Polityka Bezpieczeństwa Informacji Akademia Sztuk Pięknych im. Eugeniusza GEPPERTA we Wrocławiu (ASP)

System Zarządzania Bezpieczeństwem Informacji wraz z opisem procedur

ZATWIERDZAM

REKTOR
Akademii Sztuk Pięknych
im. Eugeniusza Gepperta
we Wrocławiu
prof. Wojciech Pukocz

Spis treści

1. Metryka dokumentu.

Właściciel	AKADEMIA SZTUK PIĘKNYCH IM. EUGENIUSZA GEPPERTA WE WROCŁAWIU			
Tryb zatwierdzenia:	Dokument zatwierdza REKTOR ASP			
Stan	**ZATWIERDZONY**	Data zatwierdzenia: 15.01.2025		
Adresaci	Z dokumentem (lub wyciągiem z PBI) należy zapoznać: • Najwyższe kierownictwo • Użytkowników systemów informacyjnych ASP			
Historia dokumentu	Wersja	Data utworzenia	Autor	Opis zmian (szczegóły zmian w Rejestrze zmian)
	1.0	14.01.2025		Utworzenie dokumentu

2. Wstęp.

Na podstawie § 19 Rozporządzenia Rady Ministrów z dnia 21 maja 2024r. w sprawie Krajowych Ram Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2024 poz. 773) oraz art. 24 ust 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (DZ.U UE L Nr 119s.1 oraz DZ.U UE L Nr 127 s.2) oraz w związku z *Ustawą o Krajowym systemie cyberbezpieczeństwa* z dnia 5 lipca 2018r. (Dz.U. 2024 poz. 1077 t.j.) ustanawia się System Zarządzania Bezpieczeństwem Informacji zapewniający poufność, integralność oraz dostępność informacji niezbędnych do niezakłóconej realizacji usług.

System Zarządzania Bezpieczeństwem Informacji w ASP opisuje niniejsza Polityka Bezpieczeństwa Informacji (PBI).

Podstawowym zadaniem PBI jest udokumentowanie opracowanych i wdrożonych lub planowanych do wdrożenia zaleceń i regulacji dotyczących obszaru bezpieczeństwa informacji w oparciu o międzynarodową normę PN-ISO/IEC 27001, które zapewnią odpowiedni poziom bezpieczeństwa dla całej organizacji (Akademii Sztuk Pięknych im. Eugeniusza Gepperta we Wrocławiu), ze szczególnym uwzględnieniem systemu informatycznego niezbędnego do zapewnienia niezakłóconej realizacji usług.

3. Pojęcia, definicje, skróty:

W dokumentach składających się na całość Polityki Bezpieczeństwa Informacji zastosowano wymienione w poniższej tabeli definicje i skróty będące uzupełnieniem **dokumentu Zarządzanie Ryzykiem (Pojęcia i definicje).**

Lp.	Pojęcia, definicje, skróty	Definicja/Rozwinięcie skrótu
1.	ASI	Administrator Systemów Informatycznych
2.	Cyberbezpieczeństwo	odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.
3.	CSIRT GOV	Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego
4.	CSIRT NASK	Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy
5.	Incydent krytyczny	incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV
6.	Incydent poważny	incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;
7.	Obsługa incydentu	czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetowanie, podejmowanie działań naprawczych i ograniczenie skutków incydentu;
8.	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 (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 wraz z przetwarzanymi w nim danymi w postaci elektronicznej).
9.	Jednostka	jednostka rozumie się przez to Akademię Sztuk Pięknych we Wrocławiu
10.	Inspektor Ochrony Danych	Inspektor Ochrony Danych (IOD)-osoba wyznaczona przez Rektora ASP, odpowiedzialna za organizację oraz nadzorująca przestrzeganie zasad dotyczących ochrony danych osobowych;
11.	KRI	rozumie się przez to rozporządzenie Rady Ministrów z dnia 9 listopada 2017 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów Publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
12.	RODO	rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679zdnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
13.	Użytkownik	użytkownik pracownik jednostki posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;

Lp.	Pojęcia, definicje, skróty	Definicja/Rozwinięcie skrótu
14.	Zabezpieczenie Systemu Informatycznego	zabezpieczenie systemu informatycznego należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
15.	Nośnik Informacji	nośnik informacji(wymienny)-nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde itp.;
16.	Informatyk	informatyk-należy przez to rozumieć pracownika Działu IT w Akademii Sztuk Pięknych we Wrocławiu.
17.	ASP	Akademia Sztuk Pięknych im. Eugeniusza Gepperta we Wrocławiu.
18.	Gestor	Rektor
19.	Najwyższe Kierownictwo	Rozumie się przez to Rektora, Prorektorów i Kanclerza

4. Cel i zakres Polityki Bezpieczeństwa Informacji:

Postanowienia ogólne

1. Niniejsza Polityka Bezpieczeństwa Informacji w ramach Systemu Zarządzania Bezpieczeństwem Informacji Akademii Sztuk Pięknych im. Eugeniusza Gepperta we Wrocławiu jest dokumentem głównym ustanowionego w jednostce systemu zarządzania bezpieczeństwa informacji.
2. Dokument ma charakter deklaratywny, zawierający ogólne ramy, wymagania, zasady, procedury oraz instrukcje w zakresie ochrony informacji przetwarzanych w jednostce oraz jest nadrzędny w stosunku do pozostałych wewnętrznych aktów prawnych dotyczących bezpieczeństwa informacji obowiązujących w jednostce, tworząc wspólnie z nimi kompleksową, spójną dokumentację bezpieczeństwa.
3. Ponieważ informacje to aktywa, które podobnie jak inne ważne aktywa są niezbędne dla prawidłowego funkcjonowania jednostki, z tego powodu podlegają ochronie.
4. Zakres ustanowionego SZBI obejmuje:
   - realizowane w jednostce procesy związane z przetwarzaniem informacji;
   - wszelkie informacje przetwarzane w ramach ww. procesów, w tym:
     - przetwarzane w formie tradycyjnej (m.in. informacje wydrukowane lub zapisane na papierze),
     - przetwarzane w formie elektronicznej (np. w systemach informatycznych jednostki, przesyłane za pomocą poczty elektronicznej lub urządzeń elektronicznych, elektronicznych nośników informacji).
     - przetwarzane w postaci słownych wypowiedzi, będące własnością jednostki lub zainteresowanych stron, o ile zostały przekazane lub pozyskane na podstawie obowiązujących przepisów prawa lub zawieranych umów;
   - aktywa wspierające przetwarzanie informacji w ramach ww. procesów m.in.:
     - personel (w tym wszyscy pracownicy jednostki bez względu na podstawę zatrudnienia, praktykanci, stażyści, wolontariusze),
     - budynki i pomieszczenia jednostki, w których są lub będą przetwarzane informacje,

- sprzęt, w tym sprzęt komputerowy, urządzenia mobilne oraz inne nośniki danych, na których znajdują się informacje podlegające ochronie, oprogramowanie, infrastruktura sieciowa,
- technologie służące pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i udostępnianiu informacji, do których zalicza się zarówno systemy papierowe jak i elektroniczne wspomagające realizację zadań publicznych,
- strukturę organizacyjną jednostki, określoną w wewnętrznych uregulowaniach w postaci Regulaminu Organizacyjnego jednostki.

5. Dokumentami powiązanymi z niniejszym PBI są w szczególności:
   - Polityka Ochrony Danych Osobowych;
   - Procedury audytu wewnętrznego, kartę audytu wewnętrznego oraz Kodeks etyki audytora wewnętrznego;
   - Regulamin Pracy stanowiący załącznik do Zarządzenia Rektora nr I/49/2019;
6. Najwyższe kierownictwo ASP dąży do tego, aby dokumenty były ze sobą spójne.

Deklaracje Kierownictwa

Rektor ASP świadomy jest zagrożeń związanych z przetwarzaniem w jednostce dużej liczby informacji, w tym szczególnie chronionych danych osobowych oraz wynikających z tego zagrożeń związanych z dynamicznym rozwojem metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych. Zgodnie z treścią § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów Publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, w ASP realizującym zadania publiczne ustanawia się, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Zaś art.24 Rozporządzenia Parlamentu Europejskiego i Rady(UE)2016/679 z dnia 27 kwietnia 2016r.wsprawie ochrony osób fizycznych w z przetwarzaniem danych osobowych iw sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE określa obowiązki administratora polegające na założeniu, iż uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Wielopoziomowy i zintegrowany System Zarządzania Bezpieczeństwem Informacji (SZBI) oparty został na podejściu wynikającym z szacowania ryzyka i odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji, tj. ochrony informacji na każdym etapie jej przetwarzania. Wymagania SZBI mają charakter zintegrowany z innymi procesami realizowanymi przez Akademii Sztuk Pięknych im. Eugeniusza Gepperta we Wrocławiu.

Rektor ASP deklaruje zamiar:

1. Doskonalenia systemu zarządzania bezpieczeństwem informacji, aby zapewnić poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

2. Stosowania odpowiednich środków informatycznych, technicznych i organizacyjnych zapewniających ochronę przetwarzanych informacji ze szczególnym uwzględnieniem danych osobowych, a w szczególności ich zabezpieczeniem przed:

- udostępnieniem osobom nieupoważnionym,
- przetwarzaniem z naruszeniem obowiązujących przepisów,
- zmianą, utratą, uszkodzeniem lub zniszczeniem;

3. Podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem informacji, w tym zapewnienia, aby dane te były:

- Przetwarzane zgodnie z prawem;
- Przetwarzane wyłącznie w celu realizacji ustawowych zadań;
- Zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu;
- Przetwarzane niezgodnie z tymi celami;
- Merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
- Przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;

4. Stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających informacje w ASP w zakresie problematyki bezpieczeństwa tych informacji;

5. Właściwego traktowania obowiązków osób zatrudnionych przy przetwarzaniu informacji wynikających z niniejszego dokumentu jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby;

6. Doskonalenia i rozwijania organizacyjnych, technicznych oraz informatycznych środków ochrony informacji, przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznymi tak, aby skutecznie zapobiegać zagrożeniom związanym z:

- Infekcjami wirusów i innego niebezpiecznego oprogramowania mogącego przyczynić się do nieautoryzowanego przejęcia zasobów komputera lub danych przetwarzanych sieciowo;
- Spamem, wprowadzającym nieład informacyjny mogącym stanowić potencjalne zagrożenie dla informatycznych zasobów ASP;
- Dostępem do stron internetowych, które zaopatrzone są w skrypty pozwalające wykradać zasoby komputera;
- Lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez ich zabezpieczenia;
- Brakiem świadomości niebezpieczeństwa dopuszczania osób postronnych do swojego stanowiska pracy;
- Atakami z sieci mającymi na celu opóźnienie lub uniemożliwienie dostępu do danych;
- Działaniami mającymi na celu zaburzenie integralności danych, w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści;
- Kradzieżą sprzętu lub nośników z danymi;
- Przekazywaniem sprzętu z danymi do serwisu;

- Innymi zagrożeniami mogącymi wystąpić w przyszłości w związku rozwojem technik i metod przetwarzania danych;

Jednocześnie Rektor ASP zamierza doskonalić i rozwijać nowoczesne metody przetwarzania informacji.

Podstawowe cele ustanowienia zasad dotyczących zapewnienia bezpieczeństwa informacji systemu teleinformatycznego w ASP to:

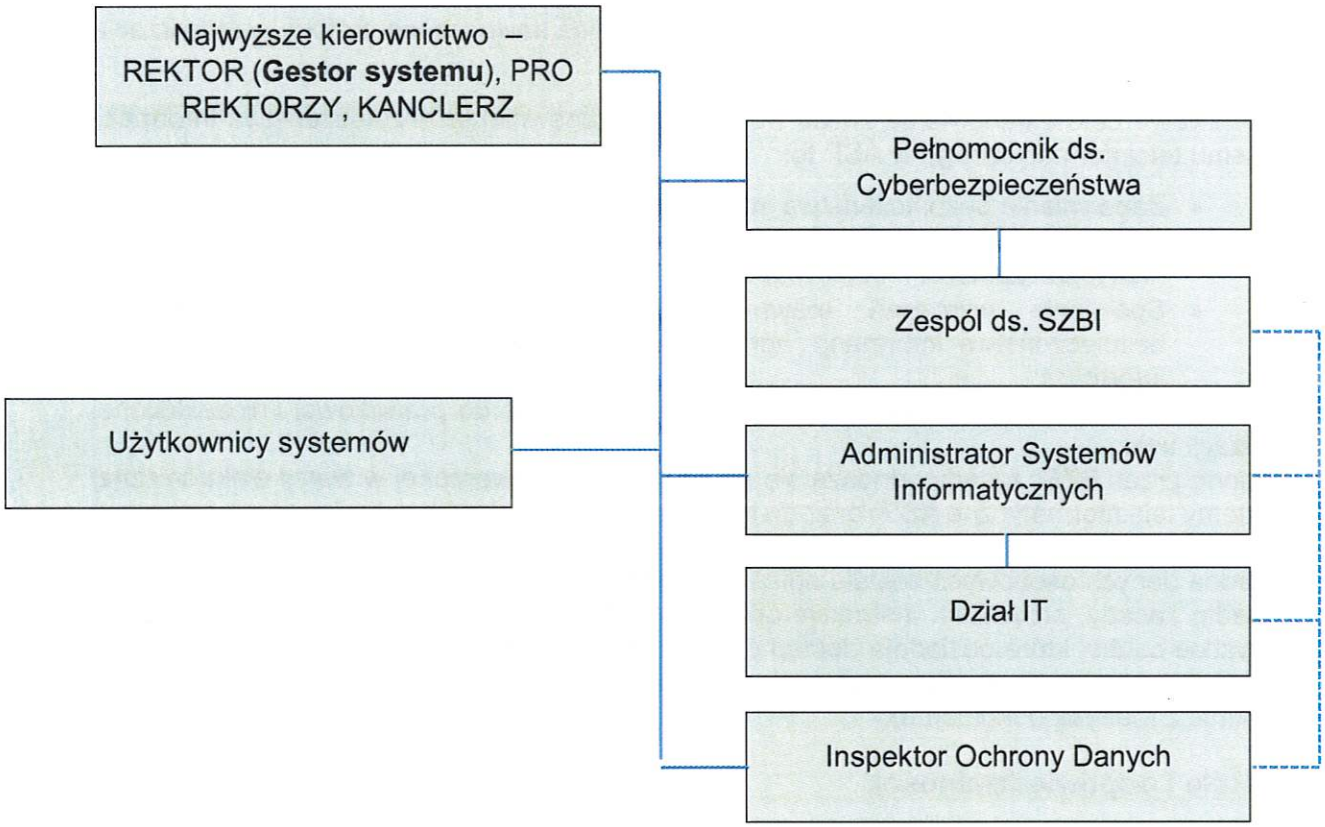
- Zapewnienie bezpieczeństwa informacji (poufności, integralności oraz dostępności z uwzględnieniem dodatkowych atrybutów: autentyczności, rozliczalności, niezaprzeczalności i niezawodności);
- Spełnienie wymagań prawnych (obowiązujących przepisów prawa dot. bezpieczeństwa informacji, norm branżowych, norm z zakresu bezpieczeństwa informacji;

Zakres SZBI obejmuje systemy informacyjne ASP niezbędne do prawidłowej i niezakłóconej realizacji usług.
Opisane przez SZBI zasady odnoszą się do informacji przetwarzanej w wersji elektronicznej (systemy teleinformatyczne ASP) oraz do informacji przetwarzanych w tradycyjny (papierowy) sposób, niezbędnych do realizacji usług kluczowych.
Ochrona danych osobowych została opisana w **Polityce ochrony danych osobowych.**
Ponadto zasady, procedury, instrukcje opisane w dokumencie muszą być stosowane przez wszystkie osoby, które posiadają dostęp do systemów informacyjnych ASP. Dokument musi być znany wszystkim osobom posiadającym dostęp do informacji chronionych tą polityką (zgodnie z metryką dokumentu).

