Polityka Bezpieczeństwa Informacji i Systemów Teleinformatycznych w Akademii Łomżyńskiej

Spis treści

1. Definicje używane w niniejszej polityce:

1) Administrator Danych (AD) - oznacza Akademię Łomżyńską, reprezentowaną przez Rektora, który ustala cele i środki przetwarzania danych osobowych.
2) 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.
3) Autoryzacja – przydzielenie osobie fizycznej lub prawnej, uprawnień w systemie teleinformatycznym po jej pozytywnym uwierzytelnieniu lub potwierdzenie woli realizacji czynności w postaci elektronicznej przez uwierzytelnionego użytkownika za pomocą dodatkowych danych.
4) Bezpieczeństwo informacji – ogół działań podejmowanych w celu zapewnienia poufności, dostępności, integralności i autentyczności operacji przetwarzanych informacji.
5) 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 i autentyczności oraz technologii funkcjonujących w środowisku ładu informatycznego.
6) Dział Systemów Komputerowych (DSK) - jednostka organizacyjna Akademii Łomżyńskiej, której głównym zadaniem jest administrowanie uczelnianymi systemami IT oraz zapewnienie dostępu do tych zasobów pracownikom i studentom.
7) Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
8) Dostawca IT – każda firma zewnętrzna, która na podstawie zamówienia, zlecenia lub zawartej umowy dostarcza określoną usługę IT – produkt, wsparcie, oprogramowanie, licencje, dostęp do chmury obliczeniowej, baz danych itd.
9) Dostępność informacji – właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym.
10) 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, studentów oraz kontrahentów.
11) Integralność informacji – właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony.
12) 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.
13) Inspektor Ochrony Danych (IOD) – oznacza osobę odpowiedzialną za operacyjne i wykonawcze wsparcie i realizację obowiązków administratora wynikających z RODO. Szczegółowy opis zakresu obowiązków roli IOD znajduje się w dokumencie „Polityki Ochrony Danych Osobowych”.

14) Jednostka organizacyjna - Wydziały, jednostki organizacyjne wchodzące w skład Wydziałów, jednostki ogólnouczelniane, międzywydziałowe, a także jednostki administracyjne i samodzielne stanowiska.
15) 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.
16) Incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na funkcjonowanie Uczelni.
17) Podatność – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa.
18) Polityka Bezpieczeństwa Informacji i Systemów Teleinformatycznych (PBI) – zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania.
19) Poufność informacji – właściwość zapewniająca, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom lub podmiotom, w celu niezgodnym z przeznaczeniem.
20) Przełączniki sieciowe – urządzenia łączące segmenty sieci komputerowej ich zadaniem jest przekazywanie ramki między segmentami sieci z doborem portu przełącznika, na który jest przekazywana.
21) Przetwarzanie informacji – operacje wykonywane w stosunku do informacji (np. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie) również w systemach informatycznych.
22) Sieć komputerowa - zbiór urządzeń do transmisji danych oraz mediów przewodowych i bezprzewodowych zapewniających przekazywanie informacji między urządzeniami końcowymi.
23) System informacyjny – system teleinformatyczny, o którym mowa w art. 3 pkt 3 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r., Nr 64, poz. 565 ze zm.), wraz z przetwarzanymi w nim danymi w postaci elektronicznej.
24) System teleinformatyczny - zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej (Dz. U. z 2024 r., poz. 1221).
25) Urządzenie końcowe – komputery stacjonarne oraz mobilne, serwery, drukarki sieciowe, dyski i inne urządzenia wykonujące usługi bezpośrednio dla użytkownika.
26) Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika.
27) Użytkownik – osoba posiadająca dostęp do systemu informacyjnego Uczelni, w szczególności pracownik lub student.
28) Zasób 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.

29) 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.
30) Złośliwe oprogramowanie - ogół programów mających szkodliwe działanie w stosunku do systemu komputerowego lub jego użytkownika.

2. Cel polityki

Celem opracowania i utrzymania aktualnej Polityki Bezpieczeństwa Informacji i Systemów IT w Uczelni jest:

1. zapewnienie bezpieczeństwa zasobów IT,
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”,
3. zapewnienie rozliczalności aktywności Użytkowników,
4. zapewnienie optymalnego wykorzystania zasobów IT,
5. zapewnienie prawidłowej i bezpiecznej eksploatacji poszczególnych zasobów IT,
6. doskonalenie zasad zarządzania bezpieczeństwem zasobów IT.

