System Zarządzania Bezpieczeństwem Informacji (SZBI) według normy PN-ISO/IEC 27001:2013

ZATWIERDZIŁ

J.M REKTOR
dr hab. inż. Zbigniew Osadowski, prof. AP

……..

/podpis na oryginale/

Listopad 2019 r.

SPIS TREŚCI

1. AKADEMIA POMORSKA

1.1 Informacje ogólne

Akademia Pomorska w Słupsku jest wyższą uczelnią publiczną o czterdziestoletniej tradycji. Powstała w 1969 r. na podstawie Rozporządzenia Rady Ministrów (DzU Nr 18 poz.134) pod nazwą Wyższa Szkoła Nauczycielska. Bazą dla WSN było Studium Nauczycielskie istniejące od 1957 r.

W trakcie wieloletniej działalności uczelni jej nazwa była kilkakrotnie zmieniana, co wynikało z wymogów formalnych i poszerzania oferty edukacyjnej. Akademia Pomorska w Słupsku obecną nazwę przyjęła w 2006 r., wcześniej – w 1974 r. WSN przekształciła się w Wyższą Szkołę Pedagogiczną, a w 2000 r. WSP – w Pomorską Akademię Pedagogiczną.

Obecnie na Akademii Pomorskiej w Słupsku istnieją pięć wydziałów: Wydział Filologiczno-Historyczny, Wydział Matematyczno-Przyrodniczy i Wydział Nauk Społecznych, Wydział nauk o Zdrowiu, Wydział Nauk o Zarządzaniu i Bezpieczeństwie. W ich obszarze działa 10 instytutów i 5 katedr.

Uczelnia posiada także jednostki ogólnowydziałowe, tj.: Wydawnictwo Naukowe, Archiwum Uczelniane i Bibliotekę Główną oraz międzyuczelniane: Studium Praktycznej Nauki Języków Obcych, Studium Wychowania Fizycznego i Sportu.

1.2 Postanowienia

Norma międzynarodowa ISO 27001:2013 dotyczy wszystkich rodzajów organizacji oraz określa wymagania dotyczące ustanawiania, wdrażania, stosowania, monitorowania, przeglądania, utrzymywania i udoskonalania udokumentowanego SZBI (Systemu Zarzadzania Bezpieczeństwem Informacji) w całościowym kontekście ryzyk biznesowych. Wyznacza ona wymagania dotyczące wdrażania zabezpieczeń dostosowanych do potrzeb pojedynczych organizacji lub ich części

Wdrożony w Akademii Pomorskiej w Słupsku SZBI jest zaprojektowany tak, aby zapewnić adekwatne i proporcjonalne zabezpieczenia, które odpowiednio chronią aktywa informacyjne Akademii Pomorskiej oraz aby uzyskać zaufanie studentów i innych zainteresowanych stron.

Wdrażając SZBI w Akademii Pomorskiej i ustanawiając zabezpieczenia wykorzystane zostały wytyczne normy ISO/IEC 17799:2005.

1.3 Definicje

Zamieszczone poniżej definicje mają na celu przybliżenie i usystematyzowanie terminologii stosowanej w zakresie zarządzania bezpieczeństwem informacji oraz zdefiniowanie pojęć, których znajomość jest niezbędna do zrozumienia treści niniejszej pracy.
W podanym słowniku pojęć podano wyłącznie definicje zawarte w normach związanych z bezpieczeństwem i audytem systemów informatycznych (PN ISO/IEC 27001, PN-I-02000:2002, PN-I-07799-2:2005, PN-I-13335-1:1999). Zdarza się, że ujęte w słowniku terminy definiowane są odmiennie

przez różne źródła. Samodzielna interpretacja nie powinna jednak wypaczyć podstawowego charakteru określenia. Słownik podzielony został na grupy tematyczne.

- **bezpieczeństwo** (security) - stan lub ochrona przed niekontrolowanymi stratami lub skutkami, kombinacja usług zapewniających poufność, integralność i dostępność
- **bezpieczeństwo informacji** (information security) - bezpieczeństwo polegające na zachowaniu poufności, integralności i dostępności informacji
- **System Zarządzania Bezpieczeństwem Informacji (SZBI)** - z ang. ISMS (Information Security Management System) - część całościowego systemu zarządzania oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji Uwaga: system zarządzania obejmuje strukturę organizacyjną, polityki, planowane działania, odpowiedzialności, zasady, procedury, procesy i zasoby (aktywa)
- **polityka bezpieczeństwa** (security policy) - zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonego systemu
- **bezpieczeństwo informacji** (information security) - zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność [ISO/IEC 17799:2005]
- **bezpieczeństwo systemu informatycznego** (IT security) - wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności systemu informatycznego
- **aktywa** (assets) - wszystko, co ma wartość dla organizacji [ISO/IEC 13335- 1:2004]
- **zasoby** - to samo, co aktywa
- **poufność** (confidentiality) - właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom [ISO/IEC 13335-1:2004]
- **integralność** (integrity) - właściwość zapewnienia dokładności i kompletności aktywów [ISO/IEC 13335-1:2004]
- **dostępność** (availability), zwana też dyspozycyjnością - jest zdefiniowana jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne [ISO/IEC 17799:2005] lub dostępność - właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu [ISO/IEC 13335-1:2004]
- **autentyczność** (authenticity) - właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana; autentyczność dotyczy takich podmiotów, jak użytkownicy, procesy, systemy i informacja [ISO/IEC 13335-1:2004]
- **niezawodność** (reliability) - właściwość oznaczająca spójne, zamierzone zachowanie i skutki
- **rozliczalność** (accountability) - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (ISO 7498-2:1989)
- **zagrożenie** (threat) - potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji
- **analiza zagrożeń** (threat analysis) - badanie działań i zdarzeń, które mogą szkodliwie wpływać na system przetwarzania danych

- **podatność** (vulnerability) - słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie
- **zdarzenie związane z bezpieczeństwem informacji** (security information event) - jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe przełamanie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem [ISO/IEC TR 18044:2004]
- **incydent związany z bezpieczeństwem informacji** (security information incident) - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji [ISO/IEC TR 18044:2004]
- **następstwa** (impact) - rezultat niepożądanego incydentu
- **ryzyko** (risk) - prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów
- **zabezpieczenie** (safeguard) - praktyka, procedura lub mechanizm redukujący ryzyko
- **analiza ryzyka** (risk analysis) - systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka [ISO/IEC Guide 73:2002]
- **szacowanie ryzyka** (risk assessment) - szacowanie zagrożeń, ich wpływu, podatności informacji i urządzeń do przetwarzania informacji oraz prawdopodobieństwa ich wystąpienia.
- **ocena ryzyka** (risk evaluation) - proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka [ISO/IEC Guide 73:2002]
- **audyt bezpieczeństwa** (security audit) - niezależny przegląd i sprawdzenie zapisów oraz funkcji systemu przetwarzania danych w celu sprawdzenia prawidłowości kontroli systemowej, zapewnienia zgodności z przyjętą polityką bezpieczeństwa i procedurami działania w celu wykrycia przełamania bezpieczeństwa oraz zalecenia określonych zmian w kontroli, polityce bezpieczeństwa i procedurach
- **badanie zgodności** (validation) - przeprowadzenie testów i dokonanie ocen bezpieczeństwa w celu ustalenia zgodności ze specyfikacją i z wymaganiami systemu bezpieczeństwa
- **dokumentacja** (documentation) - pisemna lub zarejestrowana w innej formie informacja o przedmiocie oceny, wymagana do jego oceny
- **ciągłość działania** (continuity operations) - utrzymanie niezbędnych usług systemu informatycznego po poważnej awarii w centrum informatycznym, która może być spowodowana przyczynami naturalnymi, takimi jak pożar lub trzęsienie ziemi, lub zdarzeniami wywołanymi umyślnie, np. sabotażem

1.4 Powołania normatywne

Wdrożony w Akademii Pomorskiej System Zarzadzania Bezpieczeństwem Informacji (SZBI) jest zgodny z międzynarodowymi normami:

- **ISO/IEC 27001:2013**; Techniki informacyjne — Techniki bezpieczeństwa — System zarzadzania bezpieczeństwem informacji — Wymagania
- **ISO/IEC 17799:2005**, Information technology — Security techniques — Code of practice for information security management

1.5 Infrastruktura systemu teleinformatycznego Uczelni

Istniejąca struktura teleinformatyczna Akademii Pedagogicznej w Słupsku opiera się o sieć podłączoną do naukowo-akademickiej sieci światłowodowej **PIONIER**. Uczelnia od 2006 roku jest fizycznie podłączona do sieci PIONIER dzięki podpisanej umowie z TASK (Trójmiejska Akademicka Sieć Komputerowa)
Do informatycznej sieci naukowej podłączonych jest ponad 700 urządzeń (komputery, drukarki, skanery), oraz około 300 urządzeń w akademikach. Cała sieć pracuje w technologii Ethernet. Szkielet sieci stanowi światłowód w technologii jednomodowej łączący wszystkie budynki Uczelni rozmieszczone w całym mieście (wszystkie światłowody pracują na urządzeniach o przepustowości j/w 1 GB).
Styk sieci uczelnianej z siecią PIONIER realizowany jest łączem o przepustowości 1GB w technologii Ethernet i zlokalizowany jest w węźle sieci W1 w budynku przy ul. Arciszewskiego 22b. Pierwszymi urządzeniami do obsługi routingu są CISCO Catalyst 3550 oraz CiSCO Catalyst 2970, które służą do dystrybucji sygnały do poszczególnych węzłów sieci w technologii 1 GB z wykorzystaniem WLAN.

