. mechanizmy zapobiegające wyciekom danych.

Rozdział 9. Zarządzanie zmianą zasobów IT

§ 9

1. Rozwój zasobów IT musi uwzględniać działania mające na celu wdrożenie właściwej ochrony systemów oraz informacji przetwarzanych z wykorzystaniem tego zasobu, a w szczególności:
   1.1. poziom klasyfikacji informacji przetwarzanych przez dany zasób IT;
   1.2. analizę wymagań w zakresie bezpieczeństwa przetwarzanych informacji;
   1.3. klasyfikację bezpieczeństwa związaną z wdrażaniem nowego zasobu IT lub jego zmiany;
   1.4. zaprojektowanie architektury i funkcjonalności zasobu IT z uwzględnieniem aspektów bezpieczeństwa;
   1.5. testowanie przedwdrożeniowe w celu weryfikacji zgodności zasobu IT z wymaganiami bezpieczeństwa IT przed jego uruchomieniem;
   1.6. dokumentowanie zasobów IT w zakresie ich bezpieczeństwa.
2. Dopuszcza się przy formułowaniu wymagań dla właściwej ochrony informacji i zasobu IT, stosowanie ogólnie dostępnych standardów i dobrych praktyk w zakresie bezpiecznego pisania kodu i realizacji bezpiecznej funkcjonalności, w zakresie adekwatnym dla danego zadania.
3. Zasoby IT wykorzystywane do przetwarzania informacji chronionych muszą zapewniać mechanizmy bezpiecznej identyfikacji i weryfikacji tożsamości użytkowników. Domyślną metodą weryfikacji tożsamości w zasobach IT jest zastosowanie spersonalizowanych kont dostępowych.
4. Rozwój i testowanie zasobów IT, również w trakcie realizacji projektu budowy i wdrożenia, muszą być przeprowadzane wyłącznie z wykorzystaniem danych testowych.
5. Dokumentacja powykonawcza musi opisywać wszystkie zastosowane mechanizmy bezpieczeństwa IT dla danego zasobu IT.
6. Zarządzanie zmianą Zasobów IT wymaga zatwierdzenia przez Dyrektora CSK.

Rozdział 10. Kopie zapasowe

§ 10

1. Czynności realizacji tworzenia kopii zapasowych powinny zapewniać:
   1.1. zgodność kopii informacji z informacjami źródłowymi,
   1.2 jednoznaczną identyfikację informacji zapisanej na nośniku wykorzystywanym w procesie tworzenia kopii zapasowej/archiwizowania,
   1.2. możliwość odtworzenia kompletnej informacji z posiadanych kopii.
2. Zakres wymagań dla zasad tworzenia kopii zapasowej dla danego zasobu IT powinien obejmować następujące informacje:
   2.1 ile poprzednich wersji powinno być dostępnych do odtworzenia,
   2.2 jakie są wymagania dotyczące dostępności danych (tj. jak szybko powinien być system dostępny w przypadku awarii (RTO),
   2.3. jak często powinny być tworzone kopie zapasowe danych (np.: codziennie, raz na tydzień, raz w miesiącu, itp.),
   2.4. jaki jest okres przechowywania kopii zapasowych,
3. Dokumentowanie wykonywanych kopii zapasowych musi obejmować co najmniej następujące informacje:
   3.1. datę i godzinę wykonania kopii,
   3.2. oznaczenie typu kopii będącej odnośnikiem do metody wykonywania kopii bezpieczeństwa (np. kopia pełna, przyrostowa, kolejna w cyklu),
   3.3. zakres danych podlegających backupowi (nazwa zbioru, katalogu itd.),
   3.4. miejsce składowania kopii.
4. Dokumentacja, o której mowa w ust. 3, może być prowadzona w formie papierowej lub w przeznaczonym do tego celu zasobie IT.
5. Zasady tworzenia kopii zapasowych dla każdego Zasobu IT przygotowuje odpowiedzialny ASI, a zatwierdza Dyrektor CSK.