3. Klasyfikacja bezpieczeństwa zasobów IT

1. Zasoby IT eksploatowane w Akademii Łomżyńskiej należy ewidencjonować w Rejestrze zasobów IT. Wzór rejestru określa Załącznik nr 1 do PBI w AŁ.
2. Dla każdego zasobu oraz systemu IT lub grupy zasobów IT, Administrator Systemów Informatycznych przeprowadza ocenę istotności i przydziela poziom bezpieczeństwa zasobowi IT, które zatwierdza Rektor.
3. Definiuje się następujące poziomy bezpieczeństwa zasobów IT:
    a. Wysoki (kluczowy) - przetwarzanie dużego zakresu danych osobowych lub zasób wymagany dla ciągłości funkcjonowania Uczeni,
    b. Średni - przetwarzany mały zakres danych osobowych, brak dostępności zasobu może zakłócić pracę pojedynczych jednostek organizacyjnych,
    c. Niski – przetwarzane dane nie są objęte ochroną lub brak dostępu nie zakłóca ciągłości funkcjonowania Uczelni.
4. W przypadku zasobów IT zakwalifikowanych do wysokiego poziomu bezpieczeństwa minimum raz na rok przeprowadza się analizę ryzyka. Proces przeprowadzania analizy ryzyka został opisany w Procedurze szacowania ryzyka systemów IT w Akademii Łomżyńskiej stanowiącej Załącznik nr 2 do PBI w AŁ.

4. Bezpieczeństwo komunikacji sieciowej

1. Dział Systemów Komputerowych odpowiada za wdrożenie wymaganych mechanizmów zabezpieczeń kontroli ruchu sieciowego i transmisji danych w Uczelni.
2. Sieć IT należy planować z uwzględnieniem aspektów, mających wpływ na kontrolę ruchu sieciowego i przepływ danych między systemami informacyjnymi.
3. Sieć lokalną Uczelni należy dzielić na obszary przeznaczone do celów dydaktycznych, w których nie są przetwarzane istotne dane oraz sieci, w których instalowane i przetwarzane

są dane chronione. Możliwość komunikacji między tymi sieciami należy ograniczać do niezbędnej minimalnej ilości usług.

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. Do zarządzania zasobami IT spoza infrastruktury informatycznej Uczelni wykorzystywane powinny być połączenia zapewniające szyfrowanie komunikacji (np. SSH, TLS, VPN).
7. Wysyłanie informacji chronionych poza sieć wewnętrzną wymaga stosowania mechanizmu szyfrowania np. poprzez SSH, SSL itp.
8. Zasób IT powinien zapewniać mechanizmy szyfrowania informacji chronionych przesyłanych przez sieci publiczne, za co odpowiada ASI danego zasobu IT.

5. Kontrola dostępu do zasobów IT

1. Zasady kontroli dostępu do zasobów IT muszą uwzględniać:
    a. Zasadę wiedzy koniecznej, tzn. konieczność nadania uprawnień/upoważnień wynikających wprost z rzeczywistych potrzeb związanych z wypełnianiem obowiązków służbowych.
    b. Zasadę minimalnych uprawnień, tzn. potrzebę przydzielenia tylko tych uprawnień, które są wymagane do wypełniania obowiązków służbowych.
    c. Ograniczenia prawne.
    d. Przydzielanie uprawnień do przetwarzania danych osobowych zgodnie z upoważnieniem wydanym przez AD.
2. Autoryzacja musi się odbywać każdorazowo przed próbą uzyskania dostępu do systemu IT. Jeżeli to możliwe, zaleca się stosowanie systemów wieloskładnikowego uwierzytelniania.
3. Zasady kontroli dostępu do systemów IT, w których przetwarzane są informacje chronione, muszą dodatkowo uwzględniać ograniczanie liczby użytkowników posiadających szczególne uprawnienia typu:
    a. prawo umożliwiające nieograniczony dostęp do systemów IT (tzw. prawa administratora);
    b. prawo umożliwiające zmianę przywilejów innych użytkowników;
    c. prawo umożliwiające zmianę logów systemu, wykraczające poza prawo zmiany tych logów na skutek bezpośredniego i zamierzonego przez twórców systemu wykonywania normalnych funkcji.
4. Zarządzanie uprawnieniami i kontrolą dostępu zgodnie z Polityką ochrony danych osobowych w Akademii Łomżyńskiej odbywa się z uwzględnieniem następujących metod:
    a. Podstawową metodą uwierzytelniania użytkowników w systemach komputerowych służących do przetwarzania danych osobowych są konta użytkowników. Konto składa się z identyfikatora użytkownika i hasła. W zależności od systemu dla danego konta można stosować zamiennie identyfikatory użytkownika (np. adres e-mail, numer indeksu, PESEL) z zachowaniem kontroli właściwego hasła.
    b. Identyfikator użytkownika jest jawny i może być nadawany przez administratora właściwego systemu informatycznego indywidualnie, generowany automatycznie lub wyznaczany na podstawie zapisanych danych użytkownika (np. adres e-mail, nr