W sieci Uczelni można wyróżnić następujące podsieci logiczne

- sieć naukowa
- sieć studencka
- sieć administracji

Węzły sieci szkieletowej znajdują się każdym budynku Uczelni. Usługa dystrybucji sygnału w poszczególnych węzłach sieci naukowej realizowana jest na urządzeniach HUAWAI S3900.

WĘZŁY SIECI:

A) **Węzły sieci przy ul. Westerplatte 64 (W12) (parter, p. 04)**

Węzeł sieci dystrybucyjnej (W3-DY)
Węzeł dostępowy (W13-DO):

- Instytut Pedagogiki,
- Katedra Socjologii i Pracy Socjalnej ,

Węzeł dostępowy (W12-DO):

- Instytut Nauk o Zdrowia,

B) **Węzły sieci przy ul. Arciszewskiego 22b (Wydziała MP) (W1) (pok. 104, piętro 1)**

Węzeł sieci dystrybucyjnej (W1-DY)
Węzeł dostępowy (W1-DO):

- Instytut Biologii i Ochrony Środowiska,
- Instytut Fizyki ,

Węzeł dystrybucyjny (W1-DY):

- główny węzeł dystrybucyjny sieci do węzłów.

C) **Węzły sieci przy ul . Arciszewskiego 22a (pok. 41 , piętro 1)**

Węzeł sieci dystrybucyjnej (W3-DY)
Węzeł sieci dostępowej(W3-DO):

- Instytut Historii i Politologii,
- Instytut Polonistyki ,

D) **Węzły sieci przy ul. Arciszewskiego 22c**

Węzeł sieci dystrybucyjnej (W8-DY)

Węzeł sieci dostępowej (W8-DO):

- Biblioteka Główna

E) **Węzły sieci przy ul. Arciszewskiego 22d (KBN)**

Węzeł sieci dystrybucyjnej (W9-DY)

Węzeł sieci dostępowej (W10-DO):

- Katedra Bezpieczeństwa Narodowego

F) **Węzeł sieci przy ul. Partyzantów**

Węzeł sieci dostępowej(W15-DO):

- Instytut Geografii.
- Instytut Muzyki

G) **Węzeł sieci przy ul. Słowiańskiej**

Węzeł sieci dostępowej(W14-DO):

- Instytut Neofilologii,

H) **Węzeł sieci przy ul. Kozietulskiego 6-7**

Węzeł sieci dostępowej(W16-DO):

- Instytut Matematyki,
- Instytut Nauk o Zdrowia,

SERWEROWNIE:

A) **Arciszewskiego 22b**

Serwery WWW, Storage sieciowy QNAP, poczta WWW, Legitymacja Studencka,

Lista serwerów:

- Serwery rackowe IBM x 3 szt. (usługi WWW, poczta e-mail),
- Qnap serwer (storage sieciowy),
- Serwer rack – legitymacja studencka,
- Serwer desktop – zarządzanie centralami telefonicznymi,
- Serwer rack MAXDATA – (usługi WWW),
- Serwer Desktop – brama główna sieci naukowej

B) **Arciszewskiego 22a**

Serwery Administracji, Wirtualny Dziekanat, system HMS

Lista serwerów:

- LACIE (storage sieciowy),
- Serwer rack – bramki dostępowe,

C) **Arciszewskiego 22c**

Serwery Biblioteki Głównej

Lista serwerów:

- Serwer do gromadzenia i udostępniania zasobów bibliotecznych
- 1 serwer brama główna sieci bibliotecznej
- 1 serwer PROLIB
- 1 serwer kopii zapasowych

D) **Arciszewskiego 22d**

Serwery Katedry Bezpieczeństwa Narodowego

Lista serwerów:

- Serwery KBN (GIS)

E) **Westerplatte 64**

Serwery ICT Moodle, Serwery WWW, Plany zajęć.

Lista serwerów:

- Serwery rackowe ITANIUM 64 x 18 szt. (ICT, WWW, usługi sieciowe, monitorowanie usług, statystyki, dostęp VPN, usługi DNS),
- Serwery rackowe IBM x 4 szt. (ICT, WWW),
- Serwer desktop (Solar Optima)
- Serwery rackowe IBM x 2 szt. (Wirtualny Dziekanat, Rekrutacja, HMS, FK),
- Wirtualizator SOA

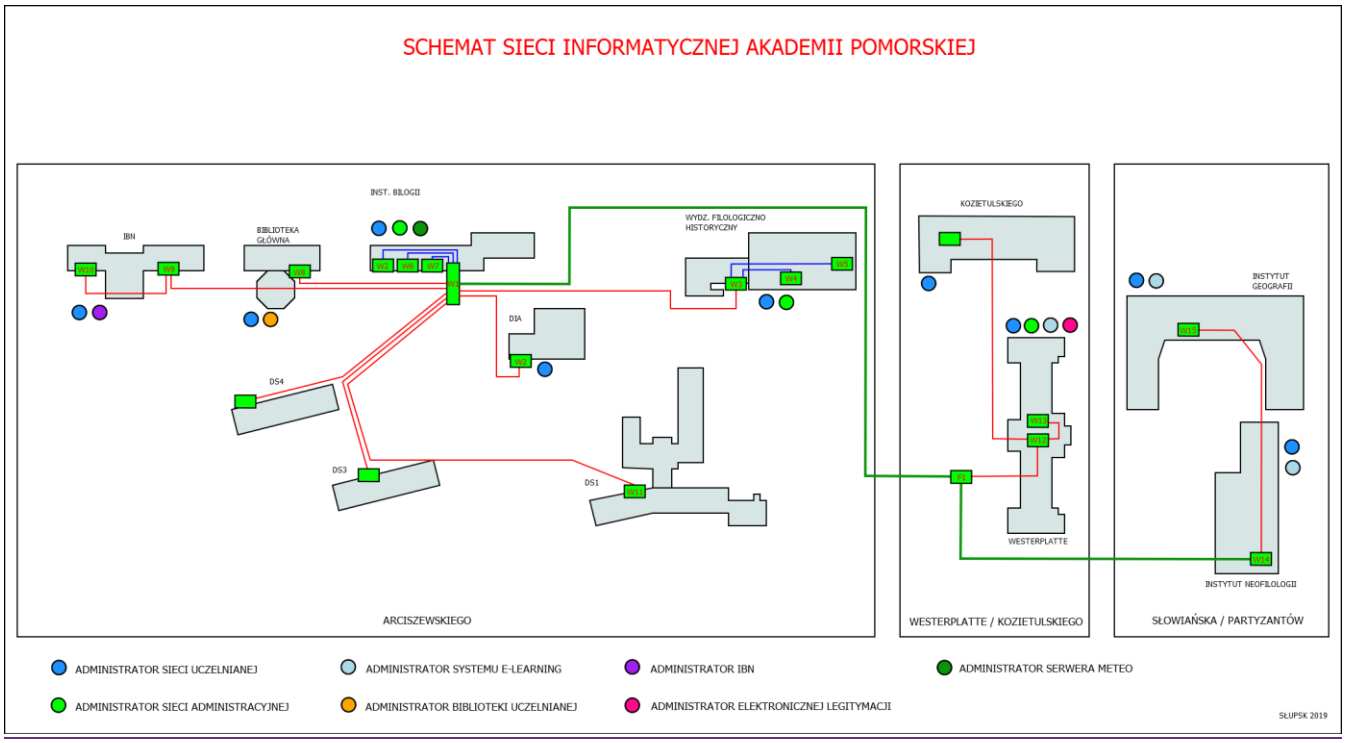
F) **Słowiańska 8**

Lista serwerów:

- Serwer Domeny Windows Zakładu Informatyki,
- 2 x Serwery WWW

SIEĆ BEZPRZEWODOWA:

Na Uczelni funkcjonuje system bezprzewodowego dostępu do Internetu EDUROAM w którym pracuje ponad 90 urządzeń firm CISCO i UBIQUITI. Umożliwia on dostęp do sieci tylko zarejestrowanym użytkownikom.



