Zarządzenie Nr 110/2024
Rektora Politechniki Białostockiej
z dnia 7 listopada 2024 roku
w sprawie ustalenia „Polityki Bezpieczeństwa Informacji w Politechnice Białostockiej”

Na podstawie art. 23 ust. 2 pkt 2 ustawy z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce
(Dz.U. z 2024 r. poz. 1571, z późn. zm.) oraz § 26 ust. 2 pkt 2 Statutu Politechniki Białostockiej, zarządza się, co następuje:

§ 1

Ustala się „Politykę Bezpieczeństwa Informacji w Politechnice Białostockiej”, w brzmieniu określonym w załączniku do zarządzenia.

§ 2

Odpowiedzialnymi za prawidłową realizację zarządzenia czynię kierujących jednostkami organizacyjnymi.

§ 3

Nadzór nad prawidłową realizacją zarządzenia sprawuje Prorektor ds. Rozwoju.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

I Zastępca Rektora

dr hab. inż. Mirosław Świercz, prof. PB

Polityka Bezpieczeństwa Informacji

w Politechnice Białostockiej

Spis treści

Wstęp 3

Deklaracja o ustanowieniu Polityki Bezpieczeństwa Informacji w Politechnice Białostockiej 4

Cele i zadania Polityki Bezpieczeństwa Informacji 5

Słownik pojęć 7

Zakres Polityki Bezpieczeństwa Informacji 11

Zarządzanie aktywami i klasyfikacja informacji 11

Bezpieczeństwo informacji niejawnych 12

Role, odpowiedzialność i uprawnienia 12

Obszar przetwarzania informacji i jego bezpieczeństwo 17

Bezpieczeństwo przetwarzania informacji i danych osobowych 19

Bezpieczeństwo teleinformatyczne 19

Zasady zarządzania Systemami Informatycznymi Politechniki Białostockiej 19

Zasady bezpieczeństwa przetwarzania informacji w formie tradycyjnej - „Polityka czystego biurka” 20

Zasady bezpieczeństwa przetwarzania informacji w Systemie Informatycznym 21

Rozpoczęcie, zawieszenie i zakończenie pracy w systemach informatycznych - „Polityka czystego ekranu” 22

Zasady bezpiecznego użytkowania Sprzętu komputerowego i programów 23

Zasady korzystania z Elektronicznych nośników danych 24

Bezpieczeństwo wymiany informacji 25

Przechowywanie dokumentacji archiwalnej 25

Zasady bezpiecznej pracy na odległość 25

Zasady postępowania w przypadkach incydentów bezpieczeństwa informacji i danych osobowych 25

Kategorie incydentów 26

Zakres obowiązywania procedur zarządzania incydentami 27

Zgłaszanie incydentów 28

Postępowanie z incydentami 28

Zarządzanie danymi badawczymi 31

Zarządzanie ryzykiem w zapewnieniu bezpieczeństwa informacji i danych osobowych 31

Identyfikacja ryzyka 32

Analiza ryzyka 33

Plan zarządzania ryzykiem, monitorowanie ryzyka 33

Dokumentowanie, monitorowanie i ocena wyników działania systemu zarządzania bezpieczeństwem informacji 33

Postanowienia końcowe 35

Załączniki 35

Wstęp

§ 1

Określone w Polityce Bezpieczeństwa Informacji w Politechnice Białostockiej zasady zarządzania bezpieczeństwem informacji zostały opracowane zgodnie z obowiązującymi przepisami prawa oraz na podstawie właściwych norm, standardów i dobrych praktyk, w szczególności:

Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/ 679 z dnia 27 kwietnia 2016 roku 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) (Dz. U. UE. L. 2016.119.1 z 04.05.2016 r.), zwanego dalej „RODO”;

Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781);

Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2022 r., poz. 2509);

Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r., poz. 1557);

Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077);

Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r., poz. 902);

Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r., poz. 632);

Ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r., poz. 1524);

Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r., poz. 773);

Polskich i Międzynarodowych Norm:

PN-ISO/IEC 27001 – Technika informatyczna – Techniki bezpieczeństwa – Systemy Zarządzania bezpieczeństwem informacji – Wymagania,

PN-ISO/IEC 27002 – Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji,

PN-ISO/IEC 27005 – Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.

Deklaracja o ustanowieniu Polityki Bezpieczeństwa Informacji w Politechnice Białostockiej

§ 2

Władze Politechniki Białostockiej dostrzegają zagrożenia związane z bezpieczeństwem informacji i danych osobowych, gromadzonych i przetwarzanych w celu realizacji statutowych zadań Uczelni - zarówno w systemach teleinformatycznych, jak również w formie papierowej i innej. Uznają zatem za swój obowiązek ochronę zasobów informacyjnych Uczelni, które mogą być narażone na utratę poufności, integralności i dostępności w trakcie ich przetwarzania. Za szczególnie istotne władze Politechniki Białostockiej uznają bezpieczeństwo systemów teleinformatycznych, od których sprawności i niezawodności jest uzależnione niezakłócone funkcjonowanie Uczelni.

Polityka Bezpieczeństwa Informacji w Politechnice Białostockiej wyraża stanowisko władz Uczelni w zakresie zarządzania bezpieczeństwem informacji i danych osobowych. W celu zapewnienia właściwej ochrony informacji własnych i powierzonych Politechnice Białostockiej, władze Uczelni deklarują podejmowanie wszechstronnych działań na rzecz stałego zwiększania poziomu bezpieczeństwa informacji, poprzez:

adekwatne zabezpieczanie informacji i danych osobowych przetwarzanych w Politechnice Białostockiej;

stałe podnoszenie świadomości pracowników Uczelni przetwarzających informacje i dane osobowe;

egzekwowanie właściwego wykonywania obowiązków pracowniczych od osób zatrudnionych przy przetwarzaniu informacji i danych osobowych.

Rektor Politechniki Białostockiej, wprowadzając Politykę Bezpieczeństwa Informacji w Politechnice Białostockiej deklaruje, że wynikający z jej zapisów System Zarządzania Bezpieczeństwem Informacji w Politechnice Białostockiej, będzie podlegał ciągłemu doskonaleniu, zgodnie z wymaganiami prawa. Jednocześnie Rektor deklaruje wsparcie dla

realizacji Polityki Bezpieczeństwa Informacji w Politechnice Białostockiej, a także zapewnienie odpowiednich środków do jej wdrożenia.

Cele i zadania Polityki Bezpieczeństwa Informacji

§ 3

Polityka Bezpieczeństwa Informacji w Politechnice Białostockiej opiera się na trzech podstawowych zasadach:

zasadzie poufności informacji, która polega na zagwarantowaniu tajemnicy informacji
oraz udzielaniu pracownikom dostępu do informacji tylko w zakresie niezbędnym do wykonywania pracy lub zadań na zajmowanym stanowisku oraz przyznanych uprawnień. Poufność informacji polega na:

ograniczeniu zbioru osób, które mają dostęp do informacji przetwarzanych w Uczelni wyłącznie do grupy uprawnionych Użytkowników (poprzez uwierzytelnianie osób, procesów lub innych podmiotów mających dostęp do informacji),

ograniczeniu dostępu do informacji, zgodnie z klasyfikacją informacji oraz poziomem uprawnień Użytkownika,

zachowaniu tajemnicy informacji przekazywanej w formie komunikatów lub plików między osobami lub podmiotami;

zasadzie integralności informacji, która polega na zapewnieniu dokładności (wierności)
oraz kompletności informacji w dwóch punktach czasu i przestrzeni, tj.:

zapewnieniu, że informacje nie zostały wcześniej zmienione lub zniszczone w nieautoryzowany sposób,

zapewnieniu, że system informatyczny realizuje swoją zamierzoną funkcję w sposób nienaruszony, wolny od celowej lub przypadkowej, nieautoryzowanej manipulacji,

zapewnieniu kompletności, dokładności oraz ważności informacji,

niedopuszczeniu do omyłkowego lub intencjonalnego zniekształcenia informacji;

zasadzie dostępności informacji, która polega na zapewnieniu, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy istnieje taka potrzeba, dzięki:

zapewnieniu ciągłości obsługi dostępu do informacji,

zapewnieniu bezpieczeństwa dostępu,

spełnieniu warunków wydajności (zapewnieniu założonego czasu odpowiedzi na żądanie dostępu),

przestrzeganiu terminów przetwarzania informacji.

Cele Polityki Bezpieczeństwa Informacji w Politechnice Białostockiej obejmują w szczególności:

określenie zasad właściwej ochrony aktywów Uczelni;

zagwarantowanie zachowania poufności gromadzonych i przetwarzanych informacji;

zapewnienie integralności gromadzonych i przetwarzanych informacji oraz dostępności do nich;

zagwarantowanie wymaganego poziomu bezpieczeństwa przetwarzanych informacji;

maksymalne ograniczenie występowania ryzyka i zagrożeń dla bezpieczeństwa informacji;

zapewnienie poprawnego i bezpiecznego funkcjonowania systemów informatycznych;

zapewnienie gotowości do podejmowania działań w sytuacjach kryzysowych;

zapewnienie odpowiedniego poziomu wiedzy dotyczącej bezpieczeństwa informacji wśród pracowników oraz osób trzecich i podmiotów, które współpracują z Uczelnią;

zapewnienie ciągłości działania procesów przetwarzania informacji i właściwej reakcji na incydenty związane z bezpieczeństwem informacji;

ochronę wizerunku Uczelni.