indeksu), w zależności od specyfiki systemu komputerowego i uwierzytelniania użytkowników.

c. Identyfikator użytkownika, który stracił prawo do przetwarzania danych, należy niezwłocznie zablokować lub zmodyfikować uprawnienia w taki sposób, aby przetwarzanie nie było możliwe w systemie, do którego odwołano uprawnienia.
d. Ważność identyfikatora użytkownika w systemie służącym do przetwarzania danych, może być określana przez ASI na podstawie informacji zawartych na upoważnieniu lub na podstawie danych kadrowych, tj. dacie rozpoczęcia i zakończenia umowy o pracę lub zlecenia.
e. W przypadku utraty uprawnień użytkownika do przetwarzania danych, w/w identyfikatora nie można przydzielać innej osobie.
f. Hasło użytkownika powinno spełniać następujące wymagania:
    - hasło nie może być jednakowe z identyfikatorem użytkownika i nie może zawierać danych personalnych (np. imienia, nazwiska, daty urodzenia użytkownika),
    - hasło musi składać się z co najmniej 12 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
    - hasło musi być unikalne i nie powinno być powtarzane.
g. Nie może być wyświetlane na ekranie w trakcie wpisywania. Użytkownik zobowiązany jest do zachowania hasła w tajemnicy, również po ustaniu jego ważności.
h. Zaleca się okresową zmianę hasła np. co około 60 dni. Zasada ta nie dotyczy kont systemowych służących do automatycznej wymiany danych między systemami.
i. Hasła głównych kont systemowych, kont administracyjnych, interfejsów wymiany danych mogą być znane administratorom systemu i mają oni obowiązek zachowania ich w tajemnicy.
j. W przypadku złamania poufności hasła, użytkownik zobowiązany jest do jego natychmiastowej zmiany oraz do zgłoszenia tego faktu IOD oraz ASI.
k. W przypadku, gdy użytkownik zapomniał hasła, powinien:
    - samodzielnie wykonać procedurę resetowania hasła pod warunkiem, że aplikacja udostępnia taką funkcjonalność i istnieje możliwość dodatkowej weryfikacji tożsamości użytkownika,
    - zgłosić się do właściwego ASI w celu zresetowania hasła. Hasło wpisane przez ASI powinno być niezwłocznie zmienione przez użytkownika.
l. Zabrania się przesyłania haseł jawnym tekstem w wiadomościach e-mail.

5. DSK odpowiada za zarządzanie dostępem do zasobów IT.

6. Zabezpieczanie urządzeń końcowych

1. Za bezpieczeństwo fizyczne urządzeń końcowych, w tym nośników wymiennych, odpowiada osoba kierująca jednostką organizacyjną, w ramach której urządzenie końcowe jest eksploatowane. Konfigurację oprogramowania wykonuje właściwy pracownik DSK.
2. Konfiguracja urządzeń końcowych powinna zostać ustawiona na podstawie zaleceń producentów wykorzystywanego oprogramowania oraz ogólnie uznanych za poprawne, zasady i standardy bezpieczeństwa. W szczególności powinna obejmować:

a. instalację wyłącznie niezbędnych pakietów oprogramowania,
b. aktualizację zainstalowanego oprogramowania zgodnie z zaleceniami ich producentów,
c. wdrożenie zasad kontroli dostępu, w tym zmianę domyślnych parametrów związanych z bezpieczeństwem,