5. Role i odpowiedzialności:

PBI została opracowana zgodnie z wymaganiami normy PN-ISO/IEC 27001. w ramach podziału ról w ASP utworzono stanowisko Pełnomocnika ds. cyberbezpieczeństwa oraz powołano Zespół ds. SZBI.

5.1. Struktura odpowiedzialności za bezpieczeństwo informacji:



5.2. Wykaz ról i odpowiedzialności:

Rola	Odpowiedzialność (zadania)	Zależność
Administrator Systemów Informatycznych (ASI)	Do zadań **Administratora Systemów Informatycznych** należy: • Tworzenie, utrzymanie, aktualizacja polityk, procedur i innych regulacji z zakresu eksploatacji systemów informatycznych. • Współpraca z **Inspektorem Ochrony Danych.** • Współpraca **z Pełnomocnikiem ds. Cyberbezpieczeństwa.** • Udział w pracach Zespołu ds. Cyberbezpieczeństwa. • Planowanie architektury bezpieczeństwa systemów informatycznych, w szczególności planowanie niezbędnych zmian w architekturze bezpieczeństwa, akceptacja mechanizmów bezpieczeństwa poszczególnych systemów. • Kontrola i monitorowanie we współpracy z **Pełnomocnikiem ds. cyberbezpieczeństwa** oraz	**Rektor**

	Inspektorem Ochrony Danych, poprawności funkcjonowania mechanizmów bezpieczeństwa systemów informatycznych od strony technicznej. • Czynny udział w procesie analizy ryzyka dotyczących systemów informatycznych. • Raportowanie i okresowa ocena z zakresu bezpieczeństwa systemów informatycznych. • Współpraca z innymi podmiotami np. podmiotami realizującymi zadnia na rzecz **Rektora.** • Udzielanie rekomendacji w zakresie bezpieczeństwa systemów informatycznych. • Uczestnictwo w procesach wymagających decyzji z zakresu bezpieczeństwa informacji. • Nadzór nad przeprowadzanymi naprawami, pracami związanymi z konserwacją bądź likwidacją urządzeń wchodzących w skład systemu informatycznego, • Dbałość o aktualizację oprogramowania. • Ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym. • Nadzór nad wykonywaniem kopii zapasowych, ich testowaniem, przechowywaniem oraz ich późniejszą likwidacją.	
Audytor wewnętrzny	Rola odpowiedzialna za obszar związany z potrzebą kontroli (badania zgodności) organizacji/systemów z wytycznymi dotyczącymi bezpieczeństwa informacji. • Przygotowanie planu audytowego (ustalenie zakresu, terminów). • Ogłoszenie planu audytowego. • Bieżące raportowanie wykrytych niezgodności. • Reprezentacja komórki audytu na wszystkich etapach prowadzonego audytu wewnętrznego. • Opracowanie i dostarczenie do **Rektora** raportu z audytu. • Przekazanie audytowanemu (dotyczy także uprawnionych kierowników komórek organizacyjnych audytowanego) wniosków wynikających z kontroli (w porozumieniu z **Rektorem**).	**Rektor**
Rektor	Rektor ASP podejmuje decyzje: • O wdrożeniu systemu zarządzania bezpieczeństwem w systemie informacyjnym. • O zakresie wykorzystania systemu/aplikacji oraz w zakresie zapewnienia bezpieczeństwa informacji systemu. Gestor systemu odpowiada: • Za wdrożenie i respektowanie postanowień niniejszej PBI przez wszystkich uczestników systemu.	

	• Zapewnienie prawidłowej realizacji zadań Pełnomocnika ds. Cyberbezpieczeństwa. • Za realizację procesu zarządzania ryzykiem. Dokonuje akceptacji wyników szacowania ryzyka i wybranych sposobów postępowania z ryzykiem oraz akceptacji ryzyka. • Zapewnia realizację audytów bezpieczeństwa informacji. • Jest głównym właścicielem ryzyka bezpieczeństwa informacji systemu. • Przypisuje wybrane działania postępowania z ryzykiem do realizacji właściwym kierownikom komórek organizacyjnych (właścicielom ryzyka). • Przeprowadza przegląd zarządzania bezpieczeństwem informacji. • Zapewnia właściwy nadzór na PBI i związanymi z nią dokumentami, stanowiącymi dokumentację bezpieczeństwa. • Prowadzi proces ciągłego doskonalenia polityki bezpieczeństwa informacji i zarządzania bezpieczeństwem informacji w ASP	

Pełnomocnik ds. Cyberbezpieczeństwa	Do głównych zadań Pełnomocnika należy:
	• Utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
	• Prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem.
	• Przygotowanie dla Rektora sprawozdania z analizy ryzyka wraz z planem postępowania z ryzykiem.
	• Wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym:
	  • utrzymanie i bezpieczną eksploatację systemu informacyjnego,
	  • bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
	  • bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,
	  • wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
	  • objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi
		Rektor

	kluczowej systemem monitorowania w trybie ciągłym.
	• Współpraca z Inspektorem Ochrony Danych,
	• Zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.
	• Zarządzanie incydentami.
	• Stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego, w tym:
	  • stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
	  • niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa;	

Użytkownik	Użytkownik to osoba korzystająca z systemu informacyjnego ASP.	**Rektor**
Inspektor Ochrony Danych	Zadania i obowiązki IOD opisane są w Polityce Bezpieczeństwa Przetwarzania Danych Osobowych obowiązującej w ASP.	**Rektor**

6. Struktura dokumentacji PBI:

Polityka Bezpieczeństwa Informacji opisuje zasady zarządzania i zapewnienia bezpieczeństwa informacji ustanowione dla systemu informacyjnego niezbędnego do prawidłowej i niezakłóconej realizacji zadań przez ASP.
Wszystkie procedury, instrukcje, zasady dotyczące PBI zostały zawarte i opisane w niniejszym dokumencie.
Częścią PBI jest dokument: **Zarządzanie Ryzykiem** stanowiący integralną część Polityki Bezpieczeństwa Informacji dla systemów informacyjnych niezbędnych do zapewnienia przez ASP niezakłóconej realizacji usług.

6.1. Zgodność dokumentacji PBI:

Dokumentacja PBI została opracowana na podstawie normy PN-ISO/IEC 27001:2022 opisującej wymagania Systemu Zarządzania Bezpieczeństwem Informacji oraz PN-ISO/IEC 27002:2014 opisującej praktyczne zasady zabezpieczania informacji.
System zarządzania ryzykiem jako integralna część PBI, opracowano na podstawie normy PN-ISO/IEC 27005:2014.
Instrukcje, procedury dotyczące ciągłości działania odnoszą się do normy PN- EN-ISO/IEC 22301.
W procedurach opisujących zarządzenie systemami informatycznymi wykorzystano zapisy normy PN-ISO/IEC 20000-1/2014.

6.2. Nadzór nad dokumentacją PBI:

Rektor ASP zapewnia właściwy nadzór nad dokumentacją PBI. w imieniu Rektora nadzór nad PBI sprawuje Kanclerz i Pełnomocnik ds. Cyberbezpieczeństwa.
PBI oraz związana z nią dokumentacja Zarządzania Ryzykiem podlegają nadzorowi w celu zapewnienia:

- Przydatności i adekwatności;
- Użyteczności i dostępności;
- Poufności, integralności;
- Uniemożliwieniem niewłaściwego użycia;

Nadzór nad dokumentacją jest realizowany poprzez zapewnienie odpowiednich sposobów postępowania oraz uprawnień i odpowiedzialności obejmujących:

- Opracowywanie, aktualizowanie i zatwierdzanie;
- Dystrybucję, dostęp, wyszukiwanie i wykorzystywanie;
- Przechowywanie i zabezpieczanie;
- Nadzorowanie zmian;
- Archiwizację lub likwidację;

6.2.1. Przegląd i zatwierdzanie dokumentacji bezpieczeństwa.

- PBI podlega zatwierdzeniu w momencie jej ustanowienia i kolejnym zatwierdzeniom po każdej aktualizacji;
- Dokumentację bezpieczeństwa zatwierdza Rektor ASP
- PBI po zatwierdzeniu wprowadzane jest zarządzeniem Rektora do obiegu aktów prawnych obowiązujących w ASP;
- Dokumentacja bezpieczeństwa podlega okresowemu przeglądowi, który powinien być przeprowadzony przynajmniej raz w roku i w razie stwierdzenia potrzeby aktualizacji powinna zostać zaktualizowana;
- Odpowiedzialny za okresowe przeglądy PBI jest Pełnomocnik ds. Cyberbezpieczeństwa;
- Dokumentacja bezpieczeństwa podlega przeglądowi i aktualizacji każdorazowo w związku z wdrażanymi nowymi funkcjonalnościami systemu informacyjnego;
- Dla użytkownika dostępna jest tylko aktualna wersja PBI;

6.2.2. Dystrybucja, udostępnianie, pobieranie i wykorzystanie.

- O adresatach dokumentacji bezpieczeństwa oraz zakresie udostępnianej dokumentacji decyduje Rektor ASP;
- Rektor może zapoznać użytkownika tylko z częścią dokumentacji;
- PBI może funkcjonować w wersji elektronicznej dostępnej dla Pracowników – strona internetowa ASP;
- Bez zgody Rektora ASP zabrania się powielania, udostępniania dokumentacji osobom nieupoważnionym;

- Na potrzeby użytkownika za zgodą Rektora/Kanclerza ASP można sporządzić wyciąg z PBI;

6.2.3. Przechowywanie i zabezpieczenie PBI.

- Dokumentacja przechowywana jest w zamykanej na klucz szafie biurowej. Dostęp do pomieszczenia, w którym przechowywana jest dokumentacja ma tylko upoważniony personel Działu IT;
- Dostęp do dokumentacji może mieć tylko upoważniony użytkownik;
- Dokumentacja w wersji elektronicznej podlega takiej samej ochronie jak dane przetwarzane przez system (kopia zapasowa, kontrola dostępu, ochrona antywirusowa, uprawnienia użytkownika);

6.2.4. Nadzorowanie zmian PBI.

- Wszelkie zmiany w dokumentacji bezpieczeństwa są nadzorowane dla zapewnienia jej integralności i rozliczalności;
- Za nadzór nad zmianami dokumentacji odpowiedzialny jest Pełnomocnik ds. Cyberbezpieczeństwa;
- Zmiany dokumentacji PBI dokonywane są w formalnym procesie zarządzania zmianą i wymagają każdorazowej akceptacji Rektora;

6.2.5. Archiwizacja i likwidacja PBI.

- W ASP przechowuje się dokumentację dotyczącą PBI systemu informacyjnego przez co najmniej 2 lata od dnia jej wycofania z użytkowania z uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164 t.j.);

7. Kontekst wewnętrzny i zewnętrzny Akademii Sztuk Pięknych we Wrocławiu (Kontekst organizacji).

7.1. Kontekst wewnętrzny.

W procesie identyfikacji czynników wewnętrznych uwzględniono:

- Strukturę i rozmiar jednostki (Szczegółowy opis w Zarządzaniu Ryzykiem);
- Informacje dotyczące liczby osób korzystających z usług ASP (Szczegółowy opis w Zarządzaniu Ryzykiem);
- Informacje dotyczące regulacji wewnętrznych i norm (Szczegółowy opis w Zarządzaniu Ryzykiem);
- System teleinformatyczny ASP:
- W ASP funkcjonuje centralna serwerownia zlokalizowana na terenie budynków ASP, w których umieszczone są urządzenia serwerowe niezbędne do pracy systemów teleinformatycznych.

- W systemie teleinformatycznym ASP wykorzystywana jest wirtualizacja serwerów obsługujących stacje robocze.
- Na stacjach roboczych zainstalowany jest system operacyjny Windows.
- W sieci teleinformatycznej ASP funkcjonują dodatkowo inne systemy informatyczne.

7.2. Kontekst zewnętrzny.

W procesie identyfikacji czynników zewnętrznych uwzględniono:

- Informacje dotyczące regulacji prawnych (Szczegółowy opis w Zarządzaniu Ryzykiem);
- Informacje dotyczące korzystania z usług podmiotów zewnętrznych (Szczegółowy opis w Zarządzaniu Ryzykiem);
- Informacje dotyczące statusu ASP;
- Zadania i obowiązki:
  - Prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
  - Wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym:
    - utrzymanie i bezpieczną eksploatację systemu informacyjnego,
    - bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
    - wdrażanie, dokumentowanie i utrzymywanie planów umożliwiających ciągłe i niezakłócone działania oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
    - objęcie systemu informacyjnego systemem monitorowania w trybie ciągłym;
  - Zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego;
  - Zarządzanie incydentami;
  - Stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego, w tym:
    - stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym.
    - dbałość o aktualizację oprogramowania.
    - ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym.
    - niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa.

8. Przywództwo.

8.1. Kierownictwo i jego zaangażowanie.

Najwyższe kierownictwo oświadcza, że będzie dbało o zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzania informacji w systemie informacyjnym niezbędnym do realizacji zadań w oparciu o obowiązujące przepisy prawa, odpowiednie normy, jak również w oparciu o dobre praktyki z dziedziny bezpieczeństwa informacji.