Rozdział 11. Dostępność zasobów IT

§ 11

1. Przez zapewnienie dostępności zasobów IT należy rozumieć:
   1.1. Każde działanie na etapie rozwoju zasobu IT mające na celu uzgodnienie wymagań na dostępność tego zasobu oraz rozwiązań organizacyjnych i technicznych mających zapewnić ich spełnienie po wdrożeniu zasobu.
   1.2. Każde działanie organizacyjne lub techniczne mające na celu przeciwdziałanie występowaniu awarii lub innych zdarzeń skutkujących lub mogących skutkować ograniczeniem dostępności informacji przetwarzanej z wykorzystaniem zasobu IT.
   1.3. Każde działanie organizacyjne lub techniczne mające na celu minimalizowanie skutków awarii lub innych zdarzeń skutkujących lub mogących skutkować ograniczeniem dostępności informacji przetwarzanej z wykorzystaniem zasobu IT oraz przywrócenie dostępności informacji w uzgodnionym czasie.
   1.4. Dyrektor CSK wraz z ASI określa następujące parametry:

1.4.1. RTO (ang. *Recovery Time Objective*) tj. maksymalny czas od momentu zaistnienia sytuacji skutkującej niedostępnością informacji przetwarzanych przez zasób IT, do momentu przywrócenia dostępu do niej.

1.4.2. RPO (ang. *Recovery Point Objective*) tj. maksymalny dopuszczalny czas niedostępności informacji przetwarzanych przez zasób IT, niepowodujący negatywnych skutków dla wspieranego przez ten zasób procesu.

Rozdział 12. Zarządzanie podatnościami zasobów IT

§ 12

1. Zasoby IT muszą być na bieżąco monitorowane i badane pod kątem występowania w nich podatności.
2. Priorytet monitorowania i badania podatności powinien zależeć od klasyfikacji bezpieczeństwa danego zasobu IT lub grupy takich zasobów.
3. Eliminacja podatności zasobu IT musi zostać poprzedzona przetestowaniem zaproponowanych zmian eliminujących podatność - przed jego zastosowaniem, w celu oceny skuteczności tego mechanizmu oraz braku jego negatywnego wpływu na funkcjonowanie zasobu.

Rozdział 13. Eksploatacja i utrzymanie zasobów IT

§ 13

1. Zasoby IT muszą być regularnie monitorowane pod kątem aktualności ich komponentów, które mają wpływ na poufność, dostępność lub integralność informacji chronionych przetwarzanych przez te zasoby.
2. Konfiguracja komponentów zasobu IT, mających wpływ na poufność, dostępność lub integralność informacji chronionych przetwarzanych przez te zasoby, musi być okresowo – nie rzadziej niż raz na rok – przeglądana pod kątem aktualności i adekwatności względem wymagań bezpieczeństwa.
3. Serwisowanie lub naprawa zasobów IT, przetwarzających informacje chronione, przez dostawców IT może odbywać się wyłącznie:
   3.1. pod nadzorem ASI zasobu IT,
   3.2. bez nadzoru ASI, za zgodą Dyrektora CSK, jeśli wcześniej zostały przez ASI skutecznie usunięte z nich wszystkie informacje chronione.

Rozdział 14. Wycofywanie zasobów IT z eksploatacji

§ 14

1. Zasób IT, co do którego nie planuje się dalszego użytkowania, powinien zostać wycofany z eksploatacji.
2. W ramach procesu wycofywania zasobu IT z eksploatacji należy zapewnić bezpieczeństwo informacji chronionych przetwarzanych w zasobie IT poprzez:
   2.1 archiwizację informacji chronionych,
   2.2 usunięcie informacji chronionych, zgodnie z obowiązującymi przepisami prawa i wewnętrznymi regulacjami.

3. Za sposób zabezpieczenia informacji chronionych przetwarzanych z wykorzystaniem zasobu IT wycofywanego z eksploatacji odpowiada Dyrektor CSK.
4. Niszczenie nośników informacji danego zasobu IT, w szczególności przetwarzającego informacje chronione musi zapewnić, iż dane takie zostaną zniszczone bezpowrotnie, dotyczy to:
   4.1. dysków fizycznych,
   4.2. pamięci szybkich (SSD),
   4.3. nośników podręcznych (USB),
   4.3. taśm z backupami.
5. Procedura niszczenia, może być, za zgodą Dyrektora CSK, realizowana przez dostawcę IT zapewniając:
   5.1. skuteczne zniszczenie nośnika,
   5.2. zniszczenie struktury fizycznej nośnika, o ile jest to fizycznie możliwe.
6. Dopuszcza się niszczenie danych w sposób elektroniczny, przy użyciu algorytmów nadpisujących dane na nośnikach w sposób uniemożliwiający ich przywrócenie i odczytanie.