3. Urządzenia końcowe powinny być tak skonfigurowane by zapewnić bieżącą aktualizację oprogramowania i instalację poprawek, zarówno systemowych jak i bezpieczeństwa.
4. Ochronie antywirusowej podlegają wszystkie urządzenia końcowe, na których taka ochrona jest technologicznie możliwa i nie wpłynie ona znacząco na ich funkcjonalność, wydajność lub dostępność.
5. Ustawienia ochrony antywirusowej muszą zapewniać następujący minimalny zakres funkcjonalności:
   a. mechanizmy ochrony antywirusowej blokują aktywność złośliwego oprogramowania (wirusów),
   b. konfiguracja ochrony zapewnia codzienną automatyczną aktualizację baz sygnatur,
   c. działanie ochrony przez cały czas (tzn. realizacja tzw. ochrony w czasie rzeczywistym).
6. Urządzenia nieprzyłączone do sieci z dostępem do Internetu muszą być aktualizowane ręcznie. Za ich cykliczną aktualizację odpowiada właściwy ASI zasobu IT.
7. Użytkownik powiadomiony o aktywności złośliwego oprogramowania musi niezwłocznie zgłosić takie zdarzenie zgodnie z obowiązującą w Uczelni Procedurą zarządzania incydentami związanymi z bezpieczeństwa informacji.

7. Ochrona urządzeń mobilnych

1. Kierownicy jednostek organizacyjnych Uczelni zobowiązani są do opracowania i aktualizacji wykazu pracowników, którzy otrzymali urządzenia mobilne (np. laptop, przenośne nośniki pamięci) do realizacji zadań służbowych poza siedzibą Uczelni.
2. Mechanizmy ochrony urządzeń mobilnych implementowane są zgodnie z zakresem przedstawionym dla urządzeń końcowych.
3. W urządzeniach mobilnych, które mogą służyć do przetwarzania informacji poufnych należy stosować metody szyfrowania uniemożliwiające odczyt danych przy pomocy innego oprogramowania niż zainstalowane i skonfigurowane przez pracownika DSK.
4. Dostęp do zasobów chronionych z urządzenia mobilnego spoza siedziby uczelni możliwy jest za pośrednictwem połączenia VPN i jest ograniczony do minimalnej ilości usług.
5. Pełny dostęp do zasobów chronionych możliwy jest z wykorzystaniem połączenia VPN i usług pulpitu zdalnego w systemie zainstalowanym w siedzibie Uczelni. Metoda ta powinna uniemożliwiać zapisywanie danych na urządzeniu mobilnym.
6. Naprawa przez dostawców IT urządzenia zawierającego informacje chronione może odbywać się po wcześniejszym usunięciu z niego wszystkich informacji chronionych zawartych na dysku, w sposób uniemożliwiający ich odczytanie. W przypadku braku możliwości usunięcia danych z nośnika, należy go zdemontować.
7. Wsparcie w zakresie realizacji zapisów pkt. 2-6, na wniosek kierownika jednostki organizacyjnej Uczelni lub użytkownika wykonuje DSK.

8. Usługi zewnętrzne i chmurowe

1. Zasoby IT funkcjonujące poza infrastrukturą Uczelni lub w tzw. chmurze publicznej lub w infrastrukturze innego zewnętrznego podmiotu mogą przetwarzać dane chronione pod warunkiem przeprowadzenia oceny ryzyka związanego z takim przetwarzaniem.
2. W analizie ryzyka usług zewnętrznych należy ocenić w szczególności:
    a. możliwość wglądu w bezpieczeństwo infrastruktury dostawcy takich usług,
    b. mechanizmy detekcji i usuwania zagrożeń,
    c. szyfrowanie danych,
    d. zapewnienie odpowiedniej granulacji ról i uprawnień,
    e. mechanizmy zapobiegające wyciekom danych.