Cele, sformułowane w ust. 2, będą realizowane poprzez:

właściwą organizację uczelnianego systemu zapewnienia bezpieczeństwa informacji, opartą na udokumentowanych politykach, instrukcjach i procedurach;

skuteczną ochronę przetwarzanych informacji, ze szczególnym uwzględnieniem informacji prawnie chronionych;

wdrażanie, eksploatację i rozwój systemów teleinformatycznych w sposób gwarantujący zachowanie zasad bezpieczeństwa;

zapewnienie odpowiedniego poziomu dostępności informacji i niezawodności systemów informatycznych;

skuteczne zarządzanie ryzykiem w zakresie bezpieczeństwa informacji, w celu uzyskania akceptowanego poziomu ryzyka;

wykonywanie okresowych audytów i kontroli we wszystkich obszarach związanych z zakresem bezpieczeństwa informacji;

stałą edukację pracowników przetwarzających informacje;

zapewnienie przez społeczność akademicką Politechniki Białostockiej wsparcia władzom Uczelni w działaniach na rzecz bezpieczeństwa informacji.

Słownik pojęć

§ 4

Użyte w Polityce Bezpieczeństwa Informacji terminy i pojęcia oznaczają:

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. Administratorem Danych Osobowych przetwarzanych w Uczelni jest Politechnika Białostocka, w imieniu której działa Rektor;

Administrator Systemu Informatycznego (ASI) – wyznaczony pracownik odpowiedzialny za parametryzację aplikacji Systemu i/lub nadawanie uprawnień Użytkownikom lub pracownik odpowiedzialny za utrzymanie techniczne Systemu;

Aktywa – zasoby wykorzystywane przez Politechnikę Białostocką w procesie przetwarzania informacji i danych osobowych np.: personel, obiekty, urządzenia, sprzęt komputerowy, oprogramowanie, sieć i infrastruktura teleinformatyczna, elektroniczne nośniki informacji, umiejętności, technologie, informacje, dane, itp., które są niezbędne do prowadzenia działalności Uczelni;

Analiza ryzyka – proces identyfikacji, oceny i klasyfikacji ryzyka związanego z ochroną danych osobowych oraz bezpieczeństwem informacji i systemów informatycznych;

Bezpieczeństwo informacji – ogół działań podejmowanych w celu zapewnienia poufności, integralności i dostępności przetwarzanych informacji;

Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

Elektroniczny nośnik informacji – urządzenie lub medium (np. dyski HDD/SSD, pamięci USB, karty pamięci, płyty CD/DVD/Blue-ray, chmury obliczeniowe) służące do zapisywania, przechowywania, przetwarzania i odczytywania danych w postaci cyfrowej;

Identyfikator użytkownika – unikalny ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę w systemie informatycznym;

Incydent – niespodziewane lub niepożądane zdarzenie lub seria takich zdarzeń świadczących o naruszeniu lub wysokim ryzyku naruszenia bezpieczeństwa informacji;

Informacje – wszelkie zasoby stanowiące wartość dla Uczelni, w tym dane osobowe, wiedza, dokumenty, dane badawcze, finansowe, itp., niezależnie od ich postaci (papierowej, cyfrowej, jaki niematerialnej) lub sposobu ich przetwarzania;

Informacje chronione – wszystkie nieujawnione do wiadomości publicznej informacje o charakterze technicznym, technologicznym, handlowym, kadrowym, finansowym, organizacyjnym, strategicznym lub inne informacje posiadające wartość dla Uczelni, wymagające ochrony; w szczególności mogą to być dane osobowe pracowników, doktorantów, studentów oraz kontrahentów;

Infrastruktura teleinformatyczna (InT) – sprzęt komputerowy, zespół urządzeń i łączy transmisyjnych (stanowiących elementy InT) obejmujący w szczególności platformy sprzętowe (np.: serwery, macierze, stacje robocze), sieć teleinformatyczną (w tym: routery, przełączniki, punkty dostępowe WiFi, zapory sieciowe oraz inne urządzenia sieciowe), oprogramowanie systemowe, narzędziowe (w tym systemy operacyjne, serwery aplikacji, silniki baz danych) oraz inne elementy umożliwiające bezawaryjną i bezpieczną pracę ww. zasobów (w tym zasilacze UPS, generatory prądotwórcze, urządzenia klimatyzacyjne dedykowane dla punktów dystrybucji), realizujących usługi utrzymania zasobów dla SI;

Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Uczelnię, wykonująca zadania, o których mowa w art. 39 RODO, w szczególności

odpowiedzialna za monitorowanie przestrzegania w Uczelni przepisów o ochronie danych osobowych;

Jednostka organizacyjna – jednostka organizacyjna Uczelni w rozumieniu Regulaminu Organizacyjnego Politechniki Białostockiej;

Osoby pełniące funkcje kierownicze – należy przez to rozumieć osoby, wymienione w Statucie Politechniki Białostockiej: Rektora, Prorektorów, Kanclerza i Kwestora;

Kierujący Jednostką organizacyjną – kierownik jednostki organizacyjnej, zgodnie z definicją sformułowaną w Regulaminie Organizacyjnym Uczelni;

Konto użytkownika – logiczna przestrzeń utrzymywana w ramach SI lub InT i/lub zbiór zasobów przypisany lub udostępniony Użytkownikowi;

Mechanizm uwierzytelnienia użytkownika (Uwierzytelnianie) -– proces weryfikacji tożsamości lub innych atrybutów zgłaszanych przez podmiot lub przejętych od podmiotu (Użytkownika, procesu lub urządzenia) pozwalający na jego jednoznaczną identyfikację;

Nośnik informacji – medium fizyczne, które w sposób ulotny (fale elektromagnetyczne, fale dźwiękowe) lub trwały (dokumenty papierowe lub wykonane z innego materiału, Elektroniczne nośniki informacji) zawiera lub przenosi Informacje;

Pełnomocnik Rektora ds. Systemu Zapewnienia Bezpieczeństwa Informacji (SZBI) – osoba wyznaczona przez Rektora Uczelni, odpowiedzialna za nadzór i koordynację działań związanych z zarządzaniem bezpieczeństwem informacji;

Polityka Bezpieczeństwa Informacji w Politechnice Białostockiej – dalej: Polityka lub Polityka Bezpieczeństwa Informacji;

Przetwarzanie Informacji – operacja lub zestaw operacji wykonywanych na Informacjach lub zestawach Informacji w sposób zautomatyzowany lub niezautomatyzowany, taka jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

RODO – Rozporządzenie Parlamentu Europejskiego i Rady 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) (Dz. U. UE. L. 2016.119.1 z dnia 2016.05.04);

Sprzęt komputerowy (Urządzenie komputerowe, Komputer) – Urządzenie, które przetwarza Informacje w postaci Danych na podstawie programu lub sekwencji instrukcji dotyczących sposobu przetwarzania tych danych;

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

SZBI – System Zarządzania Bezpieczeństwem Informacji;

Środki bezpieczeństwa – środki ochrony, zastosowane w celu spełnienia wymogów bezpieczeństwa (tj. poufności, integralności i dostępności) informacji. Środki bezpieczeństwa mogą obejmować funkcje zabezpieczeń, ograniczenia zarządzania, bezpieczeństwo personelu i bezpieczeństwo struktur fizycznych, obszarów i urządzeń;

Uczelnia – Politechnika Białostocka;

Użytkownik – pracownik, współpracownik, student, doktorant lub osoba z zewnątrz upoważniona do dostępu do SI Uczelni. W szczególnych przypadkach proces lub mechanizm, któremu nadano uprawnienia do uzyskania dostępu do określonych zasobów;

Właściciel danych – osoba pełniąca funkcję kierowniczą w Uczelni, Kierujący Jednostką organizacyjną, pracownik zatrudniony na samodzielnym stanowisku, który realizuje procesy związane z przetwarzaniem informacji i danych osobowych, posiada wiedzę o czynnościach wykonywanych na danych, zakresie danych oraz aktywach wykorzystywanych w procesie przetwarzania danych, w szczególności określający cel powstania lub wdrożenia systemu informatycznego lub zbioru nieinformatycznego w procesie i sprawujący nad nim merytoryczny nadzór;

Właściciel InT (WInT) – wyznaczony Kierujący Jednostką organizacyjną, odpowiedzialny za utrzymanie, rozwój oraz bezpieczeństwo infrastruktury teleinformatycznej uczelni. WInT nadzoruje działania związane z zarządzaniem siecią, serwerami, sprzętem komputerowym oraz innymi elementami infrastruktury teleinformatycznej, współpracując z innymi Jednostkami organizacyjnymi, w celu zapewnienia ciągłości działania i wysokiej dostępności zasobów teleinformatycznych;

Zewnętrzny System Informatyczny (ZSI) – SI którego właścicielem i stroną odpowiedzialną za jego utrzymanie oraz zapewnienie odpowiedniego poziomu Bezpieczeństwa Informacji jest podmiot zewnętrzny;

Zarządzanie ryzykiem – działania mające na celu minimalizację ryzyka lub jego całkowitą eliminację.

Zakres Polityki Bezpieczeństwa Informacji

§ 5

Zakresem Polityki Bezpieczeństwa Informacji są objęte:

Wszystkie istniejące obecnie lub w przyszłości systemy informatyczne oraz tradycyjne systemy papierowe, w których są lub będą przetwarzane informacje;

Informacje będące własnością Politechniki Białostockiej i/lub powierzone Politechnice Białostockiej na podstawie stosownych umów, jeśli umowa nie stanowi inaczej;

Wszystkie typy nośników informacji;

Wszystkie lokalizacje będące obszarem przetwarzania informacji;

Wszyscy pracownicy, współpracownicy, studenci, doktoranci oraz inne osoby mające dostęp
do informacji w Politechnice Białostockiej.

Zarządzanie aktywami i klasyfikacja informacji

§ 6

1. Uczelnia identyfikuje aktywa, określa ich właścicieli, odpowiedzialnych za ochronę aktywów oraz zasady korzystania z aktywów przez pracowników, podmioty współpracujące z Uczelnią i strony trzecie.

2. Ze względu na wymagania w zakresie ochrony poufności informacji, wyróżnia się:

1) Informacje ogólnodostępne – informacje, które mogą być upublicznione, zgodnie z przepisami prawa dostępu do informacji publicznej;

2) Informacje wewnętrzne, dostępne dla wszystkich pracowników Uczelni;

3) Informacje wewnętrzne, dostępne dla wszystkich studentów i doktorantów Uczelni;

4) Informacje chronione – informacje dostępne dla wybranej grupy pracowników, posiadających określone uprawnienia.