Rozdział 15. Bezpieczeństwo poczty elektronicznej

§ 15

1. Usługa poczty elektronicznej nie może zezwalać na nieautoryzowane wysyłanie wiadomości poczty elektronicznej zarówno z sieci zewnętrznej jak i wewnętrznej.
2. Wysłanie wiadomości poczty elektronicznej musi być poprzedzone pozytywną identyfikacją i weryfikacją tożsamości użytkownika.
3. Serwer SMTP (Usługi IT poczty elektronicznej, zwany dalej „serwerem SMTP") musi umożliwiać negocjacje i nawiązywanie połączeń z wykorzystaniem protokołów zapewniających bezpieczne uwierzytelnianie oraz poufność i integralność przesyłanych danych (TLS).

Rozdział 16. Bezpieczeństwo aplikacji webowych

§ 16

1. Identyfikacja i uwierzytelnianie użytkownika oraz zarządzanie aktywnymi sesjami użytkowników w zasobie IT stanowiącym aplikację webową powinna brać pod uwagę następujące wymagania:
   1.1. login nie powinien rozróżniać wielkich i małych liter (case insensitive),
   1.2. identyfikacja i uwierzytelnianie użytkownika odbywa się za pomocą loginu i hasła,
   1.3. wsparcie obsługi przypadku, kiedy hasło straciło ważność, a użytkownik nadal może zalogować się tym hasłem,
   1.4. cały proces uwierzytelniania i zestawienia sesji użytkownika z aplikacją powinien być realizowany poprzez szyfrowany kanał komunikacyjny (TLS),
   1.5. początkowa strona aplikacji z formatką logowania się dla użytkownika, powinna być również przesłana do przeglądarki użytkownika poprzez szyfrowany kanał TLS,
   1.6. dla wykonania krytycznych operacji aplikacja powinna wymagać od użytkownika ponownego uwierzytelnienia,
   1.7. komunikaty o błędach procedury uwierzytelniania dla użytkownika nie powinny zawierać informacji o stanie konta,

1.8. szczegóły o błędach logowania i pełna wiedza (np. czy podano złe hasło, czy zły login, czy nie ma takiego użytkownika w domenie, itd.) powinny się znajdować wyłącznie w dziennikach zdarzeń dostępnych dla ASI,
1.9. tam gdzie jest to technicznie wykonalne, aplikacja po poprawnym uwierzytelnieniu powinna informować użytkownika o ostatnim: udanym zalogowaniu się, nieudanym zalogowaniu się - podając adres IP, datę i czas.