9. Kopie zapasowe

1. Czynności tworzenia kopii zapasowych powinny zapewniać:
    a. zgodność kopii informacji z informacjami źródłowymi,
    b. możliwość odtworzenia kompletnej informacji z posiadanych kopii.
2. Zasady tworzenia kopii zapasowej dla zasobu IT powinny obejmować w szczególności:
    a. zakres danych podlegających backupowi (nazwa zbioru, katalogu, bazy itp.),
    b. jak często powinny być tworzone kopie zapasowe danych (np.: codziennie, raz na tydzień, raz w miesiącu, itp.),
    c. jaki jest okres przechowywania kopii zapasowych lub ilość poprzednich wersji możliwych do odtworzenia,
    d. miejsce składowania kopii.
3. Dokumentacja, o której mowa w ust. 2, może być prowadzona w formie papierowej lub w przeznaczonym do tego celu zasobie IT.

10. Zarządzanie zmianą zasobów IT

1. Rozwój zasobów IT musi uwzględniać działania mające na celu wdrożenie właściwej ochrony systemów oraz informacji przetwarzanych z wykorzystaniem tego zasobu, a w szczególności:
    a. klasyfikację informacji przetwarzanych przez wdrażany lub modyfikowany zasób IT,
    b. klasyfikację niezawodności i dostępności wdrażanego lub modyfikowanego zasobu IT,
    c. jeżeli możliwe, testowanie przedwdrożeniowe w celu weryfikacji zgodności zasobu IT z wymaganiami bezpieczeństwa IT przed jego uruchomieniem,
    d. dokumentowanie wdrażanych zmian zasobów IT i ich ewentualnego wpływu na bezpieczeństwo IT.
2. Zaleca 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. Aktualizacje wersji oprogramowania należy przeprowadzać w sposób minimalizujący ryzyko uszkodzenia danych poprzez wyłączenie dostępu z sieci publicznej lub zablokowanie możliwości logowania użytkowników.
5. Wdrażanie nowych zasobów IT lub znacznych zmian mogących mieć wpływ na bezpieczeństwo danych należy testować w dedykowanym środowisku testowym lub ograniczyć dostęp do sieci wewnętrznej oraz minimalnej grupy użytkowników wykonujących prace wdrożeniowe.
6. Jeżeli to możliwe, rozwój i testowanie zasobów IT, należy przeprowadzać z wykorzystaniem danych testowych.

11. Ciągłość działania (dostępność) zasobów IT

1. Systemy o znaczeniu kluczowym dla funkcjonowania Uczelni należy monitorować i rozwijać w taki sposób aby ewentualne przerwy w funkcjonowaniu były jak najkrótsze, a planowane przerwy występowały w okresach najmniejszego zapotrzebowania tych systemów
2. Dla zasobów o znaczeniu kluczowym dla ciągłości działalności Uczelni należy opracować plan ciągłości działania ze szczególnym uwzględnieniem mechanizmów zapewniających odporność na awarie oraz sposób przywrócenia do sprawności po wystąpieniu awarii.
3. Wybrane elementy planu ciągłości działania należy okresowo testować w celu sprawdzeniu poprawności procedury, minimalizacji ewentualnych błędów w kopiach bezpieczeństwa lub konfiguracji.

12. Monitorowanie zasobów IT

1. Monitorowanie zasobów IT ma na celu zapewnienie jak najwyższego poziomu integralności, poufności i dostępności systemów IT kluczowych dla zapewnienia ciągłości działania Uczelni.
2. Monitorowanie tych zasobów realizują odpowiedni ASI.
3. Zakres rejestrowanych zdarzeń w procesie monitorowania bezpieczeństwa IT powinien obejmować:
    a. naruszenia bezpieczeństwa monitorowanego systemu i danych w nim przetwarzanych (integralności, poufności i dostępności),
    b. objawów nietypowego i nieprawidłowego działania monitorowanych systemów,
    c. symptomów niedostatecznej wydajności i dostępności dla użytkowników,
    d. innych przejawów wynikłych z wad oprogramowania, niezgodności konfiguracji systemu z dokumentacją itp.
4. Zdarzenia wykryte w następstwie monitorowania bezpieczeństwa podlegają rozpoznaniu i ewentualnej obsłudze zgodnie z obowiązującą w Uczelni „Procedurą zarządzania incydentami związanymi z bezpieczeństwem informacji ”.
5. Wyłączenie monitorowania, bądź usunięcie danego zasobu IT z procesu monitorowania, może nastąpić w następujących przypadkach:
    a. wyłączenia danego zasobu IT,
    b. zatwierdzonej zmiany klasyfikacji bezpieczeństwa takiego zasobu IT,
    c. odrębnej, uzasadnionej pisemnej decyzji w ramach obsługi odstępstwa (np. na wniosek JM Rektora, w trybie pilnym).