Rys. 1 *Schemat infrastruktury informatycznej Akademii Pomorskiej*

2. SYSTEM ZARZĄDZANIA BEZPIECZENSTWEM INFORMACJI

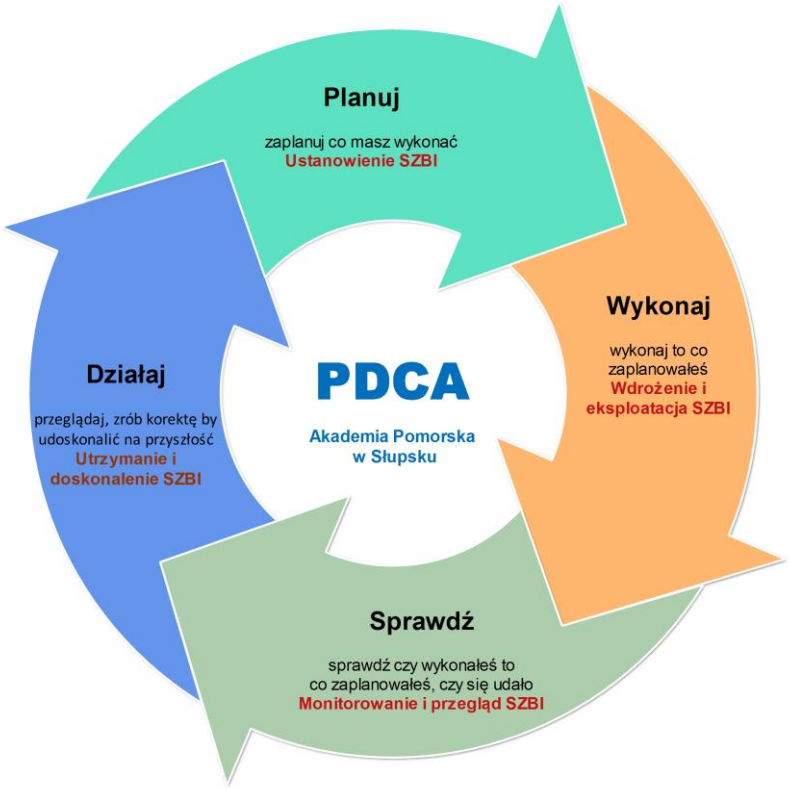
2.1 Postanowienia ogólne

Akademia Pomorska opracowała, wdrożyła, stosuje, monitoruje, przegląda, utrzymuje i doskonali udokumentowany SZBI w kontekście całościowych działań biznesowych i ryzyka, które występują na Uczelni.

Wdrożenie Systemu Zarzadzania Bezpieczeństwem Informacji zgodnego z postanowieniami międzynarodowej normy ISO 27001:2013 jest strategiczna decyzją Akademii Pomorskiej. Zastosowano procesowe podejście dla ustanawiania, wdrażania, stosowania, monitorowania, przeglądania, utrzymywania i doskonalenia Systemu Zarzadzania Bezpieczeństwem Informacji.

Zastosowany proces opiera się na modelu Deminga **PDCA** (Planuj ⇨ Wykonaj ⇨ Sprawdź ⇨ Działaj).

- Planuj - (ang. **P**lan) zapisz co zaplanowałeś wykonać
- Wykonaj - (ang. **D**o) wykonaj to co zaplanowałeś, zrób to
- Sprawdź - (ang. **C**heck) sprawdź czy wykonałeś to co zaplanowałeś, czy się udało
- Działaj - (ang. **A**ct) przeglądaj, zrób korektę by udoskonalić na przyszłość



Rys. 2 *Pętla Deminga PDCA w odniesieniu do SZBI Akademii Pomorskiej*

Działanie SZBI na Uczelni jest procesem ciągłym, stale doskonalonym i dostostosowywanym do zmieniających się okoliczności. Każdy z etapów dzieli się na bardziej szczegółowe działania, które dotyczą przede wszystkim polityki bezpieczeństwa, zarządzania zasobami i ryzykiem. Scalenie wszystkich działań w ciągły proces bezpiecznego zarządzania informacją, pozwoli na:

- Minimalizację ryzyka wycieku/utraty cennych dla Uczelni danych;
- Wzrost poziomu bezpieczeństwa informacji na Uczelni;
- Zapewnienie ciągłości funkcjonowania Uczelni;
- Wzrost konkurencyjności Uczelni na rynku;
- Postrzeganie Uczelni jako wiarygodnego, nowoczesnego, a przede wszystkim bezpiecznego partnera;
- Określenie podstawowych zasad związanych z bezpiecznym przetwarzaniem informacji;
- Określenie zasad postępowania w sytuacjach awaryjnych;
- Zapewnienie bezpieczeństwa prawnego, przez spełnienie wymagań prawa w zakresie ochrony informacji.

2.2 Zasady ogólne

Każdy pracownik Uczelni jest zapoznawany z regułami oraz z aktualnymi procedurami ochrony informacji w swojej komórce organizacyjnej. Poniższe uniwersalne zasady są podstawą realizacji polityki bezpieczeństwa informacji:

1. **Zasada uprawnionego dostępu.** Każdy uprawniony pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i o ile tyczy to danych osobowych podpisał stosowne oświadczenie o zachowaniu poufności.
2. **Zasada przywilejów koniecznych**. Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
3. **Zasada wiedzy koniecznej**. Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
4. **Zasada usług koniecznych**. Uczelnia świadczy tylko takie usługi jakich wymaga jej statut.
5. **Zasada asekuracji**. Każdy mechanizm zabezpieczający musi być ubezpieczony drugim, innym. W przypadkach szczególnych może być stosowane dodatkowe niezależne zabezpieczenie.
6. **Zasada świadomości zbiorowej**. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych Uczelni i aktywnie uczestniczą w tym procesie.
7. **Zasada indywidualnej odpowiedzialności**. Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
8. **Zasada obecności koniecznej**. Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
9. **Zasada stałej gotowości**. System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.

10. **Zasada kompletności**. Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
11. **Zasada odpowiedniości**. Używane mechanizmy muszą być adekwatne do sytuacji.
12. **Zasad akceptowanej równowagi**. Podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji.

2.3 Definicja bezpieczeństwa informacji

Utrzymanie bezpieczeństwa przetwarzanych przez Akademię Pomorską informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.

Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:

- **Poufność informacji** - rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
- **Integralność informacji** - rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
- **Dostępność informacji** - rozumiana jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
- **Zarządzanie ryzykiem** – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.

Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:

- **Niezaprzeczalności odbioru** - rozumianej jako zdolność systemu Akademii Pomorskiej do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,
- **Niezaprzeczalności nadania** - rozumianej jako zdolność systemu Akademii Pomorskiej do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie.
- **Rozliczalności działań** – rozumianej jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania wykonał.