Bezpieczeństwo informacji niejawnych

§ 7

Informacje niejawne, w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych
(Dz. U. z 2024 r., poz. 632), są wytwarzane, przetwarzane i przechowywane w Uczelni na podstawie „Planu Ochrony Informacji Niejawnych" oraz innych aktów wykonawczych, wynikających z ww. ustawy. Dokumenty te stanowią odrębne opracowania i nie będą częścią niniejszej Polityki.

Role, odpowiedzialność i uprawnienia

§ 8

Organizacja struktury SZBI ma spełniać następujące wymagania, dotyczące realizacji procesów związanych z zapewnieniem bezpieczeństwa informacji w Uczelni:

1) rozdzielenie funkcji zarządzających i kontrolnych od funkcji wykonawczych;

2) podział obowiązków i zakresów odpowiedzialności w taki sposób, aby nie pozostawały ze sobą w konflikcie;

3) zapewnienie obiektywizmu i bezstronności audytu bezpieczeństwa informacji.

Wszyscy pracownicy są odpowiedzialni za zapewnienie bezpieczeństwa informacji, do których mają dostęp w związku z realizacją obowiązków służbowych. Do przestrzegania Polityki są zobowiązane wszystkie osoby korzystające z aktywów informacyjnych Uczelni.

Za zapoznanie z Polityką osób, o których mowa powyżej, odpowiada:

kierownik pionu, w którym jest lub będzie zatrudniony pracownik na stanowisku kierowniczym;

Kierujący Jednostką organizacyjną, w której jest lub będzie zatrudniony pracownik.

Rektor Uczelni odpowiada w szczególności za:

powołanie pełnomocnika ds. SZBI, Inspektora Ochrony Danych oraz pełnomocnika ds. informacji niejawnych;

zapewnienie zasobów materialnych i ludzkich, niezbędnych do prawidłowego funkcjonowania SZBI;

zatwierdzenie wewnętrznych dokumentów SZBI (zasad ochrony grup informacji, procedur, instrukcji, itp.);

określenie zakresów uprawnień i odpowiedzialności osób, realizujących zadania związane
z bezpieczeństwem informacji w Uczelni;

podejmowanie strategicznych decyzji w procesie zarządzania bezpieczeństwem informacji;

wdrożenie Polityki w pionie Rektora;

nadzór nad procedurami klasyfikacji informacji w Uczelni;

ogólny nadzór nad ochroną aktywów informacyjnych i bezpieczeństwem przetwarzanych informacji w Uczelni;

koordynowanie wdrażania systemowych zabezpieczeń przetwarzania informacji;

inicjowanie działań zmierzających do ciągłego doskonalenia SZBI;

nadzorowanie szacowania ryzyka bezpieczeństwa informacji w odniesieniu do danych, przetwarzanych w podległych Jednostkach organizacyjnych;

nadzór nad realizacją wymogów bezpieczeństwa informacji w zakresie współpracy z podmiotami trzecimi.

Prorektorzy Uczelni odpowiadają w szczególności za:

wdrożenie Polityki w podległych pionach;

udział w podejmowaniu strategicznych decyzji w procesie zarządzania bezpieczeństwem informacji;

klasyfikację informacji – zgodnie z zakresem odpowiedzialności, wynikającym z kierowania pionem;

określenie zakresów uprawnień i odpowiedzialności osób, realizujących zadania związane z bezpieczeństwem informacji w podległych pionach;

nadzór nad ochroną aktywów informacyjnych i bezpieczeństwem przetwarzanych informacji w podległych pionach jednostkach;

koordynowanie wdrażania systemowych zabezpieczeń przetwarzania informacji w podległych pionach;

nadzorowanie szacowania ryzyka bezpieczeństwa informacji w odniesieniu do danych, przetwarzanych w podległych pionach jednostkach;

nadzór nad realizacją procedur zapewniających ciągłość funkcjonowania podległych pionów w sytuacjach awaryjnych i kryzysowych;

nadzór nad realizacją wymogów bezpieczeństwa informacji w zakresie współpracy z podmiotami trzecimi;

właściwą współpracę podległych pionów jednostek z pełnomocnikiem ds. SZBI, IOD oraz administratorami systemów informatycznych;

podejmowanie decyzji w zakresie udostępniania danych, których są właścicielem.

Dziekani i kierownicy jednostek ogólnouczelnianych odpowiadają w szczególności za:

wdrożenie Polityki w podległych Jednostkach organizacyjnych;

udział w podejmowaniu strategicznych decyzji w procesie zarządzania bezpieczeństwem informacji;

klasyfikację informacji – zgodnie z zakresem odpowiedzialności, wynikającym z kierowania Jednostką organizacyjną Uczelni;

określenie zakresów uprawnień i odpowiedzialności osób, realizujących zadania związane z bezpieczeństwem informacji w podległych Jednostkach organizacyjnych;

nadzór nad ochroną aktywów informacyjnych i bezpieczeństwem przetwarzanych informacji w podległych jednostkach;

wdrażanie systemowych zabezpieczeń przetwarzania informacji w podległych jednostkach;

nadzorowanie szacowania ryzyka bezpieczeństwa informacji w odniesieniu do danych, przetwarzanych w podległych jednostkach;

realizację procedur zapewniających ciągłość funkcjonowania podległych jednostek organizacyjnych w sytuacjach awaryjnych i kryzysowych;

nadzór nad właściwym trybem zgłaszania postępowania w związku z incydentami bezpieczeństwa informacji i naruszeniami ochrony danych osobowych;

realizację wymogów bezpieczeństwa informacji w zakresie współpracy z podmiotami trzecimi;

właściwą współpracę podległych jednostek z pełnomocnikiem ds. SZBI, IOD oraz administratorami systemów informatycznych;

podejmowanie decyzji w zakresie udostępniania danych, których są Właścicielem.

Pełnomocnik Rektora ds. Systemu Zarządzania Bezpieczeństwem Informacji:

Pełnomocnik ds. SZBI odpowiada za:

zapewnienie zgodności SZBI z aktualnymi aktami prawnymi oraz przepisami prawa uczelnianego, normami, standardami i dobrymi praktykami w obszarze bezpieczeństwa informacji,

inicjowanie oraz nadzorowanie działań wdrożeniowych, zapobiegawczych i korygujących w zakresie zarządzania bezpieczeństwem informacji,

nadzorowanie procesu zarządzania incydentami bezpieczeństwa informacji,

nadzór nad opracowaniem i aktualizacją dokumentacji SZBI,

koordynowanie procesu zarządzania ryzykiem bezpieczeństwa informacji,

organizowanie i udział w przeprowadzaniu szkoleń z zakresu SZBI,

nadzór nad procesem monitorowania i przeprowadzania okresowych przeglądów i audytów SZBI,

opiniowanie oraz wydawanie zaleceń i rekomendacji związanych z funkcjonowaniem SZBI,

podejmowanie działań w pozostałych sprawach związanych z bezpieczeństwem informacji, w zakresie niezastrzeżonym do kompetencji innych osób;

w zakresie wykonywanych zadań Pełnomocnik może wydawać wytyczne, występować z wnioskami oraz żądać udzielania informacji i opinii

dotyczących bezpieczeństwa informacji od jednostek organizacyjnych Uczelni, zgodnie z ich właściwościami.

Kanclerz Politechniki Białostockiej odpowiada za:

zapewnienie fizycznego i środowiskowego bezpieczeństwa informacji w budynkach i na terenie Uczelni;

zagwarantowanie odpowiednich środków technicznych i organizacyjnych do zapewnienia bezpieczeństwa informacji – w obszarze wynikającym z obszaru kompetencji pionu kanclerza;

nadzór nad systemem monitoringu wizyjnego;

zapewnienie skutecznej kontroli dostępu do pomieszczeń Uczelni;

adekwatne i skuteczne zapewnienie bezpieczeństwa przeciwpożarowego.

Kwestor Politechniki Białostockiej odpowiada za:

wdrożenie Polityki w podległym pionie;

klasyfikację informacji – zgodnie z zakresem odpowiedzialności, wynikającym z kierowania pionem;

zarządzania bezpieczeństwem informacji w podległym pionie, w tym określenie zakresów uprawnień i odpowiedzialności osób, realizujących zadania związane z bezpieczeństwem informacji;

nadzór nad ochroną aktywów informacyjnych i koordynowanie wdrażania systemowych zabezpieczeń przetwarzania informacji w podległym pionie;

nadzorowanie szacowania ryzyka bezpieczeństwa informacji w odniesieniu do danych, przetwarzanych w podległym pionie;

nadzór nad realizacją procedur zapewniających ciągłość funkcjonowania podległego pionu w sytuacjach awaryjnych i kryzysowych;

nadzór nad realizacją wymogów bezpieczeństwa informacji w zakresie współpracy z podmiotami trzecimi;

właściwą współpracę podległego pionu z pełnomocnikiem ds. SZBI, IOD oraz administratorami systemów informatycznych;

podejmowanie decyzji w zakresie udostępniania danych, których jest Właścicielem.