6. 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:
    a. dzienniki nie przepełnią się do czasu ich archiwizacji,
    b. nie zostaną utracone żadne informacje o zdarzeniach związanych z bezpieczeństwem,
    c. jeśli to możliwe należy stosować zewnętrzny serwer rejestrowania zdarzeń. Lub wydzielić osobny dysk bądź przynajmniej partycję i nadać im uprawnienia ograniczające dostęp do uprawnionych operatorów i administratorów,
7. Rejestrowane w systemie zdarzenia mogą być monitorowanie na jeden z poniższych sposobów:
    a. automatyczny, powiadamiający co najmniej jednego ASI danego zasobu IT o ewentualnych zdarzeniach,
    b. manualny, przez uprawnionego operatora lub administratora.

13. Zarządzanie podatnościami zasobów IT

1. Zasoby IT powinny być monitorowane i badane pod kątem występowania w nich podatności obniżających ich bezpieczeństwo.
2. Priorytet monitorowania i badania podatności powinien zależeć od klasyfikacji bezpieczeństwa danego zasobu IT lub grupy takich zasobów.
3. W zależności od źródła podatności należy je eliminować poprzez:
    a. aktualizację oprogramowania użytkowego lub systemowego, jeżeli stosowna aktualizacja została wydana,
    b. zmianę konfiguracji, jeżeli występujące błędy są jej źródłem,
    c. izolację podatności poprzez ograniczenie dostępu do zasobu, wdrożenie dodatkowego filtrowania i uwierzytelniania z wykorzystaniem systemu firewall lub podobnych, jeżeli nie jest możliwa bezzwłoczna izolacja podatności poprzez aktualizację oprogramowania lub poprawę konfiguracji,
4. Jeżeli to możliwe, należy przetestować zaproponowane zmiany eliminujące podatność przed ich zastosowaniem, w celu oceny skuteczności tego mechanizmu oraz braku jego negatywnego wpływu na funkcjonowanie zasobu.
5. 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.

14. Bezpieczeństwo poczty elektronicznej

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).
4. Serwer z poczty elektronicznej musi stosować mechanizmy SPF, DKIM oraz DMARC w celu weryfikacji nadawcy wiadomości.

15. Bezpieczeństwo aplikacji webowych

1. Dostęp do aplikacji internetowych, w których przetwarzane są dane osobowe lub informacje niepubliczne powinien być możliwy tylko w ramach sesji, w której uprzednio nastąpiło poprawne uwierzytelnienie (identyfikacja) użytkownika.
2. Zaleca się aby uwierzytelnianie użytkowników w aplikacji odbywało się przy użyciu wdrożonego na Uczelni Centralnego Systemu Uwierzytelniania lub, jeśli to niemożliwe, przy użyciu identyfikatora i hasła.
3. Cały proces komunikacji z aplikacją powinien być realizowany poprzez szyfrowany kanał komunikacyjny (HTTPS).
4. Sesja użytkownika w komunikacji z aplikacją, jest sekwencją niezależnych żądań i odpowiedzi protokołu HTTP. Każdy użytkownik musi być traktowany i śledzony przez aplikację indywidualnie w danej interakcji z aplikacją, po to by spełnić postulat poufności informacji przetwarzanej przez użytkownika.
5. Szczegóły dot. zaistniałych błędów aplikacji lub błędów logowania użytkownika powinny znajdować się wyłącznie w dziennikach zdarzeń dostępnych dla ASI.
6. Dostęp do interfejsów administracyjnych lub modułów aplikacji odpowiadających za czynności administracyjne powinien być ograniczony tylko do sieci wewnętrznej.