2. Sesja użytkownika w komunikacji z aplikacją, jest sekwencją żądań i odpowiedzi protokołu HTTP (w tunelu TLS). Każdy użytkownik w zależności od profilu, uprawnień musi być traktowany i śledzony przez aplikację indywidualnie w danej interakcji z aplikacją, po to by spełnić postulat poufności informacji przetwarzanej i udostępnianej użytkownikowi.
3. Do właściwego i bezpiecznego zarządzania sesjami użytkowników powinno się stosować następujące wytyczne:
   3.1. aplikacja powinna generować ID sesji użytkownika, wartość ID nie powinna informować o rodzaju uprawnień, o użytkowniku itp. Sama nazwa ID sesji nie powinna informować o użytej technologii (np. PHPSESSID, JSESSIONID, ASP.NET_SessionId) - nazwą sesji powinno być np. ID lub IDENTYFIKATOR,
   3.2. wartość ID powinna być generowana przez mechanizm o wysokiej entropii, tak by szansa kolizji (odgadnięcia prawidłowej ID sesji) była możliwie minimalna,
   3.3. szczegółowe informacje dotyczące każdego ID sesji powinny być przechowywane tylko po stronie serwera aplikacji (np. w obiektach sesji, repozytorium/tabeli sesji),
   3.4. mechanizm wymiany ID sesji, powinien uwzględnić czas wygaśnięcia sesji, który będzie do ustawienia przez administratora,
   3.5. aby zapewnić poufność całej sesji użytkownika z aplikacją, całość powinna być zawarta w transmisji SSL/TLS. Nie można mieszać zawartości - która raz będzie przesłana HTTP a w innym miejscu HTTPS (Ustawienie: HTTP Strict Transport Security (HSTS),
   3.6. mechanizm cookies, powinien posiadać zawsze atrybut "Secure" tak aby potencjalny intruz nie mógł przechwycić ID sesji,
   3.7. mechanizm cookies powinien zawierać atrybut "HttpOnly" tak, by potencjalny intruz nie mógł posłużyć się skryptami JavaScript, czy VBScript poprzez mechanizmy DOM. Jest to również ochrona przed atakami XSS,
   3.8. cookies wykorzystywane w zarządzaniu sesją powinno być ustawione na "non persistent", tak by po zamknięciu przeglądarki, pliki cookies zostały skasowane (tzn. atrybuty "Max-Age" i "Expires" pozostawić nieustawione),
   3.9. aplikacja nie może akceptować żadnej wartości ID sesji, której sama nie wygenerowała (Strict state),
   3.10. aplikacja powinna wygenerować ponownie ID sesji, dla tego samego użytkownika, jeśli w następnej pracy z aplikacją, użytkownik zmienił poziom uprawnień, tzn. nie można posłużyć się tym samym identyfikatorem np. w przypadku kiedy użytkownik zalogował się z rolą użytkownika X, a później uzyskał (zalogował się ponownie) jako administrator aplikacji,
   3.11. akcja wylogowania się użytkownika (bądź wymuszenie wylogowania przez administratora aplikacji) powinna skutkować zakończeniem sesji i usunięciem wszelkich informacji uwierzytelniających sesję użytkownika,
   3.12. aplikacja powinna zezwalać użytkownikowi na pojedynczą aktywną sesję (uniemożliwiać wielosesyjność użytkownika).

4. Aplikacja w komunikacji z użytkownikiem powinna wymuszać silne metody szyfrowania i przeciwdziałać możliwości wykorzystania komunikacji niezaszyfrowanej, w ten sposób, że:
   4.1. wspiera tylko mocne i nieskompromitowane protokoły i metody,
   4.2. do zestawiania bezpiecznych połączeń z użytkownikami wykorzystuje w etapie weryfikacji możliwości PKI – tj. certyfikatów maszyn i użytkowników (OSCP),
   4.3. wrażliwe informacje (np. nazwa loginu,) nie mogą być częścią URL.
5. Rejestrowanie zdarzeń systemowych, bazodanowych i aplikacyjnych stanowi istotne wymaganie bezpieczeństwa, ze względu na konieczność monitorowania i obsługi potencjalnych incydentów występujących w złożonym środowisku aplikacji, dlatego zakres informacyjny zdarzeń aplikacji powinien obejmować:
   5.1. naruszenia bezpieczeństwa monitorowanego systemu i danych w nim przetwarzanych (integralności, poufności i dostępności),
   5.2. naruszenia polityki uprawnień w monitorowanych systemach,
   5.3. objawy nietypowego i nieprawidłowego działania monitorowanych systemów,
   5.4. symptomy niedostatecznej wydajności i dostępności dla użytkowników.

6. Odpowiedzialność za przestrzeganie zasad bezpieczeństwa aplikacji opisanych w ust 1-5 spoczywa na ASI, a nadzór sprawuje Dyrektor CSK.