Najwyższe kierownictwo jest świadome negatywnego wpływu zagrożeń bezpieczeństwa informacji na prawidłowe funkcjonowanie zadań realizowanych przez ASP. Zobowiązuje się do kompleksowego wspierania procesów dotyczących rozwiązywania problemów bezpieczeństwa między innymi poprzez:

- Wyznaczenie osób odpowiedzialnych za optymalny podział i koordynację zadań związanych z zapewnieniem bezpieczeństwa informacji (Pełnomocnik ds. Cyberbezpieczeństwa);
- Wyznaczenie właścicieli dla kluczowych aktywów informacyjnych, którzy zobowiązani są do zapewnienia im wysokiego poziomu bezpieczeństwa.
- Przyjęcie do stosowania polityk i procedur bezpieczeństwa systemu informacyjnego przez wszystkich pracowników, współpracowników i kontrahentów zaangażowanych w proces rozwoju i utrzymania systemu informacyjnego jak również przez podmioty współpracujące;
- Przyjęcie do stosowania polityk i procedur bezpieczeństwa systemu informacyjnego przez wszystkich użytkowników systemu;
- Określenie procedur i zasad przetwarzania informacji, w tym stref i środowiska fizycznego;
- Regularne przeglądy i aktualizacje polityk i procedur, w celu jak najlepszej reakcji na zagrożenia i incydenty;
- Sprawowanie nadzoru i przestrzeganie zapisów PBI;
- Zobowiązanie wszystkich **użytkowników** systemu do zastosowania wytycznych normy PN-ISO/IEC 27001 we wszystkich procesach związanych z bezpieczeństwem informacji i na każdym etapie funkcjonowania systemu, aż do wycofania;
- Ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji funkcjonującego w ASP zgodnie z ustanowioną polityką bezpieczeństwa oraz dobrymi praktykami i zaleceniami pokontrolnymi;
- Wsparcie finansowe celów związanych z ciągłym doskonaleniem stosowanych środków i technologii bezpieczeństwa jak również kształcenia i rozwoju specjalistycznej kadry realizującej zadania związane z zapewnieniem bezpieczeństwa systemu;
- Pomoc i gotowość do stałej współpracy z Pełnomocnikiem ds. Cyberbezpieczeństwa w zakresie realizacji PBI, oraz ciągłego doskonalenia poziomu bezpieczeństwa systemu przyczyniającego się do niezakłóconego świadczenia usług;

8.2. Polityka bezpieczeństwa informacji (Deklaracja Kierownictwa).

Celem Systemu Zarządzania Bezpieczeństwem Informacji jest zapewnienie jak najwyższego poziomu bezpieczeństwa informacji przetwarzanych w systemie informacyjnym poprzez ustanowienie odpowiednich zasad, procesów, polityk i procedur zarządzania i postępowania. Bezpieczeństwo informacji ma na celu zachowanie takich właściwości przetwarzanych informacji, jak:

- **Poufność**;
- **Integralność**;
- **Dostępność**;

Przy zachowaniu dodatkowych atrybutów bezpieczeństwa informacji:

- **Rozliczalność;**
- **Autentyczność**;
- **Niezawodność;**

Bezpieczeństwo informacji realizowane jest:

- We wszystkich procesach cyklu życia systemu w zakresie:
  - Planowania.
  - Projektowania i wytwarzania.
  - Eksploatacji i rozwoju.
  - Wycofania z użytkowania.
- W obszarach, w zakresie:
- Organizacyjnym.
  - Technicznym i technologicznym.
  - Osobowym.
  - Fizycznym.

Postanowienia **SZBI** realizowane są przez wszystkich uczestników systemu informacyjnego. **Rektor** zapewnia, że **SZBI** jest zgodna z wymaganiami PN-ISO/IEC 27001 i wyraża **zobowiązanie**, że planowanie, wdrożenie, utrzymywanie i ciągłe doskonalenie zasad, procesów, polityk i procedur zarządzania i postępowania będzie realizowane zgodnie z wymaganiami określonymi w normie PN-ISO/IEC 27001.

9. Planowanie.

9.1. Zarządzanie ryzykiem.

W ASP opracowano i wdrożony zostanie system zarządzania ryzykiem oparty o normę PN-ISO/IEC 27005:2014.

Proces zarządzania ryzykiem opisany jest w dokumencie **Zarządzanie Ryzykiem** stanowiącym integralną cześć SZBI, który uwzględnia szacowanie i analizę ryzyka w obszarze ochrony danych osobowych zgodną z Rozdziałem XII Szacownie i analiza ryzyka Polityki Ochrony Danych Osobowych.

- Zarządzanie ryzykiem w ASP jest procesem ciągłym i obejmuje:
- Ustanowienie kryteriów szacowania ryzyka związanych z utratą poufności, integralności oraz dostępności informacji;
- Zapewnienie spójnych i porównywalnych wyników w kolejnej iteracji analizy ryzyka.
- Zidentyfikowanie kluczowych aktywów i osób za nie odpowiedzialnych;
- Określenie zagrożeń dla zidentyfikowanych aktywów;
- Rzeczywiste oszacowanie poziomu prawdopodobieństwa wystąpienia określonego zdarzenia dla bezpieczeństwa informacji;
- Określenie poziomu ryzyka;
- Przygotowanie Planu postępowania z ryzykiem obejmujący:
  - Wybór odpowiedniej opcji postępowania z ryzykiem.
  - Określenie wszystkich zabezpieczeń niezbędnych do wdrożenia wybranego sposobu postępowania z ryzykiem.
  - Uzyskanie zgody właścicieli ryzyka na wdrożenie planu postepowania z ryzykiem.

10. Wsparcie.

10.1. Zasoby.

Rektor zapewnia niezbędne zasoby:

- Osobowe;
- Finansowe;
- Lokalowe;

dla ustanowienia i realizacji wdrożenia, utrzymywania i ciągłego doskonalenia postanowień niniejszej polityki.

10.2. Kompetencje.

Rektor ASP zapewnia odpowiednie kompetencje w zakresie bezpieczeństwa informacji w systemie informacyjnym niezbędnym do niezakłóconej realizacji usług oraz związanych z ustanowieniem, wdrożeniem, utrzymywaniem i ciągłym doskonaleniem rozwiązań organizacyjnych i technicznych bezpieczeństwa informacji ustanowionych niniejszą polityką. Niezbędne kompetencje dotyczą wymagań prawnych, organizacyjnych, technicznych i technologicznych, osobowych i fizycznych bezpieczeństwa.

10.3. Uświadamianie (proces).

Rektor ASP zapewnia dostęp do wiedzy w zakresie bezpieczeństwa informacji każdemu uczestnikowi systemu informacyjnego (pracownik, współpracownik, zleceniobiorca, i podwykonawca) zaangażowanemu w realizację jakiejkolwiek funkcji związanej z ustanowieniem, wdrożeniem, utrzymywaniem i ciągłym doskonaleniem rozwiązań organizacyjnych i technicznych bezpieczeństwa ustanowionych niniejszą polityką dla zapewnienia wysokiego poziomu bezpieczeństwa informacji we wszystkich aspektach systemu.
Proces szkoleń zapewnia świadomość w zakresie postanowień i rozwiązań niniejszej polityki. Ponadto musi być realizowany cyklicznie, **co najmniej raz do roku** lub każdorazowo po wprowadzeniu zmian w SZBI.

10.4. Komunikacja.

Proces komunikacji jest prowadzony na poziomie zarządczym i wykonawczym. **Rektor** odpowiada za jego prawidłowy przebieg oraz skuteczność. w zakresie bezpieczeństwa informacji proces ten obejmuje komunikację pomiędzy **uczestnikami systemu informacyjnego** we wszystkich aspektach dotyczących bezpieczeństwa informacji.

Komunikacja prowadzona na poziomie zarządczym obejmuje wszelkiego rodzaju raporty, analizy, plany i decyzje zaadresowane w procesach i procedurach zarządzania bezpieczeństwem informacji niniejszej polityki.

Komunikacja prowadzona na poziomie wykonawczym (operacyjnym) realizowana jest przez wszystkich **uczestników systemu** i dotyczy wszelkich bieżących, operacyjnych aspektów bezpieczeństwa informacji systemu niezbędnego przy realizacji usług kluczowych.

Proces komunikacji obejmuje wszelkie kwestie dotyczące:

- Obowiązującej Polityki Bezpieczeństwa Informacji, jej celu oraz zakresu;
- Obowiązujących rozwiązań organizacyjnych i technicznych bezpieczeństwa - polityk szczegółowych i procedur dotyczących bezpieczeństwa informacji i systemu oraz ich zmian;
- Obowiązujących wymagań dotyczących bezpieczeństwa informacji i systemu, wymagań prawnych wobec systemu, wymagań technicznych i operacyjnych dla systemu informacyjnego niezbędnego do realizacji usług;
- Zakresu działania użytkowników i ich odpowiedzialności w zakresie bezpieczeństwa;
- Wyników szacowania ryzyka, planów postępowania z ryzykiem i stopnia ich realizacji;
- Stanu bezpieczeństwa systemu:
  - Stopnia spełniania wymagań dotyczących bezpieczeństwa.
  - Stopnia realizacji i skuteczności rozwiązań organizacyjnych i technicznych bezpieczeństwa oraz podejmowanych działań z tym związanych.
- Wyników audytów wewnętrznych i realizacji zaleceń;
- Wszelkich odstępstw, niezgodności, incydentów i prób naruszenia bezpieczeństwa, i podejmowanych w związku z tym działań;
- Planowanych, projektowanych i realizowanych zmian, przebudowy i rozbudowy systemu informacyjnego i ich wpływu na bezpieczeństwo danych i systemu oraz niezakłócone realizowanie usług kluczowych przez ASP;
- Innych informacji uznanych za ważne dla bezpieczeństwa informacji i systemu oraz bezpieczeństwa usług kluczowych;

10.5. Udokumentowane informacje.

Rektor zapewnia właściwy nadzór nad niniejszą Polityką Bezpieczeństwa Informacji, wraz z powiązanymi z nią dokumentami, stanowiącymi dokumentację bezpieczeństwa informacji, która obejmuje trzy dokumenty:

- Politykę Bezpieczeństwa Informacji (niniejszy dokument), oraz:
- Zarządzanie Ryzykiem;
- Politykę Ochrony Danych Osobowych;

oraz wszelkie zapisy związane z bezpieczeństwem informacji dostępne w Dziale IT, u Pełnomocnika ds. Cyberbezpieczeństwa oraz u Inspektora Ochrony Danych.

Dokumentacja bezpieczeństwa informacji podlega nadzorowi w celu zapewnienia:

- Przydatności i adekwatności;
- Użyteczności i dostępności;
- Poufności, integralności i przeciwdziałaniu przed niewłaściwym użyciem;

Nadzór nad dokumentacją bezpieczeństwa informacji jest realizowany poprzez zapewnienie odpowiednich dla charakteru systemu informacyjnego sposobów realizacji uprawnień i odpowiedzialności obejmujących:

- Opracowywanie, aktualizowanie i zatwierdzanie;
- Dystrybucję, dostęp, wyszukiwanie i wykorzystywanie;
- Przechowywanie i zabezpieczanie;
- Nadzorowanie zmian;

11. Działania operacyjne (wykonawcze).

Polityka bezpieczeństwa dla systemu informacyjnego niezbędnego do zapewnienia realizacji usług kluczowych przez ASP zostaje wprowadzona przez **Rektora** w formie zarządzenia. Wszyscy **użytkownicy systemu** są zobowiązani do przestrzegania zasad w niej zawartych.

11.1. Planowanie i nadzór nad działaniami wykonawczymi.

Zapewnienie bezpieczeństwa informacji systemu informacyjnego związanego z realizacją przez ASP usług wiąże się z koniecznością wdrożenia wszystkich zapisów niniejszej polityki, przy jednoczesnym monitorowaniu i nadzorowaniu ich realizacji przez **użytkowników systemu**.

Rektor zleca Pełnomocnikowi ds. Cyberbezpieczeństwa cykliczne przeprowadzanie przeglądów zapisów PBI, nie rzadziej **niż 1 raz w roku**, w celu oceny ich przydatności oraz skuteczności w działaniu.

Pełnomocnik konsultuje zapisy PBI z:

- Kanclerzem;
- Administratorem Systemów Informatycznych;
- Inspektorem Ochrony Danych;

11.2. Zarządzanie ryzykiem.

Rektor zobowiązał Pełnomocnika ds. Cyberbezpieczeństwa do systematycznego szacowania ryzyka w zakresie bezpieczeństwa informacji. Ustalono, że proces szacowania ryzyka będzie się odbywał nie rzadziej **niż 1 raz na dwa lata**. Przyjęto także jako obowiązkowe, szacowanie ryzyka w sytuacji istotnych zmian w systemie, mogących mieć wpływ na poziom bezpieczeństwa informacji oraz w przypadku wystąpienia incydentu bezpieczeństwa. Ocena ryzyka wskazuje także plany postępowania z ryzykiem stanowiące podstawę do dalszych czynności związanych z obsługą ryzyka. Zidentyfikowane oraz zaakceptowane ryzyka udokumentowane są w rejestrze ryzyka, a ponadto bez zbędnej zwłoki przekazane **Rektorowi w** formie Sprawozdania. Szczegółowo zasady zarządzania ryzykiem, rejestr ryzyka oraz plan postępowania z ryzykiem zostały opisane w dokumencie **Zarządzanie Ryzykiem.**

12. Monitorowanie, pomiary, analiza i ocena (Ocena wyników).

Ocena skuteczności wdrożonej polityki bezpieczeństwa dla systemu informacyjnego niezbędnego do zapewnienia realizacji usług przez ASP jest kluczowym elementem systemu zarządzania bezpieczeństwem informacji. Ocena dokonywana jest cyklicznie, podczas przeglądu zarządzania, gdzie analizowane są takie elementy jak:

- Wyniki audytów systemu, podczas których weryfikowane są:
  - Skuteczność wdrożonych zabezpieczeń opisanych w PBI.
  - Zgodność z przepisami prawa.
  - Poziom świadomości i kompetencji.
- Jakość i celowość prezentowanych w PBI zabezpieczeń;
- Proces zarządzania incydentami bezpieczeństwa, które dotyczą systemu;
- Stopień realizacji celów bezpieczeństwa informacji;
- Realizacja działań korygujących;

Procesy monitorowania, pomiaru, analizy i oceny na poziomie wykonawczym realizowane są przez **Pełnomocnika ds. Cyberbezpieczeństwa** w trybie ciągłym dla zapewnienia aktualnych informacji, niezbędnych do właściwej oceny sytuacji, podejmowania właściwych decyzji i działań odnośnie funkcjonowania systemu. Bieżące działania w tym zakresie to między innymi analiza incydentów, ocena skuteczności obsługi incydentów bezpieczeństwa, analiza niezgodności realizacji rozwiązań organizacyjnych i technicznych bezpieczeństwa, dokonywania ich usprawnień czy też analiza odstępstw. Wyniki monitorowania, pomiaru, analizy i oceny podlegają formalnemu udokumentowaniu.