Administrator Systemu Informatycznego odpowiada za powierzony mu system IT, w szczególności za:

nadawanie identyfikatorów oraz nadawanie, ograniczanie lub cofanie uprawnień Użytkownikom, opisane w Instrukcji zarządzania systemem informatycznym wraz z uaktualnianiem kont i uprawnień Użytkowników danego systemu;

opracowywanie i aktualizację procedur/instrukcji dotyczących zarządzania systemem informatycznym;

dokonywania przeglądów systemów informatycznych oraz urządzeń komputerowych pod kątem identyfikacji ryzyka w zapewnieniu bezpieczeństwa informacji i danych osobowych;

eksport danych do systemów dziedzinowych Politechniki Białostockiej;

wykonanie lub kontrolowanie procesu archiwizowania danych;

zarządzanie kopiami awaryjnymi baz danych;

określanie warunków działania oprogramowania antywirusowego przy zachowaniu maksymalnej efektywności i minimalizacji jej negatywnego wpływu na korzystanie z systemu przez Użytkowników;

wspieranie przedsięwzięć mających na celu wdrażanie technicznych i logicznych zabezpieczeń chroniących system przed nieuprawnionym dostępem do danych oraz reagowanie w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych przetwarzanych w systemie;

instalowanie, aktualizowanie i konfiguracja oprogramowania systemowego i aplikacyjnego oraz urządzeń, o ile czynności te nie są wykonywane przez upoważnionych pracowników lub przedstawicieli dostawcy systemu na podstawie zawartej umowy;

przygotowanie urządzeń, dysków i innych elektronicznych nośników informacji, zawierających informacje i dane osobowe do likwidacji, przekazania innemu podmiotowi, konserwacji lub naprawy, o ile czynności te nie są wykonywane przez upoważnionych pracowników;

przekazywania na żądanie IOD opisów struktur zbiorów danych, schematów przepływu danych pomiędzy systemami (migracji danych), zawartości poszczególnych pól informacyjnych w aplikacjach oraz wszelkich zmian w tym zakresie.

Obszar przetwarzania informacji i jego bezpieczeństwo

§ 9

Politechnika Białostocka ustala obszar przetwarzania informacji, który obejmuje wszystkie budynki i pomieszczenia, w których wykonuje się jakiekolwiek operacje na danych, w szczególności: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, przesyłanie, rozpowszechnianie, dopasowywanie, ograniczanie, usuwanie lub niszczenie danych.

Budynki i pomieszczenia, tworzące obszar Politechniki Białostockiej, w którym są przetwarzane informacje zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych.

Fizyczne i środowiskowe bezpieczeństwo informacji jest realizowane przez:

stosowanie środków bezpieczeństwa fizycznego, w szczególności:

systemu monitoringu wizyjnego,

mechanicznego zabezpieczania obiektów i pomieszczeń,

systemu elektronicznej kontroli dostępu,

systemu sygnalizacji włamania;

stosowanie środków bezpieczeństwa środowiskowego, w szczególności:

a) systemów przeciwpożarowych i gaśniczych,

b) systemów klimatyzacji i wentylacji,

c) systemów odgromowych,

d) zabezpieczeń przeciwprzepięciowych i przeciwprzeciążeniowych,

e) systemów zasilania awaryjnego;

stosowanie zabezpieczeń organizacyjnych, dotyczących w szczególności:

a) zasad dostępu do budynków i pomieszczeń,

b) zasad organizacji ruchu osób, materiałów i pojazdów;

zapewnienie bezpieczeństwa okablowania technicznego.

Za odpowiednią ochronę obszaru przetwarzania odpowiadają kierujący jednostkami organizacyjnymi Uczelni.

Bezpieczeństwo przetwarzania informacji i danych osobowych

§ 10

W celu zapewnienia poufności, dostępności oraz integralności przetwarzanych informacji, w tym danych osobowych, Administrator wdraża środki techniczne i organizacyjne zapewniające ochronę przetwarzanych informacji adekwatną do stwierdzonego poziomu ryzyka dla poszczególnych systemów
i procesów przetwarzania.

Bezpieczeństwo teleinformatyczne

§ 11

Obszar bezpieczeństwa teleinformatycznego obejmuje zasady związane z zapewnieniem niezawodności systemów teleinformatycznych, a także ochrony aktywów informacyjnych przetwarzanych w systemach teleinformatycznych, w tym zachowania poufności, integralności i dostępności danych w nich przetwarzanych oraz zapewnienia rozliczalności działań Użytkowników w systemach informatycznych. Ogólne zasady zapewniania bezpieczeństwa w systemach teleinformatycznych opisuje Załącznik nr 1.

W celu zapewnienia efektywnego zarządzania bezpieczeństwem IT została ustanowiona struktura bezpieczeństwa IT, w której określono następujące role i odpowiedzialności właściwych kompetencyjnie Osób pełniących funkcje kierownicze, realizujących działania nadzorcze i opiniujące w procesie zarządzania bezpieczeństwem IT (zgodnie z treścią § 8) poprzez:

opiniowanie/zatwierdzanie zaproponowanych przez Dyrektora Centrum Komputerowych Sieci Rozległych, Kierownika Uczelnianego Centrum Informatycznego oraz Kierownika Sekcji Serwisów Internetowych kierunków rozwoju obszaru bezpieczeństwa IT, zapewniających spójność podejmowanych działań z celami strategicznymi Uczelni;

opiniowanie/zatwierdzanie polityk, procedur i innych regulacji wewnętrznych dotyczących bezpieczeństwa IT;

opiniowanie/zatwierdzanie inicjatyw, podejmowanych w celu ograniczania ryzyka wystąpienia niepożądanych działań i zdarzeń w obszarze bezpieczeństwa IT;

zatwierdzanie potrzeb i wydatków w obszarze bezpieczeństwa IT.

Zasady zarządzania Systemami Informatycznymi Politechniki Białostockiej

§ 12

Zasady określające sposób zarządzania Systemem Informatycznym, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji, stosownie do wielkości, rangi i znaczenia przetwarzanych w nim danych oraz ryzyka wystąpienia potencjalnych zagrożeń, obejmują:

informacje o Systemie Informatycznym oraz o przetwarzanych w nim danych;

procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w danym Systemie Informatycznym, wraz ze wskazaniem osób odpowiedzialnych za te czynności;

stosowane metody i środki uwierzytelnienia oraz procedury związane z zarządzaniem i użytkowaniem środków uwierzytelniania;

procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla Użytkowników systemu;

procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych, służących do przetwarzania danych;

sposób, miejsce i okres przechowywania:

elektronicznych nośników informacji,

kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do przetwarzania danych;

sposoby zabezpieczenia Systemu Informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do informacji;

sposoby zabezpieczenia systemu informatycznego przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;

procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych;

plan ciągłości działania systemu informatycznego.

Zasady bezpieczeństwa przetwarzania informacji w formie tradycyjnej – „Polityka czystego biurka”

§ 13

Podstawową zasadą obowiązującą osoby pracujące z wykorzystaniem dokumentów w formie papierowej jest zasada „czystego biurka”, która

oznacza niepozostawianie dokumentów zawierających informacje, w sposób umożliwiający dostęp do nich osobom nieuprawnionym.

Pracownicy są zobowiązani do prawidłowego zabezpieczenia danych na swoich stanowiskach pracy.

Za bezpieczeństwo dokumentów i wydruków zawierających informacje odpowiedzialne są osoby je przetwarzające oraz Kierownicy jednostek organizacyjnych, w których jest realizowane przetwarzanie danych.

Pracownicy są zobowiązani porządkować dokumentację pod względem jej użyteczności. Wszelka dokumentacja robocza lub tymczasowa powinna być niszczona niezwłocznie po ustaniu celu przetwarzania.

Pracownik jest zobowiązany na bieżąco niszczyć wszelkie dokumenty i wydruki zawierające informacje, które przestały mu być potrzebne, a które nie podlegają archiwizacji.

Zasady bezpieczeństwa przetwarzania informacji w Systemie Informatycznym

§ 14

Wszelkie urządzenia i nośniki zawierające informacje lub dane osobowe, takie jak serwery, komputery główne, urządzenia sieci teleinformatycznych, szafy z nośnikami zawierającymi kopie danych, powinny być usytuowane w pomieszczeniach uniemożliwiających dostęp do nich osób nieupoważnionych.

System informatyczny służący do przetwarzania informacji zabezpiecza się w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu oraz przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

System informatyczny służący do przetwarzania informacji chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń, chroniących przed nieuprawnionym dostępem.

Niedozwolone jest wyłączanie, blokowanie czy odinstalowywanie przez Użytkownika oprogramowania antywirusowego, zabezpieczającego komputer przed złośliwym oprogramowaniem oraz nieautoryzowanym dostępem z zewnątrz.

W przypadku stwierdzenia na komputerze złośliwego oprogramowania, Użytkownik jest zobowiązany do zaprzestania wykonywania jakichkolwiek

czynności i niezwłocznego powiadomienia o stwierdzeniu złośliwego oprogramowania ASI lub Kierującego Jednostką organizacyjną.

Usytuowanie urządzeń komputerowych powinno uniemożliwiać dostęp do nich osób nieuprawnionych oraz wgląd do danych wyświetlanych na monitorach.

Rozpoczęcie, zawieszenie i zakończenie pracy w systemach informatycznych– „Polityka czystego ekranu"

§ 15

Przed rozpoczęciem pracy w systemie należy upewnić się, czy stanowisko pracy nie nosi oznak wskazujących na wystąpienie incydentu naruszenia bezpieczeństwa danych w postaci fizycznej ingerencji w urządzenia oraz upewnić się, czy nie występują oznaki wskazujące na wystąpienie losowych zdarzeń, które mogą doprowadzić do utraty integralności danych.

Rozpoczynając pracę w systemie informatycznym Użytkownik jest zobowiązany:

włączyć komputer i uwierzytelnić dostęp, np. wprowadzając identyfikator Użytkownika i hasło;

hasło powinno zostać wprowadzone w sposób minimalizujący ryzyko zapoznania się z nim przez osoby trzecie; w przypadku zapoznania się z hasłem przez osobę nieuprawnioną, Użytkownik jest zobowiązany do natychmiastowej zmiany hasła;

uruchomić system – w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem wprowadzanego identyfikatora i hasła, Użytkownik natychmiast kontaktuje się z ASI i bezpośrednim przełożonym.

W przypadku niestandardowego zachowania się systemu Użytkownik ma obowiązek powiadomić o tym fakcie ASI i bezpośredniego przełożonego.

Zawieszając pracę w systemie informatycznym poprzez czasowe opuszczenie stanowiska pracy Użytkownik blokuje stację roboczą. Kontynuacja pracy następuje po odblokowaniu sesji poprzez wprowadzenie hasła Użytkownika.

Każdy komputer służący do pracy z danymi powinien mieć ustawiony wygaszacz ekranu, włączający się automatycznie po zdefiniowanym okresie bezczynności Użytkownika. W przypadku wznowienia aktywności

wygaszacz powinien być wyłączany jedynie po podaniu odpowiedniego hasła. Dodatkowo przed pozostawieniem włączonego komputera bez opieki Użytkownik powinien go zablokować – włączając wygaszacz ekranu lub w przypadku dłuższej nieobecności wylogowując się z systemu.

Kończąc pracę w systemie informatycznym Użytkownik jest zobowiązany wylogować się ze wszystkich systemów i aplikacji, wyłączyć stację roboczą oraz zabezpieczyć wszystkie informatyczne nośniki informacji, wydruki oraz inne dokumenty zawierające informacje chronione. Należy upewnić się, czy wszystkie w/w przedmioty zostały umieszczone w szafie zamykanej na klucz.

W celu zapobieżenia nieautoryzowanemu dostępowi do systemu informatycznego Użytkownik nie może udostępniać innej osobie swego identyfikatora i hasła.

Zabronione jest korzystanie z systemu informatycznego z użyciem danych dostępowych innego Użytkownika.

Zasady bezpiecznego użytkowania Sprzętu komputerowego i programów

§ 16

Podstawowym wymogiem bezpieczeństwa informacji jest korzystanie ze Sprzętu komputerowego w sposób zgodny z jego przeznaczeniem i ochrona tego sprzętu przed jakimkolwiek zniszczeniem lub uszkodzeniem.

Użytkownik zobowiązuje się do zabezpieczenia Sprzętu komputerowego przed dostępem osób nieupoważnionych, a w szczególności zawartości ekranów monitorów.

Użytkownik jest zobowiązany zgłosić zagubienie lub utratę powierzonego mu Sprzętu komputerowego bezpośredniemu przełożonemu, zgodnie z zasadami postępowania w przypadkach incydentów bezpieczeństwa informacji.

Sprzęt komputerowy, na którym przetwarzane są dane osobowe i Informacje, przed wyniesieniem poza teren Politechniki Białostockiej musi zostać dostarczony do CKSR/osoby zatrudnionej w jednostce organizacyjnej Politechniki Białostockiej na stanowisku ds. informatyki, celem zaszyfrowania i właściwego zabezpieczenia np. poprzez założenie kont Użytkownika / administratora, ustawienia automatycznego wylogowania po 5 min. bezczynności, zainstalowania programu antywirusowego itp.

Zabronione jest samowolne wynoszenie Sprzętu komputerowego poza teren Uczelni, bez uzyskania zgody bezpośredniego przełożonego oraz poinformowania osoby odpowiedzialnej materialnie.

Samowolne instalowanie, otwieranie (demontaż) Sprzętu komputerowego, instalowanie dodatkowych urządzeń lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego (np. twardych dysków, pamięci) jest zabronione.

Komputery przenośne przeznaczone do prezentacji multimedialnych nie wymagają ochrony kryptograficznej, pod warunkiem, że nie znajdują się ma nich dane osobowe lub dane stanowiące tajemnicę pracodawcy.

Zabronione jest wykorzystywanie służbowego Sprzętu komputerowego do celów prywatnych.

Użytkownicy korzystający ze służbowych komputerów przenośnych odpowiadają za właściwe zabezpieczenie urządzeń oraz są zobowiązani do:

bezpiecznego ich przechowywania;

transportu w sposób minimalizujący ryzyko kradzieży lub zniszczenia;

uniemożliwienia korzystania z urządzenia osobom nieuprawnionym.

Użytkownik nie powinien instalować ani używać oprogramowania innego, niż przekazane mu przez Uczelnię. Za szkody powstałe w wyniku samowolnego działania odpowiada Użytkownik.

Zasady korzystania z Elektronicznych nośników danych

§ 17

Zabrania się wynoszenia na zewnątrz Politechniki Białostockiej, bez ich wcześniejszego zaszyfrowania, Elektronicznych nośników danych z zapisanymi danymi osobowymi lub informacjami, których utrata mogłaby narazić Uczelnię na szkodę.

W przypadku konieczności przekazania danych na nośniku należy zwrócić uwagę, aby przekazywanie nośników odbywało się z uwzględnieniem zasad bezpieczeństwa. W tym celu Użytkownik przekazujący dane powinien: powiadomić adresata o przesyłce, dane przed wysłaniem powinny zostać zaszyfrowane, a hasło powinno zostać przekazane adresatowi inną drogą, stosować bezpieczne koperty depozytowe, przesyłkę przesłać przez kuriera.

Zabronione jest wykorzystywane prywatnych nośników do przetwarzania informacji chronionych
lub danych osobowych do celów służbowych.

Bezpieczeństwo wymiany informacji

§ 18

Obieg dokumentów zawierających informacje powinien odbywać się w sposób zapewniający pełną ochronę przed ujawnieniem danych, zawartych w dokumentach.

Przesyłanie informacji z wykorzystaniem skrzynki poczty elektronicznej powinno się odbywać wyłącznie za pośrednictwem służbowych adresów e-mail.

Dane osobowe szczególnych kategorii oraz dane zawierające poza imieniem i nazwiskiem numer PESEL oraz informacje, których ujawnienie mogłoby narazić Uczelnię na szkodę, przesyła się w postaci zaszyfrowanej. Hasło dostępu do pliku przekazuje się w odrębnej wiadomości lub innym kanałem informacyjnym.

Przekazywanie informacji za pomocą nośników zewnętrznych powinno odbywać się w sposób zapewniający poufność i integralność zawartych w nim informacji.

Przechowywanie dokumentacji archiwalnej

§ 19

Dokumenty, wytworzone w toku działalności Uczelni, posiadające określoną wartość archiwalną zgodnie z Jednolitym Rzeczowym Wykazem Akt Politechniki Białostockiej, są przechowywane w wydzielonych i przystosowanych do tego celu pomieszczeniach Archiwum Uczelnianego i Centrum Historii Politechniki Białostockiej, do których dostęp posiadają jedynie upoważnieni pracownicy.

Zasady bezpiecznej pracy na odległość

§ 20

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa informacji i przetwarzanych danych osobowych podczas pracy na odległość wprowadza się Zasady bezpiecznej pracy na odległość stanowiące Załącznik nr 2 do niniejszej Polityki.

Zasady postępowania w przypadkach incydentów bezpieczeństwa informacji i danych osobowych

Kategorie incydentów

§ 21

Incydenty z zakresu bezpieczeństwa informacji mogą być zakwalifikowane jako:

Zdarzenie mniejszej wagi mające związek z nieprawidłowym działaniem infrastruktury technicznej (np. klimatyzacji, wentylacji, centralnego ogrzewania, urządzeń biurowych), informatycznej (sprzęt informatyczny) oraz systemów lub pojedynczych aplikacji nie mających wpływu na bezpośrednie naruszenie bezpieczeństwa informacji, a w szczególności danych osobowych. Zdarzenia te nie mają bezpośredniego wpływu na zachowanie informacyjnej ciągłości działania Uczelni;

Zdarzenie większej wagi mające bezpośredni wpływ na zachowanie informacyjnej ciągłości działania Uczelni, w tym mogące stanowić naruszenie ochrony danych osobowych skutkujące koniecznością powiadomienia Organu Nadzoru Ochrony Danych Osobowych (PUODO). W szczególności takim zdarzeniem może być:

zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, nagłe przerwy w zasilaniu), występowanie zdarzeń losowych zewnętrznych może prowadzić do utraty danych (np. trwała utrata danych, częściowa lub całkowita), a także dokumentacji papierowej,

zdarzenie losowe wewnętrzne (np. niezamierzone pomyłki pracowników, administratorów, awarie sprzętowe, błędy w oprogramowaniu), które może powodować zakłócenia ciągłości pracy systemów, a także prowadzić do częściowego lub całkowitego zniszczenia danych,

zdarzenie losowe wewnętrzne związane z informacjami przetwarzanymi w sposób tradycyjny (np. przypadkowe uszkodzenie, zagubienie, całkowite zniszczenie dokumentów papierowych zawierających dane osobowe lub dane ważne dla funkcjonowania Uczelni lub jej wizerunku),

zdarzenie zamierzone, świadome i celowe, mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych osobowych:

nieuprawniony dostęp do danych z zewnątrz (włamanie do systemów Uczelni),

nieuprawniony dostęp do danych z sieci wewnętrznej,

nieuprawniony transfer danych,

zainfekowanie sprzętu lub oprogramowania w celu uszkodzenia lub kradzieży danych (np. działanie złośliwego oprogramowania typu: malware, ransomware, itp.),

bezpośrednie zagrożenie materialnych elementów systemu (np. kradzież sprzętu),

celowa próba naruszenia integralności systemu lub bazy danych (sabotaż),

próba lub modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),

niedopuszczalna manipulacja danymi w systemie,

ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą elementów systemu zabezpieczeń,

praca systemu lub sieci komputerowej, która wykazuje odstępstwa od założonego rytmu pracy, wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np. praca w systemie lub sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym i nieautoryzowanym logowaniu się, itp.,

zmiana lub zniszczenie nośników z danymi bez odpowiedniego upoważnienia lub skopiowanie danych osobowych w niedozwolony sposób,

zdarzenie związane z rażącym naruszeniem dyscypliny pracy (np. niewykonanie w ustalonym terminie kopii bezpieczeństwa, praca bez zgody na danych osobowych w celach prywatnych, itp.), mające wpływ na bezpieczeństwo informacji,

celowe przełamanie tradycyjnych zabezpieczeń miejsc przechowywania danych, w tym także osobowych (np. nieuprawnione otwarcie szafy, regału, biurka, pomieszczenia),

działanie powodujące awarię sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu;

fałszywy alarm – zdarzenie nie wyczerpujące znamion zawartych w definicji incydentu bezpieczeństwa informacji.