Ilekroć w dokumencie jest mowa o:

- **RODO** - ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 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 (ogólne rozporządzenie o ochronie danych)

- **Inspektor Ochrony Danych** (Inspektor) - to osoba, której Administrator Danych Osobowych wyznaczył pełnienie obowiązków Inspektor Ochrony Danych w odniesieniu do systemu nadzoru nad informacją (aktywami) w odniesieniu do systemów informatycznych;
- **Administratorze Systemów Informatycznych** (ASI) - rozumie się przez osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków Administratora Systemów Informatycznych w odniesieniu do systemu nadzoru nad informacją (aktywami) funkcjonującą w systemach informatycznych;
- **Administrator Danych Osobowych** (ADO) -- osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych
- **danych –** rozumie się przez to dane będące w posiadaniu Uczelni w postaci elektronicznej lub w innej formie, będące w zbiorach Uczelni, wykorzystywane przez Akademię Pomorską lub osoby trzecie , a niezbędne do wykonywania zadań Akademii Pomorskiej;
- **danych osobowych** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- **szczególnych kategorii danych osobowych** - rozumie się przez to dane określone w art. 9 ut,1 oraz art. 10 RODO, a więc dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;
- **haśle** - rozumie się przez to co najmniej 8-znakowy ciąg znaków literowych, cyfrowych, zawierający duże i małe litery oraz znaki specjalne, znany jedynie osobie uprawnionej do pracy w systemie informatycznym, Administratorowi Danych Osobowych oraz Administratorowi Systemu Informatycznego
- **identyfikatorze użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w wyznaczonych przez administratora danych osobowych obszarach systemu informatycznego Akademii Pomorskiej;
- **incydent bezpieczeństwa** – czynności, zjawiska naruszające zapisy Polityki Bezpieczeństwa Informacji oraz jej procedury mogące zagrozić utracie aktywów Akademii Pomorskiej, ich integralności lub dostępności, a także dopuścić do nieuprawnionego dostępu do danych, jednoznaczne z sytuacją kryzysową;
- **procedurach ochrony danych osobowych** – rozumie się przez to sposób przetwarzania danych osobowych oraz warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych w taki sposób, by zachować ich tajemnicę, zapewnić ochronę przed zniszczeniem i kradzieżą, określone wymogami wynikające z przeprowadzonego szacowania ryzyka przetwarzania danych osobowych ,
- wymogami niniejszej Instrukcji;

- **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, wprowadzanie do systemu Akademii Pomorskiej, przechowywanie, opracowywanie, zmienianie, usuwanie i udostępnianie;
- **serwerze** - rozumie się przez to jednostkę centralną, komputer zarządzający systemem informatycznym Akademii Pomorskiej;
- **Uczelni** - identyfikuje się jako Akademię Pomorską w Słupsku;
- **służbach informatycznych Uczelni** - rozumie się przez to informatyków zatrudnionych w Akademii Pomorskiej;
- **systemie informatycznym Uczelni** - rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych. W systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną Uczelni;
- **systemy przetwarzania informacji** tzn. informacje mogą być przetwarzane wyłącznie w systemach, które spełniają warunki opisane w PBI;
- **sytuacją kryzysową** - jest to wystąpienie, zagrożenie lub domniemanie kradzieży, nieautoryzowanego dostępu, modyfikacji, zatajenia lub utraty (zniszczenia) przetwarzanej w systemie informacji zastrzeżonej. Każdy system informatyczny (SI) powinien przechodzić okresowe audyty bezpieczeństwa;
- **użytkowniku** - rozumie się przez to pracownika Akademii Pomorskiej, zatrudnionego na podstawie umowy o pracę, umowy zlecenia lub innej umowy przewidzianej przepisami prawa oraz osobę odbywającą na Uczelni staż absolwencki, praktykę studencką, wolontariat, który przetwarza dane osobowe znajdujące się w zbiorach danych Uczelni;
- **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych osobowych, dostępnych wg określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

2.4 Zakres działania administratorów Akademii Pomorskiej

Ze względu na strukturę organizacyjną Uczelni, podział logiczny sieci teleinformatycznej oraz posiadane zasoby bazodanowe można wyodrębnić następujących administratorów:

Administrator	Jednostka organizacyjna	Zakres działania
Sieci Uczelnianej	Sekcja Informatyki	WWW, FTP, DHCP, poczta, nadzór nad strukturą i podziałem logicznym sieci
Sieci Administracyjnej	Sekcja Informatyki	HMS (FK, płace, kadry, dziekanat, DS, BFP), eHMS (wirtualny dziekanat, rekrutacja), jHMS (limity, polon)
Systemu e-Learning	Sekcja Informatyki	poczta, Moodle
EDUROAM	Sekcja Informatyki	
Biblioteki Uczelnianej	Biblioteka Uczelniana	Prolib, OPAC
Systemów IBN	Instytut Bezpieczeństwa Narodowego	GIS

Serwera Meteo	Instytut Fizyki	System zbierający dane meteorologiczne
Elektronicznej Legitymacji	Sekcja Informatyki	SELS - OPTICamp

2.5 System Helpdesk

W podstawowej funkcjonalności Helpdesk IT jest punktem obsługi zdarzeń zgłoszonych przez użytkowników końcowych Uczelni oraz przez systemy monitorujące. System realizuje pełny cykl życia zgłoszenia od rejestracji, przez obsługę, a kończąc na zamknięciu zgłoszenia.

System Helpdesk IT został zbudowany w oparciu o rozwiązania open-source *„GLPI”* które jest rozpowszechniane na darmowej licencji GNU/GPL ver. 2 . Aplikacja ta działa w przeglądarce internetowej, co pozwala na uniknięcie instalowania dodatkowych elementów na komputerach użytkowników. Dzięki szerokiej gamie uprawnień przypisywanych użytkownikom możliwe jest szczegółowe zdefiniowanie obszarów, do których pracownicy Uczelni mają dostęp.

Przyjmowanie zgłoszeń od użytkowników następuje przez zarejestrowanie zgłoszenia poprzez formularz wypełniany w przeglądarce internetowej. Użytkownicy mają podgląd na zgłoszenia, które są obsługiwane w danej chwili, jak również zgłoszenia historyczne.

Administratorem systemu Helpdesk jest Sekcja Informatyki, która na wniosek użytkownika przydziela mu login i hasło dostępowe do systemu. Helpdesk dostępny jest z sieci wewnętrznej Akademii Pomorskiej i z jej zewnętrznej puli adresowej IP pod adresem: http://helpdesk.apsl.edu.pl

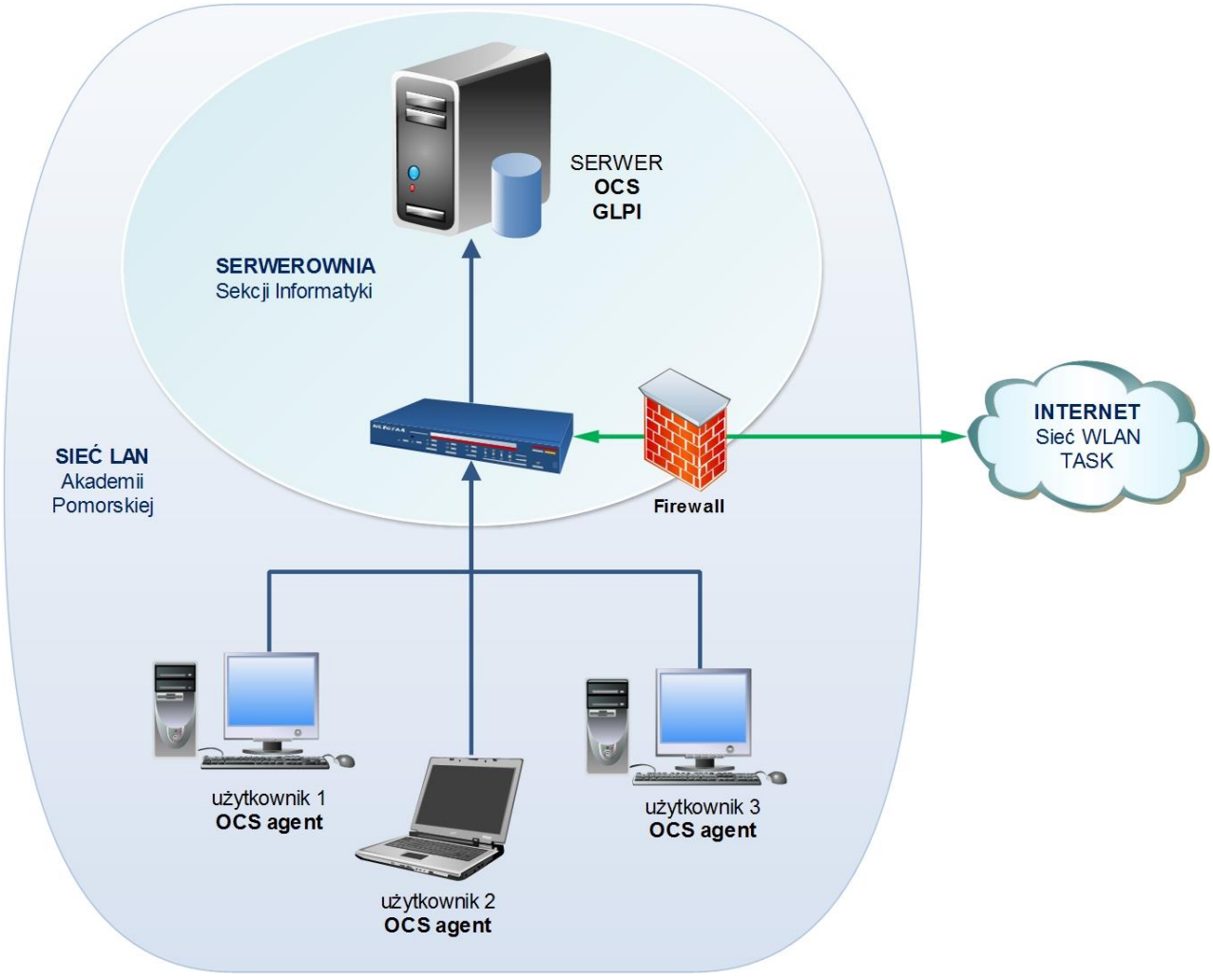
2.5 Audyt sprzętu i oprogramowania

W systemie teleinformacyjnym Akademii Pomorskiej w Słupsku jest zainstalowany i wdrożony system do automatycznego wykonywania audytu sprzętu i zainstalowanego oprogramowania „*OCS Inventory NG*” oparty o rozwiązania open-source. System działa w architekturze klient (agent) – serwer i służy do automatycznego zbierania informacji z podłączonych do sieci Uczelnianej urządzeń.