Pełnomocnik ds. Cyberbezpieczeństwa konsultuje w/w procesy z Inspektorem Ochrony Danych oraz Administratorem Systemów Informatycznych jak również z audytorem wewnętrznym.

Rektor ma obowiązek zapewnić przeprowadzenie, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego.

12.1. Audyt wewnętrzny SZBI.

Audyt wewnętrzny SZBI służy potwierdzeniu zgodności systemu ASP z wymaganiami dotyczącymi bezpieczeństwa informacji, zarówno w kontekście przepisów prawa (Ustawa o KSC, RODO) jak i innych regulacji normatywnych czy wewnętrznych. Jest mechanizmem niezależnej oceny, weryfikującym poziom świadomości i kompetencji użytkowników systemu.

Rektor jest odpowiedzialny za zapewnienie przeprowadzania audytu wewnętrznego, zapewnienie jego niezależności i bezstronności, obiektywności i niezbędnych do jego realizacji zasobów.

Wyniki audytu wewnętrznego w zakresie bezpieczeństwa informacji systemu informacyjnego przekazywane są Pełnomocnikowi ds. Cyberbezpieczeństwa oraz Inspektorowi Ochrony Danych.

Audyt wewnętrzny jest procesem systematycznym - cyklicznie powtarzalnym, który musi być przeprowadzony, co najmniej **raz na dwa lata.**

Dokumentacja dotycząca procesu audytu wewnętrznego musi zawierać co najmniej:

- Harmonogram audytów, z tematami poszczególnych audytów;
- Plany szczegółowe poszczególnych audytów;
- Raporty z audytów;
- Rejestr niezgodności;
- Zalecenia, które mają charakter wiążący dla Rektora ASP;

12.2. Przegląd zarządzania.

Rektor zapewnia realizację przeglądów zarządzania bezpieczeństwem informacji. Przegląd ma na celu zapewnienie stałej przydatności, adekwatności i skuteczności Polityki Bezpieczeństwa Informacji w zakresie zapewnienia jak najwyższego poziomu bezpieczeństwa informacji całości systemu teleinformatycznego eksploatowanego w ASP.

Przegląd zarządzania jest działaniem zarządczym, cyklicznym, polegającym na zebraniu danych dotyczących stanu i poziomu bezpieczeństwa informacji w systemie oraz skuteczności ustanowionych i wdrożonych rozwiązań organizacyjnych i technicznych bezpieczeństwa, ocenie na ich podstawie luk, podatności i zagrożeń oraz niezgodności. Dane podlegające ocenie mogą także pochodzić od **podmiotów zewnętrznych** realizujących zadania na rzecz ASP związane z systemem informatycznym.

Przegląd zarządzania bezpieczeństwem informacji realizowany jest przez **Pełnomocnika ds. Cyberbezpieczeństwa** regularnie przynajmniej **1 raz w roku**, w pierwszym kwartale danego roku.

W przeglądzie bezpieczeństwa informacji biorą udział:

- Kanclerz – nadzoruje proces;
- Pełnomocnik ds. Cyberbezpieczeństwa;
- Inspektor Ochrony Danych;
- Kierownicy komórek organizacyjnych ASP;

Przegląd zarządzania bezpieczeństwem informacji powinien uwzględniać oraz poddać analizie i ocenie, co najmniej następujące dane:

- Czynniki zewnętrzne i wewnętrzne (kontekst ASP) istotne dla systemu zarządzania;
- Stan działań podjętych w następstwie wcześniejszych przeglądów zarządzania bezpieczeństwem;
- Stopień osiągnięcia ustalonego poziomu bezpieczeństwa systemu;
- Skuteczność funkcjonowania procesów określonych niniejsza polityką;
- Występowanie, skalę, zakres oddziaływania i skutki incydentów bezpieczeństwa i niezgodności realizacji rozwiązań organizacyjnych i technicznych systemu zarządzania bezpieczeństwem;
- Stopień i poziom wdrożenia i realizacji rozwiązań organizacyjnych i technicznych systemu bezpieczeństwa systemu oraz potrzeby ich aktualizacji;
- Wyniki audytów bezpieczeństwa i stopień realizacji zaleceń autowych;
- Informacje dotyczące zarządzania incydentami bezpieczeństwa systemu informatycznego;
- Wyniki szacowania ryzyka i stopień realizacji decyzji, co do postępowania z ryzykiem (realizacja planu postepowania z ryzykiem);
- Informacje dotyczące funkcjonowania sytemu pochodzące od użytkowników;
- Informacje od podmiotów zewnętrznych (dostawców usług związanych z systemem informatycznym ASP);

Na podstawie wyników przeglądu zarządzania Pełnomocnik ds. Cyberbezpieczeństwa przygotowuje Raport zawierający wnioski i zalecenia do zatwierdzenia przez Rektora. Zalecenia mogą dotyczyć:

- Zmian lub zwiększenia skuteczności rozwiązań organizacyjnych i technicznych znajdujących się w zakresie polityki bezpieczeństwa informacji;
- Zapewnienia adekwatnych do poziomu ryzyka zasobów osobowych i technicznych;
- Doskonalenia skuteczności systemu zarządzania bezpieczeństwem informacji ustanowionego niniejszą polityką;

Zalecenia oraz wszelkie decyzje podjęte podczas przeglądu zarządzania powinny być bez zbędnej zwłoki wdrożone w obszarze, którego dotyczą.

13. Doskonalenie.

Rektor deklaruje dołożenia wszelkich starań mających na celu zapewnienie bezpieczeństwa informacji poprzez ciągłe doskonalenie między innymi w zakresie:

- Polityki bezpieczeństwa informacji;
- Optymalizacji procesów bezpieczeństwa informacji w systemie informatycznym ASP;
- Zabezpieczenie odpowiednich środków finansowych i osobowych;

13.1. Niezgodności i działania korygujące.

Zapewnienie właściwego nadzorowania i obsługi niezgodności oraz wdrażania odpowiednich działań korygujących jest kluczowe dla zapewnienia wysokiego poziomu bezpieczeństwa systemu informacyjnego. **Rektor** odpowiada za właściwe i efektywne nadzorowanie, obsługę niezgodności (w tym incydentów) oraz działań korygujących w obszarze całego systemu. W imieniu Rektora działa Pełnomocnik ds. Cyberbezpieczeństwa.

13.1.1. Nadzorowanie niezgodności.

Powstanie niezgodności może być spowodowane działaniem lub rozwiązaniem technicznym w zakresie rozwoju, wykonania, wdrożenia i eksploatacji lub utrzymania systemu informatycznego eksploatowanego ASP, które nie jest zgodne z postanowieniami ustanowionej Polityki Bezpieczeństwa Informacji.

Proces nadzorowania niezgodności zwiększa bezpieczeństwo informacji przez:

- Identyfikację niezgodności ich charakteru, zakresu, sposobu i zasięgu oddziaływania oraz wywoływanych skutków;
- Podejmowanie właściwych działań zabezpieczających sytuację czy stan techniczny, zapobiegających działaniu w niewłaściwy, niezgodny z polityką bezpieczeństwa informacji działaniami lub wykorzystywaniu, stosowaniu niewłaściwych, niezgodnych z nią rozwiązań technicznych;
- Modyfikację stanu organizacyjnego i technicznego niezgodnego ze stanem właściwym, określonym w polityce bezpieczeństwa informacji oraz dokumentacji technicznej systemu, skorygowanie niezgodnego zabezpieczenia;
- Zapobieganie wykonywaniu nieuzasadnionych zmian technicznych w systemie oraz zmian sposobu realizacji zadań i procesów rozwoju, eksploatacji lub utrzymania systemu;
- Monitorowanie i zarządzanie następstwami niezgodności;
- Poinformowanie właściwej komórki ds. bezpieczeństwa w jednostkach interesariuszy, stosownie do posiadanego zakresu uprawnień i kompetencji;
- Poinformowanie kierowników komórek organizacyjnych ASP o podjętych działaniach korygujących;

Każda niezgodność musi być każdorazowo dokumentowana, z zapewnieniem pełnej rozliczalności w dokumencie **„Rejestr niezgodności”** (poniżej wzór dokumentu), prowadzonym najlepiej w wersji elektronicznej. Dopuszczalny jest również rejestr w formie papierowej. Wszystkie działania i decyzje, w tym zgłoszenie i rejestracja, analiza i kwalifikacja niezgodności, działania zabezpieczenia i monitorowania oraz decyzje co do podejmowanych działań usuwania stanu niezgodnego muszą być zaewidencjonowane w Rejestrze niezgodności prowadzonym przez Pełnomocnika ds. Cyberbezpieczeństwa.

Wzór Rejestru niezgodności:

	PBI
	Rejestr niezgodności
Sporządził:	Pełnomocnik ds. Cyberbezpieczeństwa
Zatwierdził:	Rektor

Lp.	Osoba ujawniająca niezgodność	Data:	Opis niezgodności	Identyfikator niezgodności	Wymagania
1	Jan Kowalski (Dział IT)	10.10.20xx r	Brak poprawnego oznaczenia kopii zapasowej, brak informacji z jakiego okresu jest kopia danych.	1/10.10.20xx	Pkt. a 12.3.1 (ISO 27001 załącznik A)

13.1.2. Nadzorowanie incydentów (zarządzanie incydentami).

Celem procedury jest określenie zakresu oraz odpowiedzialności w procesie zarządzania incydentami bezpieczeństwa informacji dla systemu informacyjnego niezbędnego w celu niezakłóconej realizacji usług przez ASP.

Procedura zapewnia efektywną obsługę incydentów bezpieczeństwa teleinformatycznego w ASP, w tym:

- Skuteczne i szybkie reagowanie na wystąpienie incydentów (w tym incydentów poważnych wymagających zgłoszenia w ciągu 24 godzin do CSIRT NASK), a przez to możliwie największego ograniczenia ich skutków;
- Gromadzenie materiałów analitycznych dających największą szansę na ustalenie przyczyny incydentu;
- Poprawne gromadzenie materiałów dowodowych mogących służyć w ew. sprawach sądowych lub dyscyplinarnych;
- Analizę historii incydentów i wdrażania działań korygujących;

Procedura określa zasady:

- Zgłaszania i rejestrowania incydentów bezpieczeństwa przez użytkownika;
- Zgłaszania incydentu poważnego do CSIRT NASK;
- Obsługi incydentu poważnego;
- Analizy przyczyn incydentów i gromadzenia materiałów dowodowych;
- Okresowych przeglądów, w celu wdrażania działań naprawczych;
- Zgłaszania incydentów związanych z ochroną danych osobowych;

W procesie zarządzania incydentami biorą udział wszyscy użytkownicy systemu. Incydentem bezpieczeństwa jest zdarzenie mające wpływ na jedno bądź wiele atrybutów informacji:

- Integralność;
- Dostępność;
- Poufność;
- Autentyczność;
- Rozliczalność;
- Niezaprzeczalność;
- Niezawodność;

Przykładowe zdarzenia, które powinny być traktowane, jako incydent bezpieczeństwa informacji:

- Utrata usługi, urządzenia lub funkcjonalności (brak możliwości realizowania usług przez ASP);
- Nieprawidłowe działanie systemów, aplikacji;
- Niezgodność z politykami, instrukcjami lub zaleceniami opisanymi w PBI;
- Naruszenie zasad związanych z bezpieczeństwem fizycznym systemu informatycznego;
- Niekontrolowane zmiany w systemie IT;
- Niepoprawne działanie oprogramowania lub sprzętu;
- Naruszenie dostępu do systemów informatycznych;

Zgłaszanie i rejestrowanie incydentu bezpieczeństwa.

Pełnomocnik ds. Cyberbezpieczeństwa po wykryciu i uznaniu incydentu za poważny ma 24 godziny na przesłanie do CSIRT NASK zgłoszenia zawierającego:

- Dane podmiotu zgłaszającego (nazwa i adres);
- Imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia;
- Imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
- Opis wpływu incydentu poważnego, w tym:
  - Usługi zgłaszającego, na które incydent poważny miał wpływ.
  - Liczbę użytkowników usługi, na których incydent poważny miał wpływ.
  - Moment wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania.
  - Zasięg geograficzny obszaru, którego dotyczy incydent poważny.
  - Przyczynę zaistnienia incydentu poważnego i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne lub świadczone usługi.
- Informacje umożliwiające, CSIRT NASK na określenie czy incydent dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej;
- W przypadku incydentu, który mógł mieć wpływ na świadczenie usług, opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne;
- Informacje o podjętych działaniach zapobiegawczych;
- Informacje o podjętych działaniach naprawczych;

- Inne istotne informacje;

Pełnomocnik ds. Cyberbezpieczeństwa dokonuje zgłoszenia do CSIRT NASK za pośrednictwem strony internetowej www.nask.pl zakładka DZIAŁALNOŚC / CYBERBEZPIECZEŃSTWO / Obsługa zgłoszeń.

Każdy użytkownik systemu teleinformatycznego jest zobowiązany do zgłaszania każdego przypadku naruszenia bezpieczeństwa informacji.
Informacje o zgłoszeniu przekazywane są:

- Telefonicznie :
  - W godzinach pracy Działu IT – 71 302 58 04 wew.104
  - Po godzinach pracy i w dni wolne – 571084888
- Za pośrednictwem poczty elektronicznej: abi@asp.wroc.pl

Pełnomocnik ds. Cyberbezpieczeństwa dokonuje analizy zgłoszenia. w przypadku uznania incydentu za incydent bezpieczeństwa informacji w systemie informatycznym ASP obsługę incydentu realizuje Dział IT.