Rozdział 17. Monitorowanie bezpieczeństwa IT

§ 17

1. Monitorowaniu bezpieczeństwa IT podlegają wszystkie zasoby IT, za nadzór nad monitorowaniem bezpieczeństwa IT są odpowiedzialni ASI.
2. Każdy zgłoszony do procesu monitorowania zasób IT, musi mieć określoną odpowiednią klasyfikację bezpieczeństwa. Jest ona niezbędnym elementem w procesie monitorowania, ponieważ determinuje konfigurację odpowiednich polityk (progów alarmowych, kroków decyzyjnych silników korelacji), nadaje kontekst i wagę monitorowanym zdarzeniom w narzędziach służących do monitorowania, co pozwala na podjęcie odpowiednich czynności związanych z ewentualnymi incydentami.
3. Wszystkie czynności realizacji takiego monitorowania w zasobie IT (zmian w konfiguracji, instalacji oprogramowania, itd.) muszą być zgodne z Rozdziałem 9 PBIiSIT.
4. Zakres rejestrowanych zdarzeń w procesie monitorowania bezpieczeństwa IT powinien obejmować:
   4.1. naruszenia bezpieczeństwa monitorowanego systemu i danych w nim przetwarzanych (integralności, poufności i dostępności),
   4.2. naruszenia polityki nadawania upoważnień w monitorowanych systemach,
   4.3. objawów nietypowego i nieprawidłowego działania monitorowanych systemów,
   4.4. symptomów niedostatecznej wydajności i dostępności dla użytkowników,
   4.5. innych przejawów wynikłych z wad oprogramowania, niezgodności konfiguracji systemu z dokumentacją itp.
5. Zdarzenia wykryte w następstwie monitorowania bezpieczeństwa podlegają rozpoznaniu i ewentualnej obsłudze zgodnie z obowiązującą w Uczelni „Procedurą zarządzania incydentami z zakresu bezpieczeństwa informacji w Uniwersytecie Przyrodniczym we Wrocławiu ”.

6. Wyłączenie monitorowania, bądź usunięcie danego zasobu IT z procesu monitorowania zapewnianego przez właściwe narzędzia informatyczne, może nastąpić w następujących przypadkach:
   6.1. wyłączenia danego zasobu IT,
   6.2. zatwierdzonej przez Dyrektora CSK zmiany klasyfikacji bezpieczeństwa takiego zasobu IT,
   6.3. odrębnej, uzasadnionej pisemnej decyzji Dyrektora CSK, w ramach obsługi odstępstwa (np. na wniosek JM Rektora, w trybie pilnym).
7. Parametry mechanizmów rejestracji zdarzeń powinny być ustawione przez ASI danego zasobu IT w oparciu o dotychczasowe doświadczenie w utrzymaniu tego zasobu, tak by zapewnić, że:
   7.1. dzienniki nie przepełnią się do czasu ich archiwizacji,
   7.2. nie zostaną utracone żadne informacje o zdarzeniach związanych z bezpieczeństwem,
   7.3. jeśli to możliwe należy stosować zewnętrzny serwer rejestrowania zdarzeń. W przeciwnym razie powinno się dla dzienników wydzielić osobny dysk lub przynajmniej partycję (w systemie plików NTFS) i nadać im uprawnienia ograniczające dostęp do uprawnionych operatorów i administratorów,
   7.4. plan techniczny archiwizacji dzienników zdarzeń jest dostosowany do tempa ich przyrostu i zapełniania się.
8. Rejestrowane w systemie zdarzenia muszą być monitorowanie przynajmniej na jeden z poniższych sposobów:
   8.1. manualny, przez uprawnionego operatora lub administratora (niezbędne jest wówczas sporządzenie harmonogramu monitorowania uwzględniającego tempo zapełniania się dzienników),
   8.2. automatyczny lokalny, skonfigurowany, powiadamiający co najmniej jednego ASI danego zasobu IT o ewentualnych zdarzeniach.
9. Decyzje związane z monitorowaniem bezpieczeństwa IT zatwierdza Dyrektor CSK.

Rozdział 18. Bezpieczeństwo środowisk zwirtualizowanych

§ 18

1. Środowiska zwirtualizowane składają się z dwóch podstawowych komponentów, którym powinna być zapewniona ochrona:
   1.1. host wirtualizacyjny (wirtualizator, ang. *hypervisor*) – monitor maszyny wirtualnej pozwalający na uruchomienie jednocześnie wielu systemów operacyjnych na jednej maszynie fizycznej,
   1.2. maszyna wirtualna - środowisko wraz z systemem operacyjnym, które pozwala na uruchomienie innych programów, poprzez kontrolę komunikacji uruchamianego programu bezpośrednio z zasobami sprzętowymi (pamięć, procesor) lub systemu operacyjnego.
2. Wszystkie serwery zapewniające środowiska wirtualizacji (hosty) muszą znajdować się w miejscach do tego przeznaczonych – serwerowniach z zapewnieniem właściwej kontroli dostępu określonej w § 5 i ich rozliczalności.
3. Narzędzia służące do centralnego zarządzania wirtualizatorami i maszynami wirtualnymi powinny podlegać kontroli ruchu sieciowego i znajdować się w podsieciach (segmentach) przeznaczonych dla ASI takich zasobów IT.