16. Bezpieczeństwo serwerów

1. Systemy serwerowe wspierające zasoby IT Uczelni, w zależności od rodzaju i sposobu udostępniania zasobów przepisywane są do grup:
    a. Serwer fizyczny – system serwerowy z zainstalowanymi usługami bez zainstalowanego środowiska wirtualizacji,
    b. Serwer zwirtualizowany – system serwerowy z zainstalowanym środowiskiem wirtualizacji nadzorcy (hypervisior) systemów wirtualnych z zainstalowanymi usługami,
    c. Serwer wirtualny – system serwerowy uruchomiony jako usługa serwera zwirtualizowanego.
2. Jeżeli to możliwe, wersje testowe nowych lub modyfikowanych systemów należy testować w środowiskach odseparowanych od systemów produkcyjnych w celu minimalizacji negatywnego wpływu ewentualnych błędów lub podatności.
3. Wszystkie interfejsy zarządzania serwerami (SSH, RDP, interfejsy zarządzania systemem wirtualizacji, interfejsy typu remote management console (RMC), muszą być instalowane w sieci dostępnej dla pracowników DSK.
4. Wszystkie główne serwery muszą znajdować się przeznaczonych do tego celu pomieszczeniach specjalnych IT lub serwerowniach.
5. Dostęp do usług uruchomionych w poszczególnych systemach serwerowych musi być ograniczany do niezbędnego minimum za pomocą mechanizmów firewall i list kontroli

dostępu (ACL), realizowanych w systemie serwera lub w urządzeniu sieciowym firewall lub router.

17. Bezpieczeństwo systemów peryferyjnych

1. Urządzenia peryferyjne typu kamery CCTV, telefony IP itp. należy instalować w wyodrębnionych podsieciach IP w celu zapewnienia jakości parametrów transmisyjnych, blokowanie dostępu z sieci publicznych oraz minimalizacji wpływu na systemy przetwarzające dane chronione. Dodatkowo należy zmieniać domyślne dane uwierzytelniania oraz wyłączać protokoły i usługi, które nie są wymagane do poprawnej pacy tych systemów w Uczelni.
2. Sieciowe urządzenia drukujące i skanery należy instalować w sieciach uniemożliwiających dostęp z sieci publicznej oraz dydaktycznej.

18. Eksploatacja i utrzymanie zasobów IT

1. Serwisowanie lub naprawa zasobów IT, przetwarzających informacje chronione, przez dostawców IT może odbywać się wyłącznie:
    a. pod nadzorem właściwego ASI,
    b. bez nadzoru ASI, jeśli wcześniej zostały przez ASI skutecznie usunięte z nich wszystkie informacje chronione
    c. bez nadzoru ASI, jeżeli wcześniej zawarto stosowną umowę powierzenia danych.

19. Wycofywanie zasobów IT z eksploatacji

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:
    a. archiwizację informacji chronionych,
    b. usunięcie informacji chronionych, zgodnie z obowiązującymi przepisami prawa i wewnętrznymi regulacjami.
3. Sposób zabezpieczenia informacji chronionych przetwarzanych z wykorzystaniem zasobu IT wycofywanego z eksploatacji należy ustalić z kierownikiem jednostki, w której dany zasób był eksploatowany.
4. Nośniki danych wycofywanego z eksploatacji zasobów IT, w szczególności przetwarzających informacje chronione, powinny zostać wyczyszczone w sposób uniemożliwiający ich odtworzenie, dotyczy to:
    a. dysków fizycznych,
    b. pamięci szybkich (SSD),
    c. nośników podręcznych (USB),
    d. taśm magnetycznych do wykonywania kopii zapasowych.
5. Usuwanie, niszczenie danych z wycofywanych nośników należy przeprowadzić poprzez:
    a. Trzykrotne nadpisanie całej powierzchni dysku za pomocą specjalnego oprogramowania (np. KillDisk).
    b. Fizyczne zniszczenie nośnika typu dysk twardy, poprzez wykonanie co najmniej 3 przewiertów, w przypadku nośnika uszkodzonego lub zbyt długiego czasu wymaganego do wykonania czyszczenia przez 3 krotne nadpisanie.

    c. Fizyczne niszczenie nośników typu taśmy magnetyczne poprzez przecięcie wzdłuż średnicy szpuli z nawiniętą taśmą.
    d. Przekazanie nośników do dostawcy IT specjalizującego się w niszczeniu nośników danych.
6. Proces niszczenia nośników należy udokumentować za pomocą stosownego protokołu.
7. Zniszczone nośniki danych należy przekazać do podmiotu utylizującego urządzenia elektroniczne.