Pełnomocnik ds. Cyberbezpieczeństwa prowadzi Rejestr incydentów. Rejestr zawiera informacje:

- Zgłaszający incydent (Użytkownik systemu, administrator, itd.);
- Data i godzina zgłoszenia incydentu;
- System / element, którego dotyczy incydent (w tym także incydenty dotyczące ochrony fizycznej);
- Opis incydentu;
- Wpływ incydentu na bezpieczeństwo informacji całego systemu;
- Podjęte działania korygujące;
- Przyczyna wystąpienia incydentu;
- Podjęte działania zmniejszające prawdopodobieństwo ponownego wystąpienia incydentu;

Raz w miesiącu **Pełnomocnik ds. Cyberbezpieczeństwa** odpowiedzialny jest za dokonanie i udokumentowanie analizy zebranych zdarzeń dotyczących bezpieczeństwa systemów eksploatowanych w ASP. Analiza w szczególności polega na zbadaniu informacji:

- Czy podobne incydenty występowały już wcześniej;
- Czy incydent dotyczył realizacji usługi;
- Czy zdarzenie miało charakter cyberterroryzmu;
- Czy obsługa incydentu przebiegała prawidłowo;
- Czy incydent dotyczył ochrony danych osobowych;

W przypadku incydentu dotyczącego **ochrony danych osobowych** realizowane są procedury opisane w **Polityce bezpieczeństwa danych osobowych – Rozdział IX Procedura naruszenia danych osobowych, załącznik nr 12 - Procedura notyfikacji naruszeń danych osobowych.**

13.1.3. Nadzorowanie działań korygujących.

Działania korygujące to działania mające na celu eliminację przyczyn niezgodności. Działania korygujące zwiększają odporność i zmniejszają podatności systemu na zagrożenia bezpieczeństwa informacji systemu eksploatowanego w ASP. Działania korygujące wprowadzane są pod nadzorem **Rektora,** lub upoważnionego przez niego pracownika, który jest odpowiedzialny za ich skuteczne wdrożenie.

W ramach działań korygujących realizowany jest proces:

- Oceny zaistniałych odstępstw, niezgodności i incydentów;
- Identyfikacji ich przyczyn i eliminacji negatywnych skutków;
- Wdrożenia działań eliminujących te przyczyny i eliminujące możliwość wystąpienia negatywnych skutków, tak aby odstępstwa, niezgodności czy incydenty nie występowały ponownie;

Wdrażane działania korygujące powinny być dostosowane do skutków stwierdzonych niezgodności i incydentów bezpieczeństwa.

Po realizacji niezbędnych działań eliminujących przyczyny zdarzeń Rektor prowadzi przegląd i ocenę skuteczności ich wdrożenia oraz podejmuje stosowne decyzje w przypadku niewdrożenia lub nieskuteczności wdrożonych działań.

W przypadku niewdrożenia lub nieskuteczności rekomendowanych działań korygujących Rektor może podjąć decyzję o konsekwencjach dla osób odpowiedzialnych za ich wdrożenie.

Należy rozważyć również decyzję o ponownym wdrożeniu tych samych lub innych działań korygujących, aby zapewnić osiągnięcie celu realizacji działań korygujących.

W ramach realizacji działań korygujących mogą być wdrażane zmiany w rozwiązaniach organizacyjnych i technicznych bezpieczeństwa systemu, określone w niniejszej PBI.

Rektor może zlecić nadzór nad działaniami korygującymi Kanclerzowi.

Wzór Rejestru działań korygujących.

	PBI
	Rejestr działań korygujących
Sporządził:	Pełnomocnik ds. Cyberbezpieczeństwa
Zatwierdził:	Rektor

Lp.	Identyfikator niezgodności (z rejestru niezgodności)	Data ujawnienia	Opis działań korygujących	Data realizacji działań korygujących	Zatwierdził
1.	1/10.10.20xx	10.10.20xx	Wprowadzenie właściwych oznaczeń kopii zapasowych, inwentaryzacja posiadanych kopii, przetestowanie prawidłowości kopii danych.	01.11.20xx	Rektor

13.2. Ciągłe doskonalenie.

Polityka Bezpieczeństwa Informacji i ustanowione jej postanowieniami rozwiązania organizacyjne i techniczne podlegają ciągłemu doskonaleniu w odniesieniu do jej przydatności, adekwatności i skuteczności w osiąganiu i zapewnianiu wysokiego poziomu bezpieczeństwa systemu niezbędnego do realizacji usług przez ASP

13.2.1. Zarządzanie zmianami.

Proces kontroli zmian obowiązuje we wszystkich obszarach, w których następują zmiany i zapewnia nadzór nad wszelkimi zmianami, modyfikacjami oraz wprowadza określone reguły w zakresie komunikacji oraz odpowiednią ścieżkę akceptacji przez Rektora.

Zmiany i modyfikacje w systemie powinny być wykonywane w sposób przemyślany i ograniczone do zmian koniecznych. Ponadto wszelkie zmiany powinny być ściśle nadzorowane.

Proces kontroli zmiany składa się z części związanej z weryfikacją wprowadzanych zmian. w tym miejscu dokonywana jest analiza formalna, jak również merytoryczna wprowadzanych zmian.
Po akceptacji procesu weryfikacji rozpoczyna się implementacja zmiany, poprzedzona zakomunikowaniem zakresu zmian oraz analizą wpływu.

Ostatnim, integralnym etapem procesu jest implementacja zmiany w zaplanowanym miejscu, jak również ocena (testy) zgodności efektów z oczekiwanymi skutkami zmiany. w zależności od oceny efektu wprowadzonej zmiany podejmowana jest decyzja o jej wycofaniu bądź akceptacji.

Niezbędnym elementem procesu zmiany jest dokumentowanie każdego etapu jego przeprowadzania, w celu zachowania niezbędnej wiedzy do ewentualnych kolejnych zmian jak również na potrzeby działań audytowo-kontrolnych.

- **Forma zgłoszenia** - powinna umożliwiać przechowywanie dokumentacji związanej ze zmianą oraz późniejszą archiwizacje z uwzględnieniem mechanizmu wersjonowania i identyfikacji;
- **Treść zgłoszenia** - zakres, cel i powód zmiany powinny być opisane w dokumentacji załączonej do zgłoszenia/wniosku o zmianę w sposób zrozumiały i napisany, umożliwiając jego łatwą analizę;
- **Dane formalne** - wniosek o zmianę powinien zawierać, co najmniej:
  - Dane osoby wnioskującej.
  - Potwierdzenie zgody na rozpoczęcie procesu zmiany.
  - Ocenę wpływu na inne obszary.
  - Opis implementacji zmiany.
  - Opis metod testowania poprawności zmiany (w tym testów wpływu na systemy ASP po wdrożeniu).
  - Dokumentację wdrożeniową/instrukcje.
  - Sposób nadzoru nad zmianą (monitorowania zmiany).
  - Procedury awaryjne (w tym procedurę wycofania zmiany).

Wzór formularza zmian.

	PBI
	Formularz zmian.

Tytuł procedury (opis) / element systemu IT / konfiguracja	
Wnioskujący	
Proponowana zmiana	
Uzasadnienie zmiany	
Data	
Analiza ryzyka	
Ocena merytoryczna (weryfikacja formalna i merytoryczna)	
Akceptacja (formalna i merytoryczna) zmiany (data i podpis)	
Implementacja zmiany (data, adresaci)	
Ocena zmiany	

13.2.2. Weryfikacja zmian.

Zaplanowana zmiana musi zostać zweryfikowana zarówno pod względem formalnym jak i merytorycznym, zgodnie z poniższymi zasadami.

- **Weryfikacja formalna** - weryfikacja formalna wprowadzonych danych, ich zgodności, kompletności i adekwatności, ocena dokonywana jest poprzez osoby upoważnione przez Rektora do weryfikacji formalnej – Kierownik komórki organizacyjnej;
- **Weryfikacja merytoryczna** - weryfikacja merytoryczna wprowadzonych danych, ocena merytoryczna zmiany uwzględniająca ocenę adekwatności, zakresu, ryzyka, istnienie przeprowadzana przez osoby upoważnione przez Rektora do weryfikacji merytorycznej – Pełnomocnik ds. Cyberbezpieczeństwa;
- **Ocena ryzyka** – podczas procesu weryfikacji powinna zostać dokonana analiza ryzyka związana z prowadzoną zmianą poprzez **Administratora Systemów Informatycznych** lub **Pełnomocnika ds. Cyberbezpieczeństwa;**

13.2.3. Akceptacja zmian.

W procesie zmiany bardzo istotną role ogrywa proces decyzyjny. Akceptacja musi zostać dokonana po właściwej ocenie, być wykonana przez uprawnione osoby, powinna odbywać zgodnie z poniższym opisem.

- **Akceptacja formalna -** akceptacja w zakresie formalnym wniosku i dokumentacji powinna być dokonana przez upoważnioną przez Rektora osobę;
- **Akceptacja merytoryczna -** akceptacja w zakresie merytorycznym powinna zostać dokonana przez upoważnioną przez Rektora osobę;
- **Przechowywanie dokumentacji** - miejsce przechowywania wniosków oraz dokumentacji powinno być jasno wskazane i zapewniać dostęp dla określonych uprawnionych osób, a po zakończeniu cyklu zmiany powinna zostać uaktualniona wszelka dokumentacja, na którą wpływ miała przeprowadzona zmiana;
  Dokumentacja zmian przechowywana jest u Pełnomocnika ds. Cyberbezpieczeństwa.
- **Niedopuszczalność pojedynczej akceptacji -** zmiany w obszarach systemu informatycznego ASP nie powinny być akceptowane przez pojedynczą osobę. Ograniczenie dotyczy sytuacji, gdy np. osoba występująca z wnioskiem o zmianę dokonuje jego jednocześnie jego akceptacji merytorycznej;
- **Niedopuszczalność łączenia ról** – rola Zgłaszającego nie powinna być łączona z rolami uprawnionymi do weryfikacji oraz akceptacji zmiany. Na przykład Administrator wnioskujący o zmianę nie może być jednocześnie weryfikującym i/lub akceptującym te zmianę;
- **Zmiany w trybie awaryjnym/pilnym** – obsługiwane w trybie pilnym, bez formularzy, zgłoszenie np. telefoniczne natomiast akceptacja np. SMS. Po dokonaniu zmiany w najbliższym możliwym terminie powinny być spełnione wymagane procedurą czynności;

13.2.4. Implementacja zmian.

Implementacja zmiany odbywa się zgodnie z wytycznymi opisanymi w formularzu lub dołączoną dokumentacją techniczną do systemu lub urządzenia. Konkretna procedura techniczna dotycząca wdrożenia (np. instalacji sprzętu) implementowanego w ramach niniejszej procedury zmiany, musi zostać opracowana, udokumentowana oraz bezwzględnie podlega weryfikacji i akceptacji uprawnionych osób. Należy pamiętać, że realizacja tego punktu zależy od zakresu zmiany, to znaczy na przykład zmiany dotyczące dokumentacji będą pojedynczą czynnością polegająca na zatwierdzeniu zmiany przez osoby upoważnione, w przypadku zaś zmian w oprogramowaniu, proces ten jest znacznie bardziej rozwinięty i implementacja zmiany w pierwszej kolejności zostanie wykonana na środowiskach nieprodukcyjnych (testowych) i dopiero po potwierdzeniu ich poprawności w działaniu zmiany te będą wdrożone na środowiskach produkcyjnych.

13.2.5. Weryfikacja poprawności zmian.

Po zakończeniu implementacji należy przeprowadzić ocenę poprawności działania.
W przypadku oprogramowania będą to testy oprogramowania (w tym testy integracyjne czy bezpieczeństwa).

Pozytywny wynik testów stanowi podstawę do rozpoczęcia eksploatacji przedmiotu zmiany, natomiast negatywny wynik może być podstawą do przeprowadzenie procedury cofnięcia zmiany, a nawet rezygnacji ze zmiany.

W przypadku zmian w oprogramowaniu, należy także dokonać oceny wpływu zmiany na działanie systemów operacyjnych.

13.2.6. Komunikacja.

Niezbędnym elementem poprawnego przebiegu procesu zarządzania zmianą jest komunikacja pomiędzy jego uczestnikami z uwzględnieniem poniższych wytycznych:

- **Powiadomienie uczestników podczas rozpoczęcia procesu -** Wszyscy uczestnicy, których zmiana może dotyczyć powinni zostać powiadomieni podczas rozpoczęcia procesu zmiany, z możliwością zgłoszenia uwag. Należy pamiętać o obligatoryjnej konieczności powiadomienia Inspektora Danych Osobowych. Powiadomienie jest realizowane przez osoby upoważnione przez **Rektora;**
- **Powiadomienie uczestników przed implementacją zmiany -** Wszyscy uczestnicy, których zmiana może dotyczyć powinni zostać powiadomieni przez rozpoczęciem implementacji zmiany. Należy pamiętać o obligatoryjnej konieczności powiadomienia Inspektora Danych Osobowych. Powiadomienie jest realizowane przez osobę upoważnioną przez **Rektora**;

13.2.7. Przeglądy i raporty zmian.

Proces zarzadzania zmiana podlega przeglądom oraz odpowiedniemu raportowaniu:

- **Przeglądy procedury** – procedura kontroli zmiany podlega cyklicznym przeglądom pod kątem adekwatności, aktualności i skuteczności, przeglądy wykonywane będą nie rzadziej niż raz w roku i realizowane przez osobę upoważnioną przez **Rektora**;
- **Raporty z działania** – raporty z zakresu działań wykonywanych w ramach procedury wykonywane będą nie później niż 30 dni po zakończeniu zmiany, realizowane przez osobę upoważnioną przez Rektora;

Rektor może przeprowadzić audyt weryfikujący przestrzeganie procedury zarządzania zmianami.