4. Zdalny dostęp dla ASI musi być szyfrowany z zapewnieniem obustronnego uwierzytelniania, przy czym certyfikaty „self-signed" mogą być stosowane wyłącznie w środowiskach dewelopmentu lub testowych.
5. Konfiguracje wirtualizatorów podlegają takim samym wymaganiom bezpieczeństwa jak serwery, co zostało opisane w Rozdziale 19 „Bezpieczeństwo serwerów".
6. W przypadku „utwardzania" wirtualizatorów należy wziąć pod uwagę dodatkowo:
   6.1. ograniczenie możliwości nadużywania zasobów przez poszczególne maszyny wirtualne oraz współdzielenia schowka (ang. clipboard) pomiędzy maszyną fizyczną a wirtualną,
   6.2. szczególne zabezpieczenie maszyn fizycznych (wirtualizatorów) przed nieuprawnionym dostępem do plików maszyn wirtualnych.

Rozdział 19. Bezpieczeństwo serwerów

§ 19

1. Wszystkie serwery stanowiące, bądź wspierające zasoby IT w Uczelni muszą być przypisane do trzech głównych kategorii:
   1.1. serwer główny – maszyna z systemem operacyjnym i zainstalowanym niezbędnym oprogramowaniem służąca do realizacji funkcji zasobu IT lub usługi IT,
   1.2. serwer testowy – maszyna z systemem operacyjnym i zainstalowanym niezbędnym oprogramowaniem serwerowym służąca do testowania oprogramowania przed przekazaniem do eksploatacji,
   1.3. serwer dewelopmentu – maszyna z zainstalowanym niezbędnym oprogramowaniem służąca do rozwoju oprogramowania i elementów zasobów i usług IT.
2. Wszystkie serwery powinny mieć zapewnioną ochronę przed złośliwym oprogramowaniem, o ile istnieją takie rozwiązania dla danego systemu operacyjnego.
3. Wszystkie główne serwery muszą znajdować się przeznaczonych do tego celu pomieszczeniach specjalnych IT lub serwerowniach.
4. Serwery wraz z oprogramowaniem nie mogą udostępniać innych zasobów i usług (serwerowych, sieciowych, współdzielonych folderów) niż te, które muszą działać zgodnie z przeznaczeniem serwera w kontekście wsparcia zasobu IT.
5. Zdalny dostęp do wszystkich serwerów, o ile jest dopuszczony, powinien zapewnić szyfrowanie wymiany informacji i silne uwierzytelnianie obu stron takiej transmisji.
6. Zgodnie z zasadą „wiedzy koniecznej" i minimalnych uprawnień właściwych do wykonywania czynności administratora, granulacja uprawnień dla takich ról powinna uwzględniać rozróżnienie:
   6.1. czynności związane z zarządzaniem uprawnieniami i rolami użytkowników,
   6.2. czynności związane z zarządzaniem systemem operacyjnym zasobu IT,
   6.3. czynności związane z zarządzaniem bazą danych lub aplikacją,
   6.4. czynności związane z kontrolą logów bezpieczeństwa (*audit* i *accounting*).

Rozdział 20. Bezpieczeństwo IT

§ 20

1. Bezpieczeństwu IT podlegają:
   1.1. urządzenia, w tym urządzenia wirtualne,

1.2. systemy i oprogramowanie zapewniające spełnienie wymagań dla ochrony zasobów IT i informacji w nich przetwarzanych.