Oprogramowanie „*OCS Inventory NG*” ściśle współpracuje z opisanym w punkcie 2.5 programem „*GLPI*”. Systemem audytu sprzętu i oprogramowania administruje Sekcja Informatyki AP.

1. Systemowi audytu sprzętu i oprogramowania podlega każdy komputer którego właścicielem jest Uczelnia i który został podłączony do sieci teleinformatycznej AP
2. Na każdym komputerze podłączonym do sieci IT Uczelni należy zainstalować i uruchomić „Agenta OCS” za co odpowiadają ASI poszczególnych podsieci
3. „Serwer OCS” zbiera informacje z zainstalowanych „Agentów OCS”, co jest podstawą do wygenerowania „karty komputera” i przekazania jej użytkownikowi (kierownikowi jednostki)

4. Użytkownik nie ma prawa samodzielnie odinstalować lub dezaktywować „Agenta OCS”
5. Na wniosek pełnomocnika BSI lub ASI czy Inspektora, użytkownik ma obowiązek odinstalować oprogramowanie które zostało zdiagnozowane jako „nielegalne”
6. Komputery incydentalne, podłączane za wiedzą ASI ale nie będące środkami trwałymi AP, nie podlegają audytowi za pomocą „Agenta OCS”. Takie komputery są rejestrowane i autoryzowane w systemie za pomocą ASI



Rys. 3 *Schemat podłączenia „Agentów OCS” w sieci AP do „Serwera OCS”*

3. INSTRUKCJA BEZPIECZEŃSTWA

3.1 Opis zdarzeń naruszających ochronę danych

Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona - nie dochodzi do naruszenia poufności danych.
2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu - może nastąpić naruszenie poufności danych.
3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
   - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
   - nieuprawniony dostęp do systemu z jego wnętrza,
   - nieuprawniony przekaz danych,
   - pogorszenie jakości sprzętu i oprogramowania,
   - bezpośrednie zagrożenie materialnych składników systemu.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,

9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub kopiowano dane osobowe,
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach, pendrive czy przenośnych dyskach HD w formie niezabezpieczonej itp.

3.2 Bezpieczeństwo fizyczne i środowiskowe

3.2.1. Fizyczne zabezpieczenie wejścia do pomieszczeń

Strefy bezpieczeństwa takie jak serwerownie, wydzielone klasopracownie są zabezpieczone przed dostępem osób nieuprawnionych poprzez stosowanie zabezpieczeń fizycznych i proceduralnych typu:

- alarmy z kodami zał./wył (PIN),
- zamki i karty dostępu,
- zamykane na klucz szafy, szafki itp.

3.2.2. Zabezpieczenie biur, pomieszczeń i urządzeń IT

Zabezpieczenie biur, pomieszczeń i urządzeń realizowane jest przez stosowanie zabezpieczeń fizycznych i proceduralnych wskazanych w pkt. 3.2.1.
Na Akademii Pomorskiej w Słupsku pomieszczenia ogólnodostępne i tzw. strefy bezpieczeństwa (o szczególnym nadzorze takie jak serwerownie czy klasopracownie), po opuszczeniu pomieszczeń należy zakodować alarm za pomocą PIN lub karty dostępu, oraz zamknąć pokój na klucz.

Klucze zapasowe do pomieszczeń w strefach bezpieczeństwa – przechowywane są w kasetce metalowej na portierni. W zakresie kluczy do szaf, szafek, szuflad w pomieszczeniach biurowych obowiązuje indywidualna polityka zarządzania tymi kluczami z zachowaniem zasady, że ktoś kto nie powinien mieć do nich dostępu nie wie gdzie są przechowywane. Generalnie na biurku czy szafce nie powinno być nic – prócz aktualnie wykorzystywanych dokumentów i sprzętu.

3.2.3. Zabezpieczenie przed zagrożeniami zewnętrznymi i środowiskowymi

Ochrona fizyczna przed zagrożeniami zewnętrznymi i środowiskowymi jest zaplanowana i wdrożona. We wszystkich budynkach AP są gaśnice oraz instrukcje bezpieczeństwa przeciwpożarowego.

Należy pamiętać, że nie wolno pozostawiać włączonego sprzętu IT bez nadzoru poza godzinami pracy – w szczególności w godzinach nocnych. Wyjątkiem są pomieszczenie specjalnie do tego celu przygotowane takie jak serwerownie z działającą klimatyzacją

3.2.4. Urządzenia podtrzymujące napięcie

Sprzęt jest chroniony przed awariami zasilania i innymi zakłóceniami elektrycznymi poprzez:

- Zapewnienie odpowiednich warunków atmosferycznych w pomieszczeniu, w którym znajdują się serwery poprzez zastosowanie klimatyzatorów.
- Urządzenia podtrzymujące zasilanie UPS przy każdym stanowisku komputerowych o ile jest to wskazane.
- Listwy przeciwprzepięciowe przy każdym stanowisku komputerowym
- Urządzenia podtrzymujące UPS w serwerowniach w ilości uzasadnionej topologią sieci

3.2.5. Bezpieczeństwo okablowania

Kable zasilające i sieciowe są schowane, tak aby zabezpieczyć je przed uszkodzeniem. Są stosowane oznaczenia kabli, gniazdek oraz jest zachowana rozdzielność kabli sieciowych, zasilających i telekomunikacyjnych.

3.2.6. Zabezpieczenie sprzętu poza siedzibą Uczelni

Obowiązuje zasada, że sprzęt i nośniki nie są wynoszone poza siedzibę Uczelni. W szczególnych przypadkach sprzęt IT jest wydawany po wypełnieniu odpowiedniego rewersu który jest ewidencjonowany w jednostkach organizacyjnych zarządzających danym sprzętem. W przypadku osób upoważnionych lub uprzywilejowanych obowiązują pewne zasady postępowania w celu zapewnienia bezpieczeństwa informacji.

1. Osoba używająca komputer przenośny zawierający dane osobowe zobowiązana jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych na Uczelni.
2. Osoba używająca komputer przenośny zawierający dane osobowe w szczególności powinna:
    - stosować ochronę kryptograficzną wobec danych osobowych przetwarzanych na komputerze przenośnym.
    - zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego - identyfikator i hasło.
    - nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych.

- nie wykorzystywać komputera przenośnego do przetwarzania danych osobowych w obszarach użyteczności publicznej.
- zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych.

3. W przypadku podłączania komputera przenośnego do sieci publicznej poza siecią Akademii Pomorskiej w Słupsku należy zastosować firewall zainstalowany bezpośrednio na tym komputerze oraz system antywirusowy.
4. Użytkownik powinien zachować wyjątkową ostrożność podczas korzystania z zasobów sieci publicznej.
5. Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego formalny użytkownik.

3.3 Kontrola dostępu

Dostęp do serwerowni i chronionych pomieszczeń mogą mieć jedynie osoby upoważnione, posiadające poświadczenie bezpieczeństwa (jeśli jest taki wymóg) oraz aktualny PIN czy kartę dostępu w zakresie dostępu do zasobów informacyjnych sieci informatycznej Uczelni.

W infrastrukturze IT Uczelni istnieje sześć serwerowni do których dostęp jest szczególnie rygorystyczny i oprócz dezaktywacji alarmu wymaga karty dostępowej (zamek elektroniczny).

1. Główna serwerownia styku Uczelnia i sieć PIONIER – ul. Arciszewskiego 22b
2. Serwerownia przy ul Westerplatte 64
3. Serwerownia Administracyjna – ul. Arciszewskiego 22a
4. Serwerownia Studium Informatyki – ul. Słowiańska
5. Serwerownia Biblioteki Uczelnianej – ul. Arciszewskiego 22c
6. Serwerownia Instytutu Bezpieczeństwa Narodowego – ul. Arciszewskiego 22d

3.4 Ochrona antywirusowa

1. Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.
2. Oprogramowanie antywirusowe powinno być zainstalowane tak aby użytkownik nie był w stanie wyłączyć lub pominąć etapu skanowania.
3. Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
4. Należy stosować wersje programów antywirusowych z aktualną bazą sygnatur wirusów.
5. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instalują Administratorzy Systemu Informatycznego (ASI) niezwłocznie po ich otrzymaniu lub ściągnięciu, uprzednio weryfikując pochodzenie oprogramowania.
6. Administratorzy Systemu mają prawo odłączyć od sieci stację roboczą, na której zostanie zlokalizowany wirus, jeśli uznają, że dalsze pozostawienie go w sieci zagraża innym stacjom roboczym.

7. Użytkownik systemu na stanowisku komputerowym, importujący dane osobowe do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów.

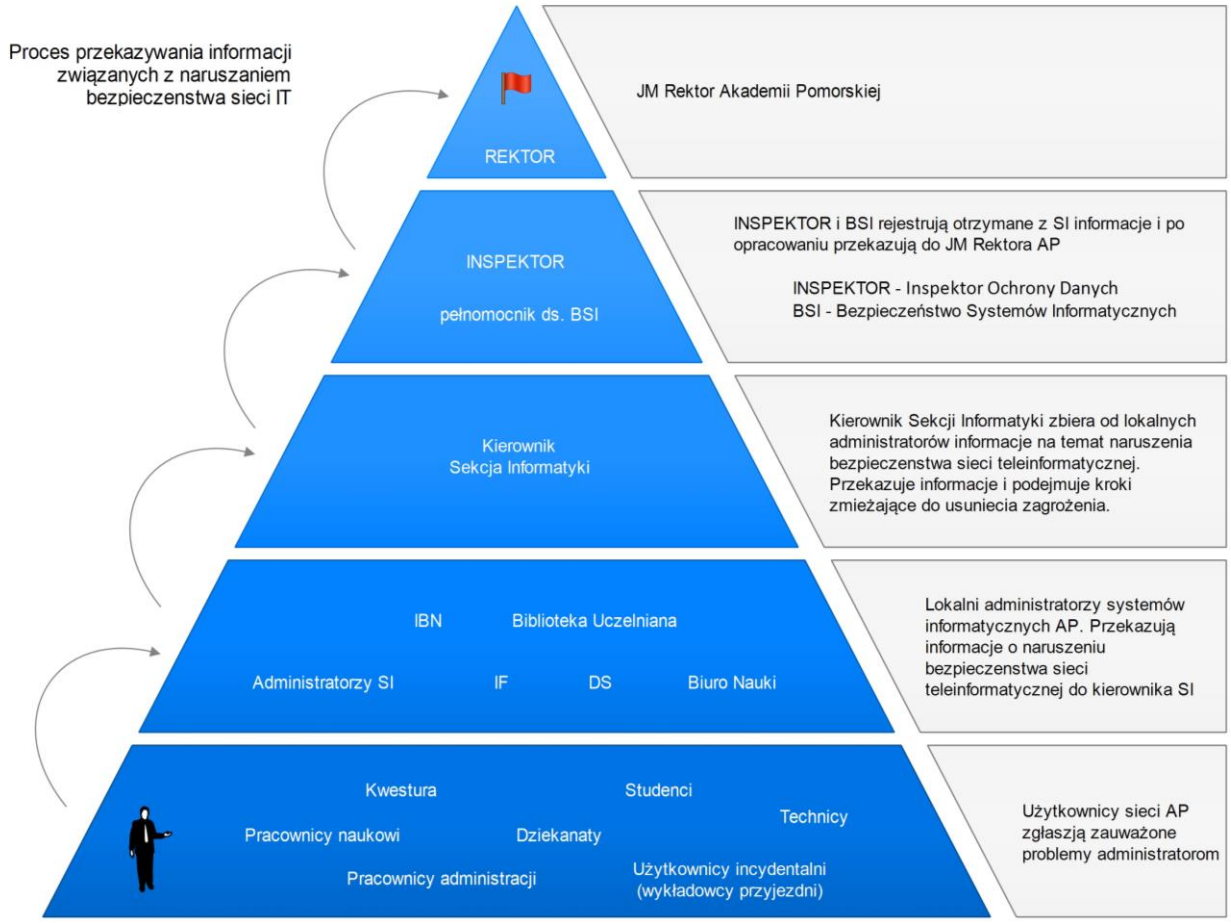
3.5 Postępowanie przy stwierdzeniu zdarzeń naruszających bezpieczeństwo informacji

Instrukcja

1. Użytkownik zobowiązany jest powiadomić Administratora Systemów Informatycznych lub uprzednio wskazanego przez niego pracownika służb informatycznych Uczelni o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:
   - naruszeniu identyfikatora i hasła (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),
   - częściowym lub całkowitym braku danych,
   - braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
   - wykryciu wirusa komputerowego,
   - zauważeniu elektronicznych śladów próby włamania do systemu informatycznego Uczelni,
   - podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
   - zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf
2. Do czasu przybycia na miejsce Administratora Systemów Informatycznych należy:
   - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, o ile istnieje taka możliwość,
   - następnie uwzględnić w działaniu również ustalenie jego przyczyn i sprawców,
   - rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   - zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   - zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
   - udokumentować w formie dokumentacji urzędowej wstępnie zaistniałe naruszenie,
   - nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia Administratora Systemów Informatycznych.
3. Administrator Systemów Informatycznych po otrzymaniu zawiadomienia, o którym mowa w ust.1, powinien niezwłocznie:
   - przeprowadzić postępowanie wyjaśniające, w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
   - podjąć działania chroniące system przed ponownym naruszeniem,
   - w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu, sporządzić raport naruszenia bezpieczeństwa systemu informatycznego Akademii Pomorskiej (wg zatwierdzonego wzoru załącznik nr 1)

4. W dalszym trybie postępowania należy, przekazać sporządzony raport do Sekcji Informatyki AP oraz podjąć inne, szczególne czynności zapewniające bezpieczeństwo systemu informatycznego Akademii Pomorskiej, bądź podjąć środki ochrony fizycznej.
5. Kierownik Sekcji Informatyki jest zobowiązany do informowania ADO i Inspektor o awariach systemu informatycznego Uczelni, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników danych, w szczególności o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania programów antywirusowych, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.
6. Inspektor, przekazuje po przeanalizowaniu i zarejestrowaniu raportu na temat naruszenia bezpieczeństwa systemu informatycznego Uczelni J.M Rektorowi.

Proces przekazywania informacji na temat zaistniałego incydentu związanego z naruszeniem bezpieczeństwa systemu informatycznego Uczelni obrazuje poniższy diagram na rysunku nr 3.



Rys. 4 *Piramida przepływu informacji związanych z naruszeniem bezpieczeństwa IT*

3.6 Rozpoczęcie, zawieszenie i zakończenie pracy w systemie IT

Przed przystąpieniem do pracy z systemem, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest postępować zgodnie z procedurą opisaną w punkcie 3.5 niniejszej instrukcji.

3.6.1. Procedura rozpoczęcia pracy w systemie IT

1. Uruchomić komputer wchodzący w skład systemu informatycznego Uczelni, który jest podłączony fizycznie do sieci lokalnej lub wydzielonej i załogować się podając identyfikator i hasło dostępu do odpowiedniego zasobu IT Uczelni.
2. Uruchomić wybraną aplikację (w szczególności aplikację bazodanową m.in. przetwarzającą dane osobowe).
3. Zalogować się do aplikacji za pomocą przydzielonego przez ASI loginu i hasła uwierzytelniającego.

3.6.2. Procedura zakończenia pracy w systemie IT

1. W trakcie pracy, przy każdorazowym opuszczeniu stanowiska komputerowego, dopilnować, aby na ekranie nie były wyświetlane dane osobowe,
2. Przy opuszczaniu pokoju na dłuższy czas ustawić ręcznie blokadę klawiatury i wygaszacz ekranu.

3.6.3. Procedura zakończenia pracy w systemie IT

1. Zamknąć aplikację,
2. Zamknąć system,
3. Wyłączyć monitor i ewentualnie drukarkę.

Nie wolno bez nadzoru pozostawiać po godzinach pracy włączonego sprzętu IT.

4. POLITYKA BEZPIECZEŃSTWA INFORMACJI AP

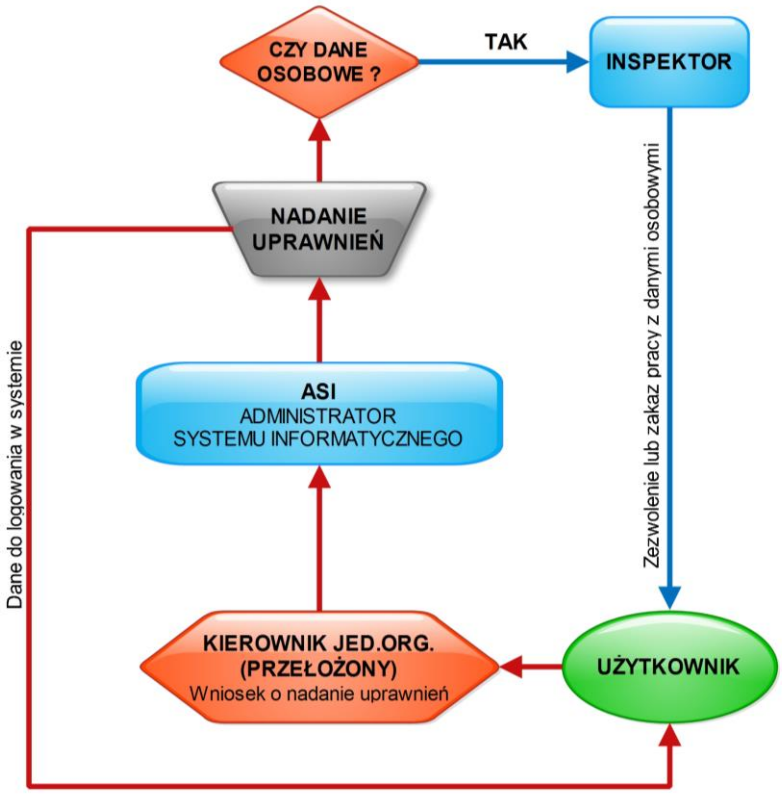
4.1 Polityka szacowania ryzyka

Polityka szacowania ryzyka związanego z bezpieczeństwem informacji stanowi odrębny dokument związany z niniejszym SZBI …….. Polityka zawiera metodologię szacowania ryzyka oraz podejście do szacowania ryzyka z uwzględnieniem bezpieczeństwa informacji w kontekście biznesowym oraz wymagań prawnych.

Celem Polityki szacowania ryzyka jest zapewnienie, że metodyka szacowania ryzyka przyjęta w Akademii Pomorskiej jest spójna ze zidentyfikowanymi wymaganiami biznesowymi i prawnymi w zakresie ochrony bezpieczeństwa informacji, zawiera kryteria akceptacji ryzyka i że zapewnia uzyskanie porównywalnych wyników w całej organizacji podczas kolejnych szacowań ryzyka.

4.2 Proces nadawania uprawnień użytkownikom systemów IT

Rozdział ten zawiera podstawowe informacje o procedurach nadawania, zmiany oraz rejestracji uprawnień do przetwarzania danych przyjętych do stosowania w systemach informatycznych Akademii Pomorskiej w Słupsku.



Rys. 5 *Proces nadawania uprawnień użytkownikowi*

4.2.1 Zasady nadawania uprawnień

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych, zwłaszcza osobowych musi zapoznać się z :
    - **RODO -** ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 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 (ogólne rozporządzenie o ochronie danych)
    - Ustawą z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. z 2018r. ,poz. 1000),
    - Obowiązującą w Akademii Pomorskiej w Słupsku Polityką bezpieczeństwa informacji
    - Niniejszą instrukcją
2. Jedynie prawidłowo wypełniony wniosek przełożonego o nadanie uprawnień (załącznik nr 2) w systemie informatycznym Uczelni lub zmianę tych uprawnień jest podstawą rejestracji uprawnień w systemie.
3. Stosowany w Akademii Pomorskiej schemat uprawnień dostępu do zasobów informatycznych sieci LAN zakłada, iż użytkownicy uzyskują dostęp do sieci na pewnym, z góry zdefiniowanym poziomie.
4. Autoryzacja odbywa się na zasadzie autoryzowania sprzętu i jest w pełni automatyczna.
5. Niniejsza instrukcja przedstawia procesy związane z nadawaniem, zmianą i usuwaniem uprawnień dotyczących obsługi danych osobowych oraz innych newralgicznych systemów bazodanowych (np. e-learning, zasoby biblioteczne itp.)

4.2.2 Procedura nadawania uprawnień

1. Kierownik (przełożony) jednostki organizacyjnej:
    a. nadaje upoważnienie do przetwarzania danych osobowych osobie, która w związku z wykonywanymi przez siebie obowiązkami będzie miała dostęp do danych osobowych
    b. wypełnia i podpisuje wniosek nadania uprawnień dla osoby upoważnionej do przetwarzania danych osobowych (załącznik nr 2)
    c. przekazuje wypełniony dokument w postaci papierowej do ASI, w celu akceptacji
    d. w przypadku wniosku dotyczącego obsługi systemu z danymi osobowymi, ASI przekazuje go do Inspektora.
2. Inspektor sprawdza poprawność przesłanego wniosku oraz
    a. w przypadku braku uwag przekazuje go ze swoją adnotacją ASI, w celu nadania uprawnień użytkownikowi w systemie,
    b. w przypadku uwag, np. gdy użytkownik nie został zapoznany z przepisami o ochronie danych osobowych, przekazuje dokument do kierownika jednostki organizacyjnej od którego dokument otrzymał. Na dokumencie dokonuje adnotacji, w której podaje przyczynę odmowy zatwierdzenia dokumentu. Kroki 1 i 2 powtarza się do czasu uzyskania akceptacji dokumentu przez Inspektora.
3. ASI odpowiednio, zgodnie z przekazanym dokumentem:
    a. rejestruje użytkownika w systemie i nadaje mu określone uprawnienia
    b. generuje użytkownikowi tymczasowe hasło

c. informuje Inspektora o nadaniu uprawnień w celu aktualizacji ewidencji osób upoważnionych do przetwarzania danych osobowych w systemie

5. Użytkownik uwierzytelnia się w systemie,
6. Użytkownik zmienia nadane mu przez ASI hasło i rozpoczyna pracę w aplikacji.

Procedurę nadania uprawnień do przetwarzania danych osobowych w systemie należy stosować odpowiednio w przypadku zmiany uprawnień w systemie albo odebrania uprawnień w systemie

4.2.3 Ewidencjonowanie uprawnień

1. Inspektor w porozumieniem z Administratorem Systemów Informatycznych (ASI) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym, o której mowa 4.2.2, punkt 3c.
2. Ewidencja osób upoważnionych może przyjmować formę elektroniczną, w takim wypadku należy jednak zapewnić ograniczenie dostępu do ewidencji, do kręgu osób upoważnionych.
3. Ewidencja praw dostępu do sieci lokalnej jest prowadzona zgodnie z zasadami określonymi w odpowiedniej dokumentacji.

4.3 Bezpieczna eksploatacja systemów informatycznych

Bezpieczna eksploatacja systemów informatycznych przetwarzających wszelkiego rodzaju dane zostaje zapewniona poprzez przestrzeganie następujących zasad:

1. użytkownikom zabrania się wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie,
2. użytkownikom zabrania się umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych,
3. użytkownikom nie wolno instalować nowego lub aktualizować już zainstalowanego oprogramowania,
4. użytkownikom nie wolno korzystać z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych,
5. użytkownikom nie wolno podejmować prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona,
6. informacje przetwarzane przy użyciu współdzielonych aplikacji sieciowych na stacjach roboczych muszą być zapisywane na dyskach serwera,
7. wszystkie aplikacje sieciowe, współdzielone zasoby użytkowe muszą być ulokowane na przeznaczonych do tego celu serwerach.
8. nieautoryzowane podłączenie własnego lub strony trzeciej urządzenia teleinformatycznego do systemu informatycznego Akademii Pomorskiej w Słupsku jest zabronione.

4.4 Metody i środki uwierzytelnienia użytkownika w systemie informatycznym

1. Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych. Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.
2. Identyfikatory i hasła użytkownik uzyskuję w procesie opisanym w punkcie 4.2.2 niniejszej instrukcji
3. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:
    - Użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego i wyłącznego użytku.
    - Hasła dostępu do systemów informatycznych powinny być tworzone przez użytkownika i stanowią tajemnicę służbową, znaną wyłącznie temu użytkownikowi
    - Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie.
    - Hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności.
    - Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).
4. Użytkownicy są odpowiedzialni za wszelkie działania w systemach informatycznych prowadzone z użyciem ich identyfikatora i hasła.
5. Administratorzy Systemów Informatycznych (ASI) są odpowiedzialni za okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach za które są odpowiedzialni.
6. Administratorzy Systemu powinni przeprowadzać przegląd autoryzacji i uprawnień nie rzadziej niż co 6 miesięcy.
7. Administratorzy zakładają na stacjach roboczych specjalne konta (profile) służące do zarządzania daną stacją roboczą.

4.5 Wymogi dotyczące uwierzytelnienia

1. Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym, zaakceptowanym przez Inspektora sposobem uwierzytelniania.
2. Identyfikator oraz nadane uprawnienia powinny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków.
3. Identyfikator użytkownika powinien być niepowtarzalny a po wyrejestrowaniu się z systemu informatycznego nie powinien być przydzielany innej osobie.

4. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
5. Hasło początkowe, które jest przydzielane przez ASI, powinno umożliwiać użytkownikowi zarejestrowanie się w systemie **tylko jeden raz** i powinno być natychmiast zmienione przez użytkownika.
6. Użytkownicy powinny wybierać hasła dobrej jakości:
   - długości co najmniej 8 znaków,
   - które są łatwe do zapamiętania, a trudne do odgadnięcia,
   - nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, data urodzenia itp.),
   - w których występuje przynajmniej jedna duża litera, jedna mała litera, jedna cyfra lub znak specjalny,
   - w których nie występują kolejne znaki, które nie są topologiczne (tzn. wynikające z układu klawiszy na klawiaturze, typu „qwer6., „zaq1xsw2CDE#. itp.).
7. Hasła nie mogą być takie same jak identyfikator użytkownika oraz nie mogą być zapisywane w systemach w postaci jawnej.
8. Hasła powinny być utrzymywane w tajemnicy również po upływie ich ważności.
9. Należy unikać ponownego lub cyklicznego używania starych haseł.
10. Rutynowe działania użytkownika nie powinny być prowadzone z wykorzystaniem kont uprzywilejowanych.
11. Udostępnienie hasła osobie postronnej należy traktować jako poważny incydent naruszenia ochrony danych osobowych.

4.6 Wymogi dotyczące zmiany haseł

1. Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:
   - Okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła).
   - W przypadku ujawnienia lub podejrzenia ujawnienia hasła.
2. W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się znajduje, użytkownik zobowiązany jest wystąpić o zmianę hasła do właściwego ASI, w sytuacji:
   - Zapomnienia/zgubienia hasła.
   - Wygaśnięcia ważności hasła.
   - Zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła.
   - Braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.
3. Zmiana haseł użytkowników powinna być wymuszana przez system co 30 dni, w przypadku braku wymuszenia przez system, użytkownik sam jest zobowiązany do zmiany hasła co 30 dni.

4.7 Kopie bezpieczeństwa

1. Kopie zapasowe zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania powinny być wykonywane na bieżąco przez Administratorów Systemu Informatycznych.
2. Kopie zapasowe należy opisywać w sposób umożliwiający szybką i jednoznaczną identyfikację zawartych w nich danych.

3. Tworzenie, przechowywanie i likwidację kopii zapasowych powinny regulować szczegółowe instrukcje operacyjne dla poszczególnych systemów informatycznych, opracowywane przez ASI, z uwzględnieniem niniejszych postanowień.
4. Kopie zapasowe powinny być tworzone w bezpiecznym systemie archiwizacji, który powinien zapewniać ograniczony dostęp fizyczny do nośników oraz przyznanie uprawnień dostępu tylko wyznaczonemu imiennie ASI oraz Inspektora.
5. Dane z kopii zapasowych powinny być odtwarzane wyłącznie przez ASI.
6. Kopie zapasowe, które uległy uszkodzeniu powinny podlegać natychmiastowemu zniszczeniu. Niszczenia kopii zapasowych, na nośnikach magnetycznych dokonuje ASI lub inna upoważniona osoba.
7. Automatyczne dzienne kopie bezpieczeństwa winny być zapisywane na urządzeniach magazynujących znajdujących się w innym pomieszczeniu (innej serwerowni)
8. Centralnym punktem zapisu kopii bezpieczeństwa poszczególnych systemów informatycznych jest serwerownia przy ul. Westerplatte 64 którą zarządza Sekcja Informatyki. Urządzeniem magazynującym jest macierz dyskowa lub wysokowydajny FTP z dyskami w układzie RAID.

5. POLITYKA BEZPIECZEŃSTWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

Polityka bezpieczeństwa w zakresie danych osobowych związanego z bezpieczeństwem informacji stanowi odrębny dokument związany z niniejszym SZBI - Zarządzenie Rektora Nr R.021.53.18, późn.zm.

Zasady przetwarzania danych osobowych w zbiorach doraźnych:

1. Dostęp do danych osobowych powinien odbywać się poprzez dedykowane aplikacje, działające w architekturze klient-serwer, lub przynajmniej, przechowujące dane na serwerach plików, nie zaś na indywidualnych stanowiskach komputerowych pracowników. Gdy zachodzi potrzeba przetwarzania danych na stacji lokalnej lub w innym formacie, np. dane w postaci pliku arkusza kalkulacyjnego, można tego dokonać w doraźnym zbiorze danych osobowych pod warunkiem, że zapisane dane będą należycie chronione, tj.
    - uniemożliwi się dostęp do danych osobom nieuprawnionym,
    - uniemożliwi się zmiany danych, a tym samym zafałszowanie informacji pochodzących z systemu,
    - zabezpieczy się bezpośredni dostęp do danych hasłem;
2. Doraźny zbiór danych osobowych należy usunąć z nośnika danych, na którym został utworzony lub zniszczyć nośnik, nie później niż 3 dni po wykorzystaniu danych.
3. Zawiadamiać Inspektora w przypadku podejrzenia lub stwierdzenia dostępu do zbioru osób nieuprawnionych.

6. ZAŁĄCZNIKI

Załącznik nr 1. Zgłoszenie naruszenia bezpieczeństwa systemu informatycznego

Załącznik nr 2. Wniosek przełożonego o nadanie uprawnień dla użytkownika w systemie informatycznym

7. TABELA ZMIAN

Wersja dokumentu	Data publikacji	Opis zmian
1.0	01.01.2014	Dokument podstawowy w wersji 1.0
2.0	01.06.2019	Nowelizacja do wersji 2.0

8. WYKAZ RYSUNKÓW

Załącznik nr 1

ZGŁOSZENIE NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

DO:	**Inspektor ochrony danych**				
OD:	Nazwisko i imię	Stanowisko	Komórka organizacyjna	Telefon	Podpis

Data i czas zajścia/zgłoszenia incydentu:	
Opis incydentu:	
Jakie przeciwdziałania zostały podjęte?	
Kto uczestniczył w incydencie?	
Kto został poinformowany o incydencie?	

Proszę podać również poniższe informacje:

Lokalizacja stacji roboczej/serwera	Nazwa stacji roboczej/serwera oraz adres IP	Nazwisko użytkownika stacji roboczej/ administratora serwera	Telefon użytkownika stacji roboczej/ administratora serwera	Uwagi

Informacje o sprzęcie:	Komputer	Monitor	Drukarka (podłączona bezpośrednio)	Inne
Producent				
Nr seryjny lub inwentarzowy				

Data i godzina przyjęcia zgłoszenia

……..

Nazwisko (czytelne) i podpis osoby przyjmującej zgłoszenie

…….

Załącznik nr 2

WNIOSEK PRZEŁOŻONEGO O NADANIE UPRAWNIEŃ DLA UŻYTKOWNIKA W SYSTEMIE INFORMATYCZNYM

☐ Nowy użytkownik	☐ Modyfikacja uprawnień	☐ Odebranie uprawnień w systemie

DOTYCZY SYSTEMU: .....
(nazwa aplikacji lub bazy danych , w której przetwarzane są dane osobowe)

Imię i nazwisko użytkownika:	**Jednostka organizacyjna**	
Pokój nr:	**Telefon nr:**	
Posiada upoważnienie do przetwarzania danych osobowych:	☐ TAK	☐ NIE
Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie:		
Data zgłoszenia:	Przełożony użytkownika systemu:	
SI:	Inspektor:	

Wyżej przedstawiony wniosek wypełnia przełożony i przesyła pocztą elektroniczną do SI / Inspektor.