14. Obszary zabezpieczeń.

14.1. Polityka bezpieczeństwa informacji.

14.1.1. Kierunki bezpieczeństwa informacji określane przez Rektora.

- Rektor zleca opracowanie i nadzór nad dokumentacją bezpieczeństwa systemu informacyjnego niezbędnego w celu realizacji usług Pełnomocnikowi ds. Cyberbezpieczeństwa;
- Dokumentacja PBI jest zatwierdzana przez Rektora i wprowadzana zarządzeniem do obiegu aktów prawnych obowiązujących w ASP;
- Dokumentacja dostępna jest w wersji papierowej w pokoju Pełnomocnika ds. Cyberbezpieczeństwa oraz w wersji elektronicznej w sieci informatycznej ASP;
- Z dokumentacją bezpieczeństwa lub jej elementami należy zapoznać wszystkich uczestników systemu (pracownicy, wykładowcy, doktoranci, współpracownicy, praktykanci, stażyści);
- Każdorazowa zmiana (aktualizacja) dokumentacji jest zatwierdzana przez Rektora;
- Pełnomocnik ds. Cyberbezpieczeństwa dokonuje regularnych przeglądów PBI, przynajmniej jeden raz w roku lub w razie istotnych zmian systemowych;

14.2. Organizacja bezpieczeństwa informacji.

14.2.1. Organizacja wewnętrzna.

- W celu skutecznego nadzorowania systemu bezpieczeństwa informacji w ASP powołano Pełnomocnika ds. Cyberbezpieczeństwa oraz Zespół ds. SZBI;

- Obowiązki i odpowiedzialności osób odpowiedzialnych za bezpieczeństwo informacji pozostające w konflikcie muszą być rozdzielane w celu zredukowania ryzyka niewłaściwego umyślnego lub nieumyślnego użycia aktywów. w tym celu powołano w/w funkcje (role). w systemie zapewniona jest rozliczalność działań związanych z dostępem do aktywów, ich modyfikacji i korzystania. w celu redukcji ryzyka niewłaściwego użycia aktywów w systemie służą również dodatkowe zabezpieczenia w postaci monitorowania aktywności, analizy logów, nadzoru kierownictwa, audytów wewnętrznych i zewnętrznych;
- W zakresie bezpieczeństwa informacji są utrzymywane kontakty z organami władzy, a także z organami regulacyjnymi i normalizacyjnymi. Rektor wyznaczył

Pełnomocnika ds. Cyberbezpieczeństwa do kontaktów w ramach Krajowego Systemu Cyberbezpieczeństwa;

- Osoby odpowiedzialne za bezpieczeństwo informacji w systemie utrzymują kontakty ze specjalistami (ekspertami) jak również specjalistycznymi forami oraz stowarzyszeniami zawodowymi w celu bieżącego uzupełniania wiedzy, wymiany informacji o nowych technologiach, produktach, zagrożeniach i podatnościach;
- Bezpieczeństwo informacji jest uwzględniane w ramach zarządzania wszystkimi projektami realizowanymi w systemie. w szczególności cele bezpieczeństwa informacji są włączane do celów projektów, a samo bezpieczeństwo informacji jest częścią wszystkich etapów stosowanej metodyki projektu. Dobór zabezpieczeń jest oparty o szacowanie ryzyka, realizowane już na wstępnym etapie projektu;

14.3. Urządzenia mobilne i telepraca.

Za urządzenia mobilne uważa się wszelkie urządzenia elektroniczne, przenośne służące do przetwarzania informacji (laptop, tablet, smartphone itp.)

14.3.1. Polityka użytkowania urządzeń mobilnych.

Praca zdalna i jej zasady zostały opisane w Polityce Ochrony Danych Osobowych - Rozdział X zarządzanie bezpieczeństwem pracy zdalnej i mobilnym przetwarzaniem danych osobowych i jest zgodna z Polityką Bezpieczeństwa Informacji oraz Załącznikiem nr 1 do Polityki Ochrony Danych Osobowych – Instrukcja ochrony danych osobowych w trakcie pracy zdalnej.

- Wszystkie urządzenia mobilne muszą być zarejestrowane w ewidencji sprzętu (spis aktywów);
- Urządzenie mobilne jest przypisane do poszczególnego pracownika , który oświadcza, że ma świadomość zagrożeń na przykład jego kradzieży, utraty lub możliwości ujawnienia danych;
- Urządzenie mobilne jest odpowiednio zabezpieczane przed kradzieżą, przejęciem poufnych danych uwierzytelniających, zgodnie z obowiązującymi zasadami bezpieczeństwa;
- Za przygotowanie urządzenia do pracy odpowiedzialna jest Dział IT:
  - Zainstalowany system operacyjny i aplikacje są na bieżąco aktualizowane;
  - Zainstalowane oprogramowanie antywirusowe jest na bieżąco aktualizowane;
  - Włączona jest kontrola dostępu do urządzenia:
    - Włączone hasło do BIOS / UEFI (laptop).
    - Włączenie zabezpieczenia hasłem.
    - Dostęp do systemu operacyjnego zabezpieczony hasłem (min. 14 znaków, częstotliwość zmian minimum co 90 dni) - opcjonalnie zastosowanie rozwiązań biometrycznych lub logowanie z wykorzystaniem elektronicznej karty.
  - Maksymalne ograniczenie uprawnień użytkownika.
- Naprawa i serwis urządzenia odbywają się w Dziale IT, w przypadku konieczności przeprowadzenia naprawy w zewnętrznym podmiocie urządzenie przekazywane są bez danych;

- Przy wycofaniu urządzenia z użytkowania personel Działu IT trwale usuwa dane.
- W trybie pracy serwisowej upoważniony personel Działu IT korzysta z zabezpieczonych połączeń VPN;
- Wszystkie przypadki naruszenia bezpieczeństwa, a szczególnie: utrata sprzętu, utrata lub podejrzenie utraty poufnych danych uwierzytelniających mające wpływ na bezpieczeństwo informacji muszą być niezwłocznie zgłaszane do Działu IT;
- W przypadku pojawienia się incydentu bezpieczeństwa informacji w tym danych osobowych powiadamiany jest Pełnomocnik ds. Cyberbezpieczeństwa;
- Nieprzestrzeganie zasad bezpieczeństwa przy korzystaniu z urządzeń mobilnych może skutkować odpowiedzialnością dyscyplinarną;

14.4. Bezpieczeństwo zasobów ludzkich.

Bezpieczeństwo zasobów ludzkich jest związane bezpośrednio i wynika z Regulaminu Pracy ASP stanowiącego załącznik do Zarządzenia Rektora nr I/49/2019 oraz niniejszej Polityki. W przypadku współpracowników czy kontrahentów Uczelni, szczegóły dotyczące zakresu ochrony i bezpieczeństwa informacji regulują szczegółowe zapisy określone w indywidualnych umowach cywilno-prawnych zarówno podczas zatrudnienia, zmiany lub jego zakończenia.

14.4.1. Przed zatrudnieniem.

W ASP w ramach postępowania rekrutacyjnego może być prowadzona weryfikacja informacji dotyczących kandydata do pracy w zakresie:

- Historii zawodowej - kompletność i dokładność przedstawionego życiorysu;
- Dostępności i treści świadectw pracy i referencji;
- Deklarowanego wykształcenie, kompetencji i kwalifikacji zawodowych, niezbędnych uprawnień, jeśli są niezbędne do pełnienia określonej funkcji;
- Tożsamości kandydata;
- Opcjonalnie niekaralności, na podstawie złożonego zaświadczenia o niekaralności;
- Innych uzasadnionych zakresem powierzonych obowiązków i realizowanych zadań na rzecz ASP;

Podczas procesu rekrutacyjnego Dział Organizacji Kadr może poprosić o udział w procesie naboru na stanowiska związane z bezpieczeństwem informacji Pełnomocnika ds. Cyberbezpieczeństwa.

14.4.2. Podczas zatrudnienia.

- Podczas zatrudnienia pracownik zapoznaje się z Polityką Bezpieczeństwa Informacji oraz innymi niezbędnymi dokumentami (Regulaminy, Polityka bezpieczeństwa danych osobowych);
- Fakt zapoznania z dokumentem PBI odnotowywany jest w karcie zapoznania z PBI;
- Nowo zatrudniony pracownik przechodzi szkolenie z podstawowej obsługi systemów informatycznych;
- Nowo zatrudniony pracownik informowany jest o możliwości wszczęcia postępowania dyscyplinarnego w związku z naruszeniem bezpieczeństwa informacji;

Każdy pracownik (współpracownik) oraz w uzasadnionych przypadkach kontrahent realizujący jakiekolwiek zadania na rzecz ASP i mający dostęp do systemów informacyjnych musi być poddany różnym formom uświadamiania, kształcenia i szkoleń w zakresie praktyk i obowiązków dotyczących bezpieczeństwa informacji systemu, tak by posiadał właściwy dla swojej roli poziom świadomości, wiedzy i nawyków działania, odpowiadający ustalonemu wysokiemu poziomowi bezpieczeństwa systemu.

W tym celu Kanclerz, Pełnomocnik ds. Cyberbezpieczeństwa wraz z Inspektorem Ochrony Danych i Administratorem Systemów Informatycznych opracowują **Plan szkoleń**.

Plan szkoleń zatwierdza Rektor.

Program szkolenia zawiera problematykę:

- Rozwiązań organizacyjnych i technicznych bezpieczeństwa informacji zawartych w **PBI;**
- Ochrony danych osobowych;
- Bezpieczeństwa systemu teleinformatycznego;

Program szkolenia może być profilowany dla różnych grup pracowników zatrudnionych w ASP.

W Planie szkoleń uwzględnia się szkolenia wewnętrzne jak i zewnętrzne.

Szkolenia w ASP odbywają się cyklicznie i podzielone są na szkolenia wstępne i okresowe.

Program szkoleń wstępnych i okresowych może obejmować następujące zagadnienia:

- Pojęcie bezpieczeństwa i atrybuty bezpieczeństwa;
- Procesy przetwarzania danych;
- Wymagania prawne w zakresie ochrony danych osobowych;
- Osobista odpowiedzialność za działania w zakresie ochrony informacji;
- Konsekwencje karne i dyscyplinarne nieprzestrzegania zasad ochrony informacji;
- Obowiązki w zakresie zabezpieczenia i ochrony informacji;
- Podstawowe procedury bezpieczeństwa informacji (np. zgłaszanie incydentów bezpieczeństwa informacji) oraz podstawowe zabezpieczenia (np. bezpieczeństwo haseł, zabezpieczenia przed szkodliwym oprogramowaniem i „czyste biurka");
- Dane kontaktowe komórki (osoby) odpowiedzialnej za bezpieczeństwo informacji systemu np. IOD, Pełnomocnik ds. Cyberbezpieczeństwa;
- Sposoby pozyskania dodatkowym informacji i materiałów dotyczących bezpieczeństwa informacji w ASP;

Kluczowe role dla bezpieczeństwa systemu informatycznego ASP pełnią pracownicy Działu IT. Rektor zapewnia dedykowane szkolenia dla personelu IT.

Program szkoleń dedykowanych może obejmować tematykę związaną z:

- Procesem bezpiecznego wytwarzania i testowania aplikacji www;
- Bezpieczeństwem systemów i aplikacji wykorzystywanych w ASP;
- Wytycznymi prawnymi bezpieczeństwa systemów informatycznych;
- Procedurami i politykami dotyczącymi rozwoju systemu ASP;
- Zabezpieczeniami kryptograficznymi;
- Bezpieczeństwem w relacjach z dostawcami usług;
- Bezpieczeństwem zasobów ludzkich;

- Bezpieczeństwem komunikacji (bezpieczeństwo systemów i sieci);
- Pozyskiwaniem, rozwojem i utrzymaniem systemów (ciągłość działania);
- Zarządzaniem incydentami związanymi z bezpieczeństwem informacji;

14.4.3. Zakończenie i zmiana zatrudnienia.

W związku ze zmianą zatrudnienia i zakresu obowiązków oraz z zakończeniem zatrudnienia lub umowy przedstawia się pracownikowi, współpracownikowi obowiązki w zakresie bezpieczeństwa informacji, szczególnie w zakresie zachowania poufności, które pozostają aktualne po zmianie lub zakończeniu zatrudnienia.

W przypadku zakończenia zatrudnienia Dział Organizacji Kadr wydaje pracownikowi kartę obiegową (rozliczenie z ASP) i przekazuje informację do Działu IT. Pracownik Działu blokuje uprawnienia do konta w systemie informatycznym.

W przypadku zmiany warunków zatrudnienia o nowe uprawnienia do systemu występuje bezpośredni przełożony pracownika.

14.5. Zarządzanie aktywami.

Aktywa systemu związane z bezpieczeństwem informacji oraz środkami przetwarzania informacji zostały zidentyfikowane i opisane w dokumencie **Zarządzanie Ryzykiem**.
Wykaz aktywów jest na bieżąco monitorowany i w razie konieczności aktualizowany.

Ewidencjonowane aktywa systemu mają jednoznacznie przypisanego właściciela.
W systemie obowiązują zasady akceptowalnego użycia informacji oraz aktywów i środków związanych z przetwarzaniem informacji, tzn.: każdy pracownik ASP ponosi odpowiedzialność za wykorzystanie zasobów przetwarzania informacji w ramach swojego zakresu odpowiedzialności.
Pracownicy oraz osoby lub podmioty realizujące zadania w systemie w momencie zakończenia zatrudnienia lub okresu obowiązywania umowy zwracają wszystkie posiadane i udostępnione im aktywa.

14.5.1. Postępowanie z nośnikami.

Celem procedury jest zapewnienie nadzoru nad prawidłowym przebiegiem wszelkich czynności związanych z zarządzaniem (cyklem życia) nośników informacji, to znaczy: wprowadzeniem nośników do użycia, obsługą bieżącą nośników, wycofaniem z obiegu oraz trwałym usuwaniem nośników. Przez nośniki informacji/danych, zwane w skrócie nośnikami, rozumie się wszelkie przedmioty fizyczne, na których możliwe jest zapisywanie i późniejsze odczytywanie informacji. Wszelkie nośniki, występujące w procesie podlegają wytycznym niniejszego dokumentu.

14.5.1.1. Dane w wersji papierowej.

W ASP dane w wersji papierowej występują w każdej komórce organizacyjnej. Dane w wersji papierowej przechowywane są w zamykanych szafach biurowych. Dostęp do pomieszczeń

posiadają tylko uprawnieni pracownicy. w pomieszczeniach ASP przestrzegana jest zasada „czystego biurka".

Zabrania się:

- Nieuprawnionego kopiowania dokumentów;
- Nieuprawnionej modyfikacji;
- Nieuprawnionego niszczenia dokumentów;
- Wynoszenia dokumentów poza siedzibę ASP (bez upoważnienia);
- Udostępniania dokumentów osobom nieuprawnionym;

W procesie niszczenia dokumentów wykorzystywane są niszczarki o minimalnej klasie bezpieczeństwa.

14.5.1.2. Nośniki elektroniczne.

Poniższe procedury dotyczą tylko nośników użytkowanych przez personel ASP do celów służbowych.

Obsługa wszelkich nośników cyfrowych jest prowadzona w sposób zapewniający bezpieczeństwo informacji zawartych na tych nośnikach.

Cykl życia użytych cyfrowych nośników informacji bezpośrednio wynika z rodzaju informacji, jakie te nośniki zawierają oraz ich „sprawności" (poprawnego działania, wynikającego ze stopnia zużycia).

W przypadku nośników, do których nie mają zastosowania określone przepisy prawa przyjmuje się, że dane powinny być przechowywane w sposób odpowiednio zabezpieczony przez okres **nie krótszy jeden rok**, od momentu ustania przyczyny, dla której zostały wytworzone. Po ustalonym okresie musi zostać niezwłocznie podjęta decyzja o ich archiwizacji lub zniszczeniu.

Każdy cyfrowy nośnik informacji przed przekazaniem go do eksploatacji jest odpowiednio zewidencjonowany. w trakcie przekazania nośnika do eksploatacji zostaje określona osoba odpowiedzialna za nośnik, jak również określane jest dopuszczalny sposób jego użycia. Właściciel aktywa jest odpowiedzialny za dany nośnik informacji cyfrowej. Wszelkie zmiany związane z nośnikiem, na przykład jego przekazanie innemu użytkownikowi, wycofanie z eksploatacji czy likwidacja jest odnotowywane w ewidencji.