2. Komponenty zabezpieczające systemy IT (nie jest to lista wyłączna):
   2.1. firewalle – filtry pakietów, aplikacyjne, proxy, wielofunkcyjne (AV, DLP, Identity Management, VPN, itd.),
   2.2. koncentratory VPN – IPSec, SSL-VPN,
   2.3. systemy ochrony antywirusowej,
   2.4. systemy ochrony przeciw włamaniom (ang. *IPS*) – sprzętowe jak i programowe,
   2.5. systemy ochrony przeciw wyciekom informacji (ang. *DLP*) – sprzętowe i programowe,
   2.6. systemy zapewniające rozliczalność i badające ruch sieciowy pod kątem występowania anomalii i symptomów potencjalnych ataków (ang. *Network Forensics*),
   2.7. systemy gromadzące i analizujące informacje ze zdarzeń rejestrowanych w systemowych dziennikach zdarzeń (ang. *SIEM*),
   2.8. systemy i środowiska analityczne wspierające rozpoznanie i klasyfikację złośliwego oprogramowania i ataków z tym związanych (ang. *Sandbox, Malware Analytics, Threat Analytics*).
3. Zgodnie z w/w wymaganiami, komponenty bezpieczeństwa IT, tam gdzie jest to możliwe muszą znajdować się w odrębnych segmentach sieci z właściwą kontrolą ruchu sieciowego.
4 Wszelkie zmiany konfiguracji komponentów również powinny być uprzednio przetestowane pod kątem wpływu na bieżące polityki ochrony i ryzyk związanych z potencjalnym obniżeniem poziomu ochrony zapewnianych przez te komponenty.

Rozdział 21. Edukacja i doskonalenie świadomości bezpieczeństwa IT

§ 21

1. Szczególny nacisk edukacji w zakresie bezpieczeństwa zasobów IT i informacji w nich przetwarzanej, powinien być nałożony na wszystkich pracowników CSK odpowiedzialnych za prawidłowe zarządzanie bezpieczeństwem IT.
2. Podnoszenie i doskonalenie świadomości bezpieczeństwa IT, są to działania ukierunkowane na szeroką skalę odbiorców koncentrujące się na dostarczeniu podstawowych informacji o wymogach, wydarzeniach i zagrożeniach, mogących mieć negatywny wpływ na bezpieczeństwo IT Uczelni.
3. Wiedza dystrybuowana w ramach podnoszenia i doskonalenia świadomości powinna być możliwa do przyswojenia przez różne grupy odbiorców nie posiadające wiedzy technicznej lub kierunkowej w bezpieczeństwie informacji.
4. W zakres informacyjny treści stanowiących podstawę dla wszelkich działań podnoszących świadomość bezpieczeństwa IT wchodzą:
   4.1. opisy zagrożeń publicznie udostępnianych, zakwalifikowanych jako istotne dla Uczelni,
   4.2. informacje o najważniejszych wymogach płynących z dobrych praktyk i polityk bezpieczeństwa,
   4.3. informacje dotyczące przeciwdziałaniu incydentom bezpieczeństwa informacji,
   4.4. zmiany prawne mające wpływ na bezpieczeństwo informacji.
5. Wszelkim działaniom związanym z podnoszeniem i doskonaleniem świadomości bezpieczeństwa IT podlegają wszyscy pracownicy CSK.

6. Działania takie mogą być realizowane poprzez:
   6.1. szkolenia – e-learning, prezentacje, sesje treningowe – wewnętrzne jak i zewnętrzne,
   6.2. specjalistyczne szkolenia dziedzinowe w zakresie podnoszenia świadomości dla poszczególnych grup pracowników Uczelni, tj.: władz Uczelni, kadry kierowniczej, osób posiadających uprawnienia/upoważnienia, pracowników obsługi.
7. Działania związane zarówno z edukacją jak i podnoszeniem świadomości bezpieczeństwa IT, powinny być realizowane cyklicznie, nie rzadziej niż raz na rok.
8. Za realizację powyższych działań odpowiada Dyrektor CSK.
9. Nadzór nad realizacją powyższych działań sprawuje właściwy kompetencyjnie prorektor.

§ 22

1. Integralną częścią PBIiSIT stanowi:
   1.1. Instrukcja Bezpieczeństwa IT Uniwersytetu Przyrodniczego we Wrocławiu
   1.2. Metodyka szacowania ryzyka dla systemów IT Uniwersytetu Przyrodniczego we Wrocławiu
   1.3. Procedura zarządzania incydentami z zakresu bezpieczeństwa informacji i systemów IT w Uniwersytecie Przyrodniczym we Wrocławiu.