Zakres obowiązywania procedur zarządzania incydentami

§ 22

Procedura zarządzania incydentami w zakresie bezpieczeństwa informacji obowiązuje we wszystkich jednostkach organizacyjnych Uczelni. Procedura

obowiązuje również podmioty zewnętrzne, które dopuszczono do przetwarzania danych, w tym danych osobowych będącymi zasobami informacyjnymi Uczelni.

Zgłaszanie incydentów

§ 23

W przypadku uzyskania informacji o wystąpieniu incydentu bądź podejrzenia naruszenia bezpieczeństwa informacji i danych osobowych w Politechnice Białostockiej, każdy pracownik ma obowiązek niezwłocznie poinformować o tym fakcie Kierującego Jednostką organizacyjną, w której jest zatrudniony.

Wystąpienie incydentu bezpieczeństwa informacji i danych osobowych w Politechnice Białostockiej, należy zgłosić Pełnomocnikowi ds. SZBI za pośrednictwem poczty elektronicznej na adres: incydent@pb.edu.pl, w celu umożliwienia przeprowadzenia postępowania wyjaśniającego okoliczności danego zdarzenia. Osoba dokonująca zgłoszenia powinna w miarę możliwości zabezpieczyć materiał dowodowy. Wzór zgłoszenia incydentu stanowi Załącznik nr 3 do Polityki bezpieczeństwa informacji.

Pełnomocnik ds. SZBI w przypadku, jeżeli zgłoszenie dotyczy systemów informatycznych, niezwłocznie informuje o tym administratora systemu informatycznego (ASI).

Postępowanie z incydentami

§ 24

Postępowanie wyjaśniające przeprowadzają:

Pełnomocnik ds. SZBI;

Inspektor Ochrony Danych – jeżeli naruszenie dotyczy danych osobowych;

ASI – jeżeli naruszenie miało miejsce w systemie informatycznym;

kierujący Jednostką organizacyjną lub pracownik Jednostki organizacyjnej, wskazany przez kierującego jednostką, w której nastąpiło naruszenie;

inne osoby, wyznaczone przez Pełnomocnika ds. SZBI.

W trakcie prowadzonego postępowania wyjaśniającego osoby je prowadzące mają prawo do pełnej swobody działania, dostępu do dokumentów, wglądu do operacji wykonywanych w systemach informatycznych, pobierania wyjaśnień od pracowników i osób mogących mieć wpływ na wyniki postępowania oraz podejmowania wszelkich

czynności mających na celu wyjaśnienie przyczyn, okoliczności i skutków zdarzenia.

W ramach postępowania wyjaśniającego podejmowane są następujące czynności:

dokładne rozpoznanie:

identyfikacja rodzaju incydentu:

w przypadku zdarzenia mniejszej wagi, ASI w najszybszym możliwym terminie usuwa jego skutki, a Pełnomocnik ds. SZBI zamyka postępowanie, o czym powiadamia osobę zgłaszającą i jej przełożonego,

w przypadku fałszywego alarmu, Pełnomocnik ds. SZBI zamyka postępowanie, o czym powiadamia osobę zgłaszającą i jej przełożonego,

w przypadku zdarzenia większej wagi, kontynuowane jest rozpoznanie,

ustalenie czasu i oznak wystąpienia naruszenia bezpieczeństwa informacji,

ustalenie jego przyczyn i skutków,

ustalenie osoby odpowiedzialnej za naruszenie,

identyfikacja zabezpieczania dowodów oraz poinformowanie o zdarzeniu odpowiednich organów lub osób, zgodnie z ustaleniami określonymi w dalszej części procedury, w zależności od charakteru incydentu;

podjęcie działań w kierunku ograniczenia szkód oraz przeciwdziałania podobnym przypadkom w przyszłości:

ASI jest zobowiązany do niezwłocznego:

zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu lub samodzielnym wykryciu tego faktu,

podjęcia kroków w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia,

szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,

przywrócenia normalnego działania systemu i analizy w celu określenia przyczyn naruszenia oraz wyeliminowania podobnych zdarzeń w przyszłości,

IOD:

w przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je organowi nadzorczemu – Prezesowi Urzędu Ochrony Danych Osobowych (PUODO), chyba że jest mało prawdopodobne, by takie naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,

jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu,

Pełnomocnik ds. SZBI:

w przypadku stwierdzania incydentu z zakresu cyberbezpieczeństwa, zawiadamia rządowy zespołu reagowania na incydenty komputerowe CERT; zgłoszenia należy dokonać jak najszybciej, przy czym nie później niż w ciągu 24 godzin od momentu wykrycia incydentu,

w przypadku stwierdzenia działań umyślnych i ustalenia sprawcy incydentu, przekazuje wyniki analizy wraz z zabezpieczonym materiałem dowodowym ADO w celu wyciągnięcia konsekwencji służbowych wobec sprawcy(ów), ewentualnego zawiadomienia organów ścigania lub podjęcia kroków prawnych wobec osób trzecich.

Po zakończeniu postępowania osoby prowadzące postępowanie przygotowują raport zawierający m.in. informacje o:

miejscu i dokładnym czasie wystąpienia naruszenia bezpieczeństwa informacji/danych osobowych;

wykazie osób uczestniczących w zdarzeniu;

przebiegu wydarzenia związanego z naruszeniem bezpieczeństwa informacji / danych osobowych;

danych, które zostały lub mogły zostać ujawnione;

wyniku przeprowadzonej analizy ryzyka (jeżeli dotyczy);

podjętych działaniach;

wnioskach ograniczających możliwości wystąpienia podobnych zdarzeń w przyszłości.

Raport jest zatwierdzany przez osoby uczestniczące w postępowaniu wyjaśniającym i przekazywany Rektorowi.

Pełnomocnik ds. SZBI informuje o zakończeniu postępowania osobę zgłaszającą incydent oraz jej przełożonego.

Pełnomocnik ds. SZBI odnotowuje wszystkie zgłoszone incydenty w Rejestrze incydentów stanowiącym Załącznik nr 4 do Polityki bezpieczeństwa informacji.

Zarządzanie danymi badawczymi

§ 25

Dla zapewnienia ochrony danych badawczych wytwarzanych i przechowywanych w Politechnice Białostockiej (w tym również powstałych we współpracy z innymi podmiotami), określa się wymagania dotyczące ich bezpieczeństwa, sformułowane w Załączniku nr 5 do Polityki.

Zarządzanie ryzykiem w zapewnieniu bezpieczeństwa informacji i danych osobowych

§ 26

Działania w zakresie bezpieczeństwa informacji i danych osobowych są realizowane w oparciu o proces zarządzania ryzykiem. Wynikiem tego procesu jest wdrożenie zabezpieczeń, które redukują ryzyko do akceptowalnego poziomu.

Uczelnia opracowuje i wdraża proces szacowania ryzyka w bezpieczeństwie informacji i danych osobowych, który:

określa kryteria ryzyka bezpieczeństwa informacji, obejmujące kryteria szacowania ryzyka w bezpieczeństwie informacji oraz kryteria akceptacji ryzyka;

zapewnia spójne, poprawne i porównywalne wyniki w kolejnych szacowaniach ryzyka;

identyfikuje ryzyka bezpieczeństwa informacji i danych osobowych – poprzez zidentyfikowanie ryzyk związanych z utratą poufności, integralności i dostępności informacji będących w zakresie SZBI oraz identyfikację właścicieli ryzyka;

nadaje ryzykom priorytety w celu określenia postępowania z ryzykiem;

dokonuje analizy i oceny poszczególnych ryzyk bezpieczeństwa informacji i danych osobowych.

Uczelnia opracowuje i wdraża plan postępowania z ryzykiem bezpieczeństwa informacji i danych osobowych, w celu:

wyboru odpowiednich sposobów postępowania z ryzykiem bezpieczeństwa informacji i danych osobowych, uwzględniających wyniki szacowania ryzyka;

określenia wszystkich zabezpieczeń niezbędnych do wdrożenia wybranych sposobów postępowania z ryzykiem bezpieczeństwa informacji i danych osobowych.

Ryzyko bezpieczeństwa informacji i danych osobowych jest szacowane cyklicznie, w zaplanowanych odstępach czasu lub gdy jest planowane wprowadzenie istotnych zmian, a także wtedy, gdy istotnie zmieniają się procesy lub otoczenie Uczelni, np. w związku z uruchamianiem nowych projektów, wdrażaniem zmian w systemach teleinformatycznych, itp.

Proces zarządzania ryzykiem opisany jest szczegółowo w Zarządzeniu w sprawie wprowadzenia w Politechnice Białostockiej zasad oceny ryzyka i oceny skutków dla ochrony danych osobowych (DPIA) oraz oceny ryzyka bezpieczeństwa informacji.

Identyfikacja ryzyka

§ 27

Identyfikację ryzyka przeprowadzają kierownicy jednostek organizacyjnych i ASI.

Zarządzenie ryzykiem dotyczy wszystkich aktywów, m.in.: systemów informatycznych, aplikacji, infrastruktury sieciowej oraz urządzeń końcowych używanych w Uczelni, jak również usług chmurowych funkcjonujących poza infrastrukturą Uczelni z uwzględnieniem następujących czynników: zagrożenia ludzkie – ocena wpływu działania czynnika ludzkiego na bezpieczeństwo systemów IT. Przegląd powinien obejmować potencjalne awarie sprzętu, luki w oprogramowaniu, błędy w konfiguracji, nieautoryzowany dostęp, poprawność i kompletność kopii bezpieczeństwa, ataki hakerskie oraz błędy Użytkowników:

zagrożenia naturalne - żywioły (m.in. powódź, pożar, wichury), problemy związane z przepięciami itp.;

zagrożenia techniczne - ocena zasobów potrzebnych do funkcjonowania systemów IT (m.in. energia elektryczna, odpowiednia wilgotność powietrza), odpowiednie działanie komponentów (m.in. dyski twarde, chłodzenie), itp.;

zagrożenia administracyjne - wynikające z naruszeń obowiązujących przepisów prawnych (m.in. ustawa o ochronie danych osobowych), itp.

Za przegląd systemów informatycznych, niezbędny do analizy ryzyka, odpowiada ASI bezpośrednio zarządzający systemami informatycznymi.

Analiza ryzyka

§ 28

Każde zidentyfikowane ryzyko jest oceniane pod kątem prawdopodobieństwa jego wystąpienia oraz potencjalnych skutków dla działania Uczelni oraz skutków dla osób w przypadku naruszenia ich praw i wolności.

Plan zarządzania ryzykiem, monitorowanie ryzyka

§ 29

Na podstawie analizy ryzyka Pełnomocnik ds. SZBI, w porozumieniu z Właścicielem InT, Właścicielem danych i Inspektorem Ochrony Danych, opracowuje plan minimalizacji ryzyka, który obejmuje m.in. środki techniczne, organizacyjne oraz edukacyjne.

Plan powinien zawierać propozycje działań zapobiegawczych oraz harmonogram ich wdrażania.

Plan zarządzania ryzykiem jest przekazywany Rektorowi oraz jednostkom organizacyjnym Uczelni, które dokonują oceny skuteczności proponowanych działań oraz sprawują kontrolę wdrażania uzgodnionych działań zapobiegawczych.

Analiza ryzyka jest przeprowadzana co najmniej raz w roku oraz każdorazowo po istotnych zmianach w infrastrukturze IT.

Dokumentowanie, monitorowanie i ocena wyników działania systemu zarządzania bezpieczeństwem informacji

§ 30

Uczelnia planuje, wdraża i nadzoruje procesy niezbędne do spełnienia wymagań dotyczących bezpieczeństwa informacji oraz wdraża działania określone w normie ISO 27001. W Uczelni przeprowadza się okresowe oceny wyników działań na rzecz bezpieczeństwa informacji oraz oceny skuteczności SZBI.

Dokumentacja Polityki bezpieczeństwa informacji jest przeznaczona wyłącznie do użytku wewnętrznego, zawiera odwołania do innych dokumentów, takich jak: procedury, instrukcje oraz wewnętrzne regulacje

Uczelni dotyczące bezpieczeństwa informacji. Zawiera również regulacje dotyczące zakresu dokumentacji poszczególnych systemów IT.

System Zarządzania Bezpieczeństwem Informacji jest stale doskonalony, w szczególności poprzez:

dokonywanie działań korygujących oraz ocenę ich skuteczności;

przeprowadzanie działań zapobiegawczych oraz ocenę ich skuteczności;

przeprowadzanie okresowych audytów bezpieczeństwa informacji;

informowanie kierownictwa Uczelni oraz osób odpowiedzialnych za zapewnienie bezpieczeństwa informacji o zagrożeniach, podjętych działaniach i udoskonaleniach systemu.

Audyty bezpieczeństwa mogą być realizowane w szczególności w ramach weryfikacji, kontroli oraz audytów zewnętrznych i wewnętrznych w zaplanowanych odstępach czasu, w celu dostarczenia informacji o zgodności SZBI z obowiązującymi przepisami prawa, standardami i normami oraz o skuteczności działania SZBI. Zadania związane z prowadzeniem audytu bezpieczeństwa mogą zostać również powierzone podmiotowi zewnętrznemu.

W ramach monitorowania i kontroli bezpieczeństwa informacji Uczelnia przeprowadza oceny i weryfikacje efektywności i skuteczności funkcjonowania SZBI, w szczególności w przypadku wystąpienia incydentu bezpieczeństwa informacji.

Dokumentacja SZBI podlega okresowym przeglądom co najmniej raz do roku oraz każdorazowo w przypadku wystąpienia istotnych zmian, które mogą wpływać na działanie SZBI. Przeglądy przeprowadza Pełnomocnik ds. SZBI pod kątem adekwatności i skuteczności systemowych mechanizmów bezpieczeństwa informacji. Przegląd jest realizowany przy współudziale jednostek organizacyjnych Uczelni i pracowników, których kompetencje zostały określone w wymaganiach stawianych SZBI. Wyniki przeglądów są dokumentowane i przechowywane.

Na podstawie wyników przeglądów SZBI Pełnomocnik ds. SZBI przygotowuje plan działań, wdrażających wnioski z przeprowadzonego przeglądu. Plan działań powinien zawierać propozycje decyzji i zmian, zmierzających do doskonalenia SZBI.

Postanowienia końcowe

§ 31

Każdy pracownik Uczelni, przed uzyskaniem dostępu do informacji, jest zobowiązany do zapoznania się z Polityką Bezpieczeństwa Informacji w Politechnice Białostockiej. Pracownik potwierdza zapoznanie się z Polityką składając oświadczenie, którego wzór stanowi Załącznik nr 6. Oświadczenie przechowywane jest przez bezpośredniego przełożonego pracownika.

Naruszenie Polityki oraz innych obowiązków z zakresu bezpieczeństwa informacji może być podstawą odpowiedzialności pracownika, w tym odpowiedzialności karnej, odpowiedzialności przewidzianej w przepisach prawa pracy lub przepisach Kodeksu cywilnego, a w szczególności może skutkować rozwiązaniem stosunku prawnego łączącego pracownika z Uczelnią.

Załączniki

Załącznik nr 1. Ogólne zasady zapewniania bezpieczeństwa w systemach teleinformatycznych Uczelni.

Załącznik nr 2. Zasady bezpiecznej pracy na odległość.

Załącznik nr 3. Wzór zgłoszenia incydentu.

Załącznik nr 4. Rejestr incydentów.

Załącznik nr 5. Zarządzanie danymi badawczymi.

Załącznik nr 6. Oświadczenie pracownika Uczelni o zapoznaniu się z Polityką Bezpieczeństwa Informacji w Politechnice Białostockiej.

Ogólne zasady zapewniania bezpieczeństwa w systemach teleinformatycznych Uczelni

§ 1

Ogólne zasady zapewniania bezpieczeństwa w systemach teleinformatycznych:

utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji;

aktualizacje oprogramowania;

usystematyzowane tworzenie i testowanie kopii zapasowych;

zarządzanie uprawnieniami użytkowników, w tym administratorów;

uwierzytelnianie użytkowników w systemach;

bezpieczne pozyskiwanie, rozwój i utrzymanie systemów teleinformatycznych;

zabezpieczenia sieci teleinformatycznej;

eksploatacja, wycofywanie i niszczenie elektronicznych nośników informacji;

konserwacja urządzeń w celu zapewnienia ich ciągłej pracy;

stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń i wymogów przepisów prawa;

nadzorowanie usług informatycznych dostarczanych przez strony trzecie;

bieżące monitorowanie aktywów informacyjnych, w tym informatycznych, pod kątem wcześniejszego wykrycia wszelkich niebezpieczeństw mogących zagrozić bezpieczeństwu systemów;

zapewnianie bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość.

§ 2

Środki techniczne implementowane w celu zapewnienia bezpieczeństwa w systemach teleinformatycznych:

kontrola dostępu - wprowadzenie systemów kontroli dostępu do zasobów informatycznych, takich jak karty dostępu, hasła, uwierzytelnianie wieloskładnikowe oraz systemy biometryczne;

szyfrowanie danych - stosowanie szyfrowania danych zarówno w trakcie przesyłania, jak i przechowywania, aby zapewnić poufność i integralność informacji;

zapory sieciowe (firewalle) - implementacja zapór sieciowych w celu ochrony przed nieautoryzowanym dostępem oraz atakami zewnętrznymi;

systemy wykrywania i zapobiegania włamaniom (IDS/IPS) - wdrożenie systemów wykrywania i zapobiegania włamaniom, które monitorują ruch sieciowy i identyfikują potencjalne zagrożenia;

oprogramowanie antywirusowe - regularne aktualizowanie i stosowanie oprogramowania do wykrywania złośliwych programów na wszystkich urządzeniach końcowych;

kopie zapasowe - regularne tworzenie zapasowych kopii danych oraz testowanie procedur odtwarzania danych w celu zapewnienia ciągłości działania;

monitorowanie i audyt - ciągłe monitorowanie systemów informatycznych oraz przeprowadzanie regularnych audytów bezpieczeństwa w celu wykrywania i reagowania na potencjalne zagrożenia;

zarządzanie łatkami i aktualizacjami - regularne aktualizowanie systemów operacyjnych, aplikacji oraz urządzeń sieciowych w celu eliminacji znanych luk bezpieczeństwa.

§ 3

Podstawowe zasady zarządzania podatnościami w systemach teleinformatycznych:

wszystkie składniki systemów teleinformatycznych muszą być na bieżąco monitorowane i badane pod kątem występowania w nich podatności;

priorytet monitorowania i badania podatności powinien zależeć od klasyfikacji bezpieczeństwa danego składnika lub grupy takich składników;

eliminacja wykrytych podatności w systemie teleinformatycznym musi zostać poprzedzona przetestowaniem zaproponowanych zmian eliminujących podatność - przed jego zastosowaniem, w celu oceny skuteczności tego mechanizmu oraz ewentualnych negatywnych skutków funkcjonowania systemu.

§ 4

Podstawowe zasady obowiązujące w trakcie eksploatacji systemów teleinformatycznych:

systemy teleinformatyczne muszą być regularnie monitorowane pod kątem aktualności tych komponentów, które mają wpływ na poufność, dostępność lub integralność informacji przetwarzanych przez te systemy;

konfiguracja składników systemu teleinformatycznego, mających wpływ na poufność, dostępność lub integralność informacji, musi być okresowo – nie rzadziej niż raz na rok – przeglądana pod kątem aktualności i adekwatności względem wymagań bezpieczeństwa;

serwisowanie lub naprawa składników systemu teleinformatycznego może odbywać się wyłącznie:

pod nadzorem ASI,

bez nadzoru ASI, za zgodą Właściciela InT (WInT), jeśli wcześniej zostały skutecznie usunięte z nich wszystkie informacje chronione;

naprawa składnika systemu teleinformatycznego przez podmioty zewnętrzne może odbywać się po wcześniejszym usunięciu z niego wszystkich nośników danych lub po skutecznym usunięciu danych z tych nośników.

§ 5

Podstawowe zasady obowiązujące przy wycofywaniu z eksploatacji składników systemów teleinformatycznych:

należy zapewnić bezpieczeństwo informacji przetwarzanych w systemie teleinformatycznym poprzez usunięcie informacji z wycofywanego składnika;

za określenie dopuszczalnego sposobu zabezpieczenia informacji ze składnika wycofywanego z eksploatacji odpowiada WInT;

niszczenie elektronicznych nośników informacji musi zapewniać bezpowrotne usunięcie danych;

procedura niszczenia może być, za zgodą WInT, realizowana przez podmioty zewnętrzne pod warunkiem zapewnienia przez nich skutecznego zniszczenia nośnika uniemożliwiającego dostęp do umieszczonych na nim danych;

dopuszcza się niszczenie danych w sposób elektroniczny, przy użyciu algorytmów nadpisujących dane na nośnikach w sposób uniemożliwiający ich przywrócenie i odczytanie;

likwidacja elektronicznych nośników informacji odbywa się na podstawie szczegółowych przepisów obowiązujących w Uczelni.

§ 6

Zasady udzielania dostępu do systemu teleinformatycznego:

do obsługi systemu informatycznego mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie nadane zgodnie z procedurą przyjętą w Uczelni;

użytkownikiem systemu informatycznego, w ramach którego są przetwarzane dane osobowe, może zostać wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych nadane przez Rektora lub osobę upoważnioną, zgodnie z procedurą przyjętą w Uczelni;

przyznanie uprawnień do systemu informatycznego polega na wprowadzeniu do systemu przez jego administratora unikatowego identyfikatora użytkownika, hasła oraz ustanowienia zakresu dostępu zgodnie z wnioskowaną rolą;

użytkownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony;

cykliczne zmiany haseł, jeśli są wymagane w systemie, muszą być wykonywane przez użytkowników lub wymuszane przez mechanizmy dostępne w systemie informatycznym; ASI może w uzasadnionych sytuacjach polecić dokonanie zmiany hasła przez użytkownika;

identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny,
a po wyrejestrowaniu użytkownika z systemu (odebraniu dostępu) nie może być przydzielony innej osobie;

składniki systemu teleinformatycznego powinny zapewniać mechanizmy uwierzytelniania użytkowników oraz kontroli dostępu do danych;

system teleinformatyczny musi zapewniać autoryzację i rozliczalność operacji, tzn. każde działanie w systemie powinno być jednoznacznie przypisane do unikalnego identyfikatora;

hasło użytkownika:

powinno składać się co najmniej z 14 znaków, w tym zawierać małe i wielkie litery oraz cyfry i znaki specjalne,

nie może być zapisywane w systemie w postaci jawnej,

nie może być wyświetlane na ekranie komputera w sposób jawny,

musi być zabezpieczone przez użytkownika przed nieuprawnionym dostępem osób trzecich;

w przypadku nieumyślnego ujawnienia hasła osobie nieuprawnionej lub podejrzenia ujawnienia, należy postąpić zgodnie z zasadami postępowania w przypadkach incydentów bezpieczeństwa informacji;

identyfikator i hasło ASI jest przechowywane w bezpieczny sposób przez kierownika jednostki organizacyjnej odpowiedzialnej za bezpieczeństwo danego systemu;

w przypadku konieczności awaryjnego użycia konta ASI konieczne jest udokumentowanie zaistniałej sytuacji.

Zasady bezpiecznej pracy na odległość

Bezpieczeństwo obszaru przetwarzania:

pracownik jest zobowiązany do zabezpieczenia dostępu do posiadanych danych służbowych przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi oraz przed nieuprawnionym zniszczeniem lub modyfikacją;

za ochronę sprzętu służbowego wykorzystywanego do pracy na odległość oraz zapewnienie ochrony danych przetwarzanych w ramach pracy na odległość odpowiada pracownik.

Urządzenia służące do pracy na odległość:

praca na odległość, związana z przetwarzaniem informacji, jest realizowana wyłącznie z wykorzystaniem sprzętu służbowego;

pracownik jest zobowiązany każdorazowo po zakończonej pracy wylogować się z wykorzystywanych systemów oraz stosować zasadę „czystego biurka”;

pracownik, przed rozpoczęciem pracy na odległość, powinien uzyskać rewers, który stanowi podstawę do wyniesienia sprzętu poza teren Politechniki Białostockiej, zgodnie z procedurą zawartą w zasadach zarządzania składnikami majątku w Politechnice Białostockiej;

zabronione jest udostępnianie powierzonych urządzeń służbowych wykorzystywanych do realizowania pracy na odległość innym osobom, np. domownikom oraz udostępnianie innym osobom danych służących do uwierzytelnienia do systemów;

zabronione jest udostępnianie osobom trzecim haseł oraz przechowywanie ich w miejscach niegwarantujących ich poufności;

minimalne wymagania w zakresie bezpieczeństwa sprzętu komputerowego:

na urządzeniu jest zainstalowane aktualne oprogramowanie,

zostały włączone automatyczne aktualizacje systemu operacyjnego,

została włączona zapora systemowa oraz oprogramowanie antywirusowe,

zalogowanie się do systemu operacyjnego wymaga podania hasła,

dysk został zaszyfrowany;

dopuszcza się wynoszenie na zewnątrz Politechniki Białostockiej służbowych elektronicznych nośników danych z zapisanymi danymi, pod warunkiem ich zaszyfrowania za pomocą specjalnych narzędzi programowych. Wsparcie w szyfrowaniu zapewniają właściwe jednostki Uczelni;

drukowanie dokumentacji niezbędnej na potrzeby pracy na odległość powinno odbywać się w siedzibie Uczelni;

w trakcie transportu sprzętu komputerowego do miejsca wykonywania pracy na odległość pracownik jest zobowiązany do jego zabezpieczenia przed utratą bądź zniszczeniem.

Zabezpieczanie przekazywanych informacji:

pracownik jest zobowiązany do wykorzystywania wyłącznie służbowej skrzynki pocztowej do wykonywania zadań służbowych;

zabronione jest przesyłanie służbowych wiadomości e-mail na prywatne skrzynki pocztowe;

przesyłane za pomocą służbowej skrzynki pocztowej pliki zawierające dane osobowe należy zabezpieczyć hasłem, przekazanym odbiorcy inną drogą komunikacji;

każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy;

pracownicy korzystający z poczty służbowej są zobowiązani do przestrzegania zasad bezpieczeństwa dostępnych na stronie https://pb.edu.pl/serwery-pocztowe/.

Zasady korzystania z dokumentów w formie papierowej:

dokumentacja papierowa zawierająca informacje chronione i dane osobowe jest udostępniana pracownikowi w zakresie niezbędnym do realizacji obowiązków służbowych podczas pracy na odległość za pisemną zgodą bezpośredniego przełożonego;

bezpośredni przełożony powinien każdorazowo ocenić niezbędność wykorzystywania przez pracownika papierowej dokumentacji zawierającej informacje chronione i dane osobowe;

oryginały dokumentów nie mogą być wynoszone poza siedzibę pracodawcy;

jeżeli do pracy na odległość niezbędny jest dostęp do dokumentów papierowych, a niemożliwe jest ich zeskanowanie lub korzystanie z ich elektronicznej formy zapisanej na zaszyfrowanym nośniku danych, pracownik zgłasza do bezpośredniego przełożonego prośbę o możliwość skopiowania dokumentów oraz zabrania kopii do miejsca wykonywania pracy na odległość; po otrzymaniu zgody pracownik może sporządzić kopię niezbędnych dokumentów;

jeżeli jest to możliwe, dokumenty przed wyniesieniem poza siedzibę Politechniki Białostockiej powinny zostać zanonimizowane, tzn. należy dokonać trwałego usunięcia danych osobowych z dokumentów, bez możliwości przypisania danych konkretnej osobie;

podczas przewożenia dokumentów do miejsca realizowania pracy na odległość należy zachować szczególną ostrożność, zapewniając odpowiedni poziom bezpieczeństwa informacji oraz danych osobowych zawartych w dokumentach, w szczególności poprzez ochronę przed nieuprawnionym ujawnieniem oraz utratą;

w miejscu wykonywania pracy na odległość dokumenty powinny być odpowiednio zabezpieczone i przechowywane w miejscu niedostępnym dla nieuprawnionych osób trzecich.

Bezpieczeństwo domowej sieci informatycznej:

sprzęt komputerowy powinien być podłączony do zabezpieczonej, domowej sieci WiFi;

zabronione jest korzystanie z otwartych sieci WiFi, na przykład WiFi hotelowe, w galeriach handlowych lub hot-spot w kawiarniach itp.;

dostęp do panelu konfiguracyjnego urządzenia sieciowego oraz dostęp do sieci bezprzewodowej (sieci WiFi) powinien być zabezpieczony silnym hasłem.

Wzór zgłoszenia incydentu

Zgłoszenie incydentu bezpieczeństwa w Politechnice Białostockiej

imię i nazwisko osoby zgłaszającej……

stanowisko/funkcja……

jednostka organizacyjna/nazwa podmiotu zewnętrznego……

Miejsce, dokładny czas i data naruszenia/stwierdzenia podejrzenia naruszenia:……
……

Krótki opis wydarzenia związany ze zdarzeniem (przebieg, podjęte działania):……

……

……

……

……

Nazwa systemu informatycznego/adres poczty elektronicznej, którego dotyczy zdarzenie:……

……

Zabezpieczone dokumenty lub inne dowody związane