Ewidencję wydanych nośników prowadzi Działu IT oraz poszczególni kierownicy komórek organizacyjnych ASP.

Zabrania się:

- Nieuprawnionego kopiowania nośników;
- Nieuprawnionej modyfikacji danych na nośniku;
- Nieuprawnionego niszczenia nośników;
- Wynoszenia nośników informacji poza siedzibę ASP (bez upoważnienia);
- Udostępniania nośników osobom nieuprawnionym;
- Wykorzystywania prywatnych nośników;
- Podłączania do systemu nośników niewiadomego pochodzenia;

Przed utylizacją nośnika (elektrośmieci) wszelkie dane są trwale usuwane.

Wymagania dla procesu fizycznej utylizacji nośników:

Utylizacja może się odbywać w zależności o przyjętej technologii wg następujących wytycznych:

- Metodę termiczną: metoda hutnicza w temperaturze powyżej 1000 st. C;
- Metodą chemiczną zmieniającą w trakcie procesu strukturę dysku w ciecz nieposiadającą właściwości magnetycznych;
- Metodę mechaniczną (wymontowanie talerzy dysku i mechaniczne zniszczenie, niszczarki dysków);

W celu ochrony danych stosuje się zabezpieczenia kryptograficzne w postaci szyfrowania nośników wymiennych.

14.6. Kontrola dostępu.

Dostęp do systemów informatycznych ASP jest możliwy tylko dla uprawnionego personelu. Użytkownicy systemu mają dostęp wyłącznie do tych sieci (zasobów), do których otrzymali uprawnienia zgodnie z zakresem obowiązków. o uprawnienia dostępu wnioskuje Kierownik komórki organizacyjnej. Uprawnienia przydziela Administrator Systemów Informatycznych.

14.6.1. Kontrola dostępu fizycznego.

W pomieszczeniach, gdzie zainstalowano elementy systemu teleinformatycznego ASP może przebywać tylko upoważniony personel.

14.6.2. Zarządzanie dostępem użytkowników.

- W systemie zarządzania dostępem funkcjonuje formalny proces rejestrowania i wyrejestrowywania użytkowników w celu przydzielania praw dostępu;
- W ograniczonym zakresie i w warunkach umożliwiających właściwy nadzór przewiduje się przydzielanie praw uprzywilejowanego dostępu;
- ASI regularnie dokonuje przeglądu kont użytkowników. Nieaktywne identyfikatory są blokowane;
- Po zakończeniu zatrudnienia konto jest blokowane. Profile użytkownika po 1 roku są trwale usuwane z systemu (AD). Podobnie profile kont poczty służbowej usuwane są po 1 roku;

14.6.3. Zarządzanie dostępem uprzywilejowanym.

W ASP dostęp do wszystkich zasobów informatycznych posiadają tylko upoważnieni pracownicy Działu IT. Konto o uprzywilejowanych uprawnieniach może być utworzone tylko za zgodą Rektora po wstępnej akceptacji Pełnomocnika ds. Cyberbezpieczeństwa.

14.6.4. Odpowiedzialność użytkownika systemu.

- Użytkownik ma obowiązek przestrzegania zapisów PBI oraz Regulaminu Pracy stanowiącego załącznik do Zarządzenia Rektora nr I/49/2019 w szczególności:
- Nieujawniania danych autoryzujących dostęp do systemu osobom trzecim.
- Niezapisywania danych autoryzujących na karteczkach lub innych miejscach łatwo dostępnych dla innych osób.
- Niezwłocznej zmiany hasła w przypadku możliwości jego ujawnienia.
- Wyboru hasła dobrej jakości i odpowiedniej długości z uwzględnieniem:
  - Łatwości zapamiętania (brak niebezpiecznych zapisów, karteczek z hasłami).
  - Nieopierania się na prostych skojarzeniach (imiona nazwiska, daty urodzenia, daty rocznic).
  - Podatności na atak słownikowy.
  - Niezawierania ciągów jednakowych znaków.
- Nieużywania tego samego hasła do różnych systemów.

14.6.5. Procedury bezpiecznego logowania.

W celu zapewnienia bezpieczeństwa danych przetwarzanych w systemach eksploatowanych w ASP opracowano procedury bezpiecznego logowania do systemów operacyjnych i aplikacji użytkowych.

- Dostęp do BIOS / UEFI komputerów zabezpieczony jest hasłem;
- Wyłączono możliwość uruchamiania systemu z zewnętrznego nośnika;
- Podczas logowania nie wyświetlane są informacji pomocnicze oraz hasło;
- Użytkownik ma ograniczoną liczbę prób logowania do systemów informatycznych;
- System wymusza użycie hasła odpowiednio silnego (m. in. znaki, litery, cyfry, znaki specjalne);
- System wymusza zmianę hasła zgodnie z ustalonymi interwałami czasowymi;

W indywidualnych przypadkach po akceptacji Pełnomocnika ds. Cyberbezpieczeństwa można odstąpić od części przytoczonych reguł.

14.7. Kryptografia.

Celem procedury kryptograficznej jest zapewnienie poufności danych przetwarzanych w systemach przenośnych oraz bezpiecznego realizowania połączeń serwisowych z sieci zewnętrznej jak również bezpieczne przysłanie danych z wykorzystaniem poczty elektronicznej.

14.7.1. Urządzenia mobilne i nośniki danych.

Wykorzystywane przez personel ASP urządzenia przenośne (jeżeli jest to niezbędne) posiadają zaimplementowane mechanizmy szyfrowania dysków:

- BitLocker (natywny szyfrator systemu Windows);
- Inny program szyfrujący;

Podobnie dane na nośnikach przenośnych szyfrowane są za pomocą w/w mechanizmów.

14.7.2. Praca zdalna (serwis IT).

W związku z potrzebą ciągłego monitorowania pracy systemów teleinformatycznych ASP zachodzi konieczność realizacji bezpiecznych połączeń serwisowych z sieci zewnętrznej i wykonywaniu niezbędnych prac serwisowych.

- W przypadku zdalnego połączenia wykorzystywane są tunele VPN;
- Konfiguracja i nadzór VPN realizowana jest przez ASI;
- Zabranie się uruchamiania przez firmy zewnętrzne usług serwisowych opartych na aplikacjach typu TeamViewer, AnyDesk. Dopuszcza się realizację tego typu usług wyłącznie pod nadzorem upoważnionego pracownika Działu IT;
- W przypadku zgody na zdalny serwis każdorazowe połączenie musi być inicjowane przez pracownika ASP i odnotowane w rejestrze zdarzeń;

14.7.3. Przesyłanie plików.

W celu bezpiecznego przesyłania plików użytkownik zobowiązany jest do korzystania z zabezpieczonej hasłem postaci np. *.zip. Hasło do odczytu należy przesyłać za pomocą innego kanału komunikacji (np. SMS, połączenie głosowe).
Dotyczy to komunikacji zewnętrznej z wyłączeniem organów państwowych (używają bezpiecznych kanałów komunikacyjnych) oraz wewnętrznej w uzasadnionych przypadkach (np. przesyłanie tabeli płac danych osobowych etc.)

14.7.4. Badanie i ocena zabezpieczeń kryptograficznych.

Adekwatność i skuteczność dobranych zabezpieczeń kryptograficznych, podlega ciągłej analizie i ocenie w zakresie rodzaju informacji, która jest zabezpieczana jak również implementowanego sposobu jej zabezpieczenia.

W dotychczasowej praktyce stosowania zabezpieczeń nie odnotowano żadnych przypadków naruszenia bezpieczeństwa informacji. Pomimo tego w Dziale IT testowane są różne rozwiązania dotyczące szyfrowania nośników danych dostępne na rynku.

14.8. Bezpieczeństwo fizyczne i środowiskowe.

Zgodnie z Załącznikiem nr 8 Polityki Ochrony Danych Osobowych - Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych - Szczegółowe zabezpieczenia fizyczne są opisane w dokumentacji prowadzonej przez Specjalistę ds. obronnych. Dokumentacja może być udostępniona tylko osobom upoważnionym przez Kanclerza ASP.

14.8.1. Obszary bezpieczne.

- Elementy serwerowe eksploatowanego systemu teleinformatycznego ASP umieszczone są w specjalnym pomieszczeniu (serwerownia);
- Dostęp do serwerowni jest chroniony i zabezpieczony przed nieuprawnionym dostępem poprzez stosowanie: środków ochrony budowlano-mechanicznych (drzwi wzmocnione wyposażone w pojedynczy zamek), elektronicznych (kontrola dostępu) oraz ochrony fizycznej;
- W ASP opracowano i wdrożono politykę kluczy;
- Dostęp do teleinformatycznych punktów dystrybucyjnych jest ograniczony tylko dla uprawnionego personelu;
- Pomieszczenie serwerowni zabezpieczone jest system kontroli ppoż.;
- Usytuowanie serwerowni wyklucza zagrożenie polegające na zalaniu pomieszczenia;
- Przed zanikiem zasilania energetycznego systemy serwerowe zabezpieczone są przez UPS;

14.8.2. Dostęp do pomieszczeń.

- Dostęp do pomieszczeń gdzie funkcjonują elementy systemów informatycznych ASP ograniczony jest tylko dla upoważnionego personelu;
- Osoby z zewnątrz przebywające w pomieszczeniach specjalnych pozostają w asyście pracownika ASP;
- Należy zwracać uwagę na osoby z zewnątrz poruszające się w pobliżu pomieszczeń specjalnych;
- Szczególną uwagę zwraca się na dostęp osób spoza ASP do:
  - Pomieszczeń, gdzie przetwarzane są dane osobowe.
  - Innych pomieszczeń specjalnych (serwerownie, archiwa, pomieszczenia techniczne).

14.8.3. Sprzęt (ochrona i lokalizacja).

- Rozmieszczenie sprzętu jest zaplanowane w taki sposób, aby możliwa była jego ochrona przed nieuprawnionym dostępem oraz wpływem zagrożeń środowiskowych;
- Sprzęt jest chroniony przed skutkami awarii systemów wspomagających;
- Okablowanie zasilające oraz teleinformatyczne, przenoszące dane lub wspomagające usługi informacyjne jest chronione przed przechwyceniem, zakłóceniem lub uszkodzeniem. Dostęp do punktów dystrybucyjnych ograniczony jest tylko dla upoważnionego personelu;

- Sprzęt jest prawidłowo i na bieżąco konserwowany;
- Sprzęt przetwarzający informacje wrażliwe może być wynoszony poza ASP tylko za zgodą Rektora;
- Przed zbyciem lub przekazaniem sprzętu do ponownego użycia nośniki danych sprawdzane są pod kątem prawidłowego usunięcia lub nadpisania chronionych danych oraz licencjonowanych programów;
- Użytkownicy są zobowiązani do zapewnienia właściwej ochrony sprzętu przenośnego na przykład poprzez odpowiednie zabezpieczenie sprzętu uniemożliwiające jego łatwe wyniesienie;
- Zabrania się spożywania posiłków i napojów bezpośrednio na stanowisku pracy przy urządzeniach przetwarzania informacji (zalanie klawiatury);

14.9. Bezpieczna eksploatacja.

W celu zapewnienia poprawnej i bezpiecznej eksploatacji systemów teleinformatycznych ASP służących zapewnieniu niezakłóconej realizacji usług opracowano poniższe zasady.

14.9.1. Instalacja i konfiguracja systemów i aplikacji.

- Za instalację i konfigurację systemów i aplikacji wykorzystywanych w ASP odpowiedzialny jest Dział IT;
- Użytkownik nie posiada uprawnień administracyjnych umożliwiających samodzielną instalację oprogramowania;
- Liczba użytkowników uprzywilejowanych (uprawnienia administratora) jest ograniczona do niezbędnego minimum;
- Wszelkie zmiany konfiguracyjne systemu są uzgadniane z ASI, a zmiany wpływające na bezpieczeństwo dodatkowo konsultowane są z Pełnomocnikiem ds. Cyberbezpieczeństwa, a w przypadku danych osobowych z IOD;
- Wszelkie zmiany w systemach mogące mieć wpływ na bezpieczeństwa informacji są testowane i dopiero po pozytywnej opinii ASI implementowane w systemie;
- Duże zmiany w systemie wymagają zgody Rektora po wstępnej akceptacji Kanclerza i Pełnomocnika ds. Cyberbezpieczeństwa;

14.9.2. Procedury rozpoczęcia, zawieszenia i zakończenia pracy.

Procedury obejmują również wszelkie zapisy określone w Polityce ochrony danych osobowych - Rozdział IX środki bezpieczeństwa i obowiązki pracowników.

14.9.2.1. Rozpoczęcie pracy.

- Przed przystąpieniem do pracy z systemem informatycznym użytkownik zobowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz dokonać oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie bezpieczeństwa informacji;
- W przypadku zablokowania dostępu do konta użytkownika systemu lub aplikacji należy powiadomić pracownika Działu IT. Pracownik w miarę możliwości ustala przyczyny

zablokowania systemu lub aplikacji oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania (np. powiadomienie ASI , odblokowanie konta);

14.9.2.2. Zawieszenie pracy.

- Przed opuszczeniem miejsca pracy użytkownik zobowiązany jest do wylogowania się z aplikacji / systemu lub do zablokowania systemu;
- W przypadku użytkowników / stanowisk z uprzywilejowanymi uprawnieniami czas automatycznego blokowania jest ustalany indywidualnie;

14.9.2.3. Zakończenie pracy.

Kończąc pracę należy:

- Wylogować się z aplikacji oraz systemu informatycznego, a następnie wyłączyć sprzęt komputerowy, jeżeli nie jest dalej wykorzystywany;
- Zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację, wydruki oraz nośniki informatyczne przed dostępem osób nieuprawnionych;

14.9.3. Zarządzanie pojemnością.

W celu zapewnienia właściwej wydajności systemów informatycznych eksploatowanych w ASP wprowadza się procedury zarządzania pojemnością dyskową.

- Dział IT jest odpowiedzialny za regularny przegląd zasobów dyskowych pod kątem pojemności;
- Nieaktualne dane usuwane są z systemu;
- Na podstawie bieżącego monitoringu zasobów dyskowych sporządzane są plany zakupów dysków (macierzy dyskowych);
- W procesie przeglądu zasobów uwzględnia się niezbędne elementy systemu kopii zapasowych;

14.9.4. Oddzielenie środowisk testowych od systemów eksploatowanych.

W celu minimalizacji ryzyka związanego z uszkodzeniem, awarią systemu eksploatowanego w ASP przy wprowadzaniu nowych rozwiązań technologicznych wprowadza się obowiązek testowania, uruchamiania aplikacji z wykorzystaniem bezpiecznego środowiska testowego.

- Dział IT jest odpowiedzialna za przetestowanie aplikacji i rozwiązań konfiguracyjnych systemów przed uruchomieniem lub wprowadzeniem w systemie informatycznym ASP;

14.9.5. Ochrona przed złośliwym oprogramowaniem.

W celu wykrywania i zapobiegania przed szkodliwym oprogramowaniem w ASP wprowadza się:

- Konieczność instalacji oprogramowania antywirusowego na każdej stacji komputerowej pracującej w systemie informatycznym ASP;
- Bieżącą i regularną aktualizację bazy danych (sygnatur) wirusów;
- Zakaz instalowania nieautoryzowanego oprogramowania;
- Zakaz podłączania do systemu informatycznego nośników nieznanego pochodzenia;
- W indywidualnych przypadkach za zgodą Pełnomocnika ds. Cyberbezpieczeństwa można odstąpić od niektórych powyższych reguł;

14.9.6. Kopie zapasowe.

Podstawowym i niezbędnym elementem zachowania ciągłości działania systemów informatycznych, a tym samym niezakłóconej realizacji zadań jest systematyczne wykonywanie kopii zapasowej danych.

Za realizację procedur wykonywania kopii zapasowych odpowiedzialna jest Dział IT.

- System kopii zapasowych w ASP jest zautomatyzowany;
- System kopii zapasowych obejmuje dane konieczne do podtrzymania procesów i zachowania ciągłości działania Uczelni;
- System kopii zapasowych realizowany jest w ustalonych cyklach;
- Dział IT regularnie testuje przydatność kopii zapasowych;
- Kopia danych przechowywana jest w innej lokalizacji niż systemy produkcyjne ASP;

14.9.7. Rejestrowanie zdarzeń i monitorowanie.

- W ASP tworzy się, przechowuje i systematycznie przegląda dzienniki zdarzeń rejestrujące działania użytkowników, usterki oraz zdarzenia związane z bezpieczeństwem informacji. Dzienniki są przechowywane, **co najmniej przez 1 rok** od daty ostatniego wpisu;
- Dzienniki mają formę elektroniczną lub papierową;
- Dzienniki w wersji elektronicznej, w miarę możliwości, powinny obejmować informacje:
  - Zmian konfiguracji systemów i aplikacji.
  - Błędów w systemach operacyjnych.
  - Usterek sprzętu teleinformatycznego.
  - Innych zdarzeń mających wpływ na pracę systemów informatycznych ASP.
- Środki służące rejestrowaniu zdarzeń oraz informacje w dziennikach zdarzeń są chronione przed manipulacją i nieuprawnionym dostępem;
- Dokumentowane są również czynności administratorów i operatorów systemów;
- Zegary wszystkich istotnych elementów systemu są zsynchronizowane z jednym wzorcowym źródłem czasu;

14.9.8. Nadzór nad oprogramowaniem.

Stały nadzór nad instalacją, uruchomieniem oraz eksploatacją programów eksploatowanych w ASP sprawuje Dział IT.

Pracownicy Działu IT na bieżąco aktualizują oprogramowanie systemowe oraz aplikacje użytkowe eksploatowane w ASP.

Wdrażanie nowego oprogramowania odbywa się z zachowaniem poniższych zasad i procedur:

- Dział IT przeprowadza kontrolę i testy aplikacji przed ostatecznym uruchomieniem w środowisku informatycznym ASP;
- Zapewniona jest kontrola konfiguracji, wszelkie zmiany mające wpływ na bezpieczeństwo informacji są dokumentowane (Zarządzanie zmianami PBI);
- Opracowana jest procedura przywrócenia poprzedniej wersji na wypadek niepowodzenia aktualizacji lub nowej instalacji;
- W przypadku kluczowych systemów ASP zapewnione jest wsparcie producenta;

14.9.9. Zarządzanie podatnościami technicznymi.

Informacje o podatnościach technicznych wykorzystywanych systemów i oprogramowania pozyskiwane przez pracowników Działu IT. Oceniany jest stopień narażenia kluczowych elementów systemów informatycznych ASP na te podatności i podejmowane są środki w celu przeciwdziałania związanemu z nimi ryzyku. Prowadzona jest analiza podatności technicznych **nie rzadziej niż 1 raz na kwartał**, z uwzględnieniem:

- Informacji od użytkowników systemów;
- Incydentów, błędów, nieprawidłowej pracy urządzeń oraz oprogramowania;
- Informacji od producentów sprzętu i oprogramowania;
- Serwisów udostępnionych w sieciach publicznych (testy penetracyjne, luki w oprogramowaniu, opinie techniczne, analizy podatności);
- Wykrytych podatności, które są niezwłocznie poddawane analizie, podejmowane są dalsze kroki (Zarządzanie zmianami) o minimalizacji ryzyka wystąpienia określonego zdarzenia;

Istotnym i kluczowym elementem pozyskiwania wiedzy o podatnościach poszczególnych elementów systemów są regularne i systematyczne szkolenia dla specjalistów Dział IT.

14.9.10. Audyt systemów informacyjnych (zalecenia).

W celu niezakłóconej pracy systemów informatycznych oraz minimalizacji wpływu czynności audytowych na te systemy zaleca się:

- Staranne zaplanowanie terminu i zakresu czynności audytowych;
- Uzgodnienie zakresu audytu z kierownikami komórek organizacyjnych;
- Ograniczenie testów oprogramowania i danych tylko w trybie do odczytu;
- Przeprowadzanie czynności testowych powodujących ograniczenie dostępności systemów zaplanować z uwzględnieniem minimalnego wpływu na pracę systemów;
- Przeprowadzanie testów mających wpływ na konfigurację systemów na kopii środowiska produkcyjnego;

14.10. Bezpieczeństwo komunikacji.

Celem procedur bezpieczeństwa komunikacyjnego jest zapewnienie ochrony informacji przesyłanych w sieciach i innych środkach przetwarzania w komunikacji wewnątrz ASP jak i na zewnątrz.

14.10.1. Zabezpieczenia sieci teleinformatycznej.

W ASP zastosowano niezbędne środki ochrony sieci teleinformatycznej służącej do realizacji usług:

- Ograniczono dostęp do aktywnych punktów sieci tylko dla upoważnionego personelu IT;
- Dostęp do punktów dystrybucyjnych i okablowania strukturalnego ograniczony jest do upoważnionego personelu;
- Dostęp do konfiguracji urządzeń sieciowych zabezpieczony jest hasłem;
- Z dostawcą usług dostępu do Internetu podpisano umowę uwzgledniającą właściwy poziom SLA;
- Na styku z siecią zewnętrzną zastosowano Firewall;
- W sieci wewnętrznej przydzielono wewnętrzna adresację IP (NAT);
- Sieć bezprzewodowa jest dostępna a dostęp do sieci zabezpieczony jest hasłem;
- Wykorzystywany jest bezpieczny protokół transmisji bezprzewodowej;
- W sieci wewnętrznej dokonano podziału na VLAN;
- Wykorzystywane są bezpieczne połączenia VPN;

14.10.2. Przesyłanie informacji.

W ASP opracowano i wprowadzono procedury przesyłania informacji wewnątrz jak i na zewnątrz.

W komunikacji wewnętrznej i zewnętrznej wykorzystywany jest system poczty elektronicznej.

14.10.3. Instrukcja bezpiecznego korzystania z poczty elektronicznej.

W celu bezpiecznego korzystania z poczty elektronicznej użytkownik zobowiązany jest do:

- Wykorzystywania poczty elektronicznej tylko w celach służbowych;
- Niekorzystania z prywatnych kont pocztowych w korespondencji służbowej;
- Zwrócenia uwagi na prawidłowość adresata (adresatów) wiadomości;
- Zwrócenia uwagi na nadawcę wiadomości;
- Zwrócenie szczególnej uwagi na komunikaty programu antywirusowego;
- Nieotwierania podejrzanych załączników;
- Nieotwierania linków do stron zewnętrznych w załączniku poczty;
- Zgłaszania do Działu IT każdego przypadku naruszenia bezpieczeństwa informacji;

14.10.4. Instrukcja bezpiecznego korzystania z sieci Internet.

W celu minimalizacji ryzyka związanego z zagrożeniami pochodzącymi z sieci Internet do podstawowych obowiązków użytkowania należy:

- Nieodwiedzania stron powszechnie uważanych za niebezpieczne;
- Zwrócenie uwagi na komunikaty programu antywirusowego;
- Niezapisywania haseł w historii przeglądarki;
- Nieotwierania podejrzanych linków do zewnętrznych stron;
- Nieuruchamiania oprogramowania nieznanego pochodzenia;
- Nieinstalowania oprogramowania nieznanego pochodzenia;
- Niewpisywania loginów i haseł w formularzach niezabezpieczonych stron (bez https w adresie strony);
- Zgłaszania do Działu IT każdego przypadku naruszenia bezpieczeństwa informacji;

14.11. Rozwój systemów informatycznych.

Podstawowym celem rozbudowy i modernizacji systemów informatycznych ASP jest zapewnienie bezpieczeństwa informacji na każdym etapie prac rozwojowych.

W procesie rozwoju systemów uwzględnia się:

- Stały nadzór Najwyższego Kierownictwa ASP nad każdym etapem projektu;
- Obowiązek konsultowania każdego projektu, którego elementy mogą być związane z bezpieczeństwem informacji, z Działem IT (np. kontrola dostępu, wsparcie dla systemów laboratoryjnych, zakup nowych urządzeń wymagających pracy w sieci teleinformatycznej itp.);
- Konsultacje wewnętrzne i zewnętrzne dotyczące bezpieczeństwa systemów;
- Przygotowanie niezbędnego środowiska testowego;
- Zapisy dotyczące poufności z dostawcami usług zewnętrznych;
- Uwagi użytkowników (pracowników);

Na każdym etapie rozbudowy systemu prowadzona jest analiza ryzyka dotycząca bezpieczeństwa prowadzonego projektu.

14.12. Relacje z dostawcami usług i sprzętu.

Relacje z zewnętrznymi podmiotami realizującymi usługi na rzecz ASP wymagają pisemnej umowy, jeżeli w związku z realizacją umowy podmiot zewnętrzny będzie miał dostęp do danych osobowych przetwarzanych w ASP konieczne będzie sporządzenie Umowy o powierzeniu przetwarzania danych osobowych. Szczegóły opisane w Polityce ochrony danych osobowych w ASP.

W celu spełnienia najwyższych wymagań dotyczących bezpieczeństwa informacji w umowach (porozumieniach) należy uwzględnić między innymi:

- Opis i zakres informacji udostępnianych podmiotowi zewnętrznemu;
- Wymagania i regulacje prawne dotyczące:
  - Ochrony danych osobowych.
  - Własności intelektualnej.
  - Praw autorskich.
  - Tajemnicy przedsiębiorstwa.
- Zapewnienie właściwego poziomu bezpieczeństwa dostarczanych urządzeń (np. stosowanie oprogramowania antywirusowego, stosowanie zapory Firewall, ograniczenie uprawnień użytkowników), wszelkie odstępstwa od wymaganego poziomu zabezpieczeń muszą być akceptowane przez Pełnomocnika ds. Cyberbezpieczeństwa;
- Wykaz pracowników uczestniczących w projekcie;
- Wskazanie osób odpowiedzialnych po stronie dostawcy i zamawiającego za realizację poszczególnych etapów usługi;
- Bezpieczną komunikację;
- Ewentualny udział podwykonawców;
- Zapisy o poufności;
- W przypadku usług serwisowych, właściwy poziom SLA;

Relacje z dostawcami podlegają ciągłemu monitorowaniu.

14.13. Zarządzanie incydentami w bezpieczeństwie informacji.

Zapewnienie skutecznego reagowania na incydenty związane z bezpieczeństwem informacji oraz informowanie o zdarzeniach i słabościach jest podstawowym celem zarządzania incydentami w ASP.
Z każdego przypadku naruszenia bezpieczeństwa informacji wyciągane są wnioski i opracowywane są plany działań minimalizujące skutki incydentów.

14.14. Zarządzanie ciągłością działania.

W celu zapewnienia ciągłości działania systemów informatycznych niezbędnych do niezakłóconej realizacji usług kluczowych w ASP wprowadzono:

- Automatyczny system kopii zapasowych pozwalający na przywrócenie do pracy systemów informatycznych;
- Redundancje (nadmiarowość) rozwiązań sprzętowych;
- Zasilanie awaryjne w postaci UPS;

- Powołano personel reagujący na incydenty bezpieczeństwa systemów informatycznych (Dział IT);

14.15. Zgodność.

- W PBI zawarto wszystkie istotne wymagania prawne, regulacyjne oraz umowne. Najwyższe kierownictwo ASP deklaruje weryfikowanie na bieżąco ich przestrzegania. Dotyczy to zarówno przepisów obowiązującego prawa, jak również wytycznych wynikających z innych dokumentów takich jak normy jakościowe, branżowe;
- W zakresie praw własności intelektualnej i użytkowania prawnie zastrzeżonego oprogramowania dozwolone jest przetwarzanie tylko w zgodzie z poszanowaniem tych praw oraz w zgodzie z przepisami obowiązującego prawa;
- Informacje w postaci zapisów istotnych dla polityki bezpieczeństwa informacji podlegają ochronione przed utratą, zniszczeniem, zafałszowaniem, nieuprawnionym dostępem i nieuprawnionym opublikowaniem zgodnie z obowiązującymi wymaganiami prawnymi. Zapisy powinny być przechowywane nie krócej niż zasady przechowywania dokumentacji, której te zapisy dotyczą;
- Zapewnia się prywatność i ochronę danych identyfikujących osobę stosownie do odpowiednich przepisów prawa i regulacji, ze szczególnym uwzględnieniem obowiązujących przepisów o ochronie danych osobowych;

15. Przegląd bezpieczeństwa informacji i postanowienia końcowe.

- Polityka Bezpieczeństwa Informacji jest dokumentem wewnętrznym ASP i nie może być udostępniana w żadnej formie, zarówno w całości, jak i w części osobom niezatrudnionym w ASP bez zgody Rektora lub Kanclerza;
- Z treścią PBI lub wyciągiem z PBI należy zapoznać wszystkich pracowników i współpracowników zgodnie z metryką dokumentu;
- PBI podlega regularnym przeglądom i aktualizacjom;
- Za przegląd bezpieczeństwa informacji odpowiedzialny jest Pełnomocnik ds. Cyberbezpieczeństwa;

16. Rejestr zmian.

Lp.	Opis zmian	Data i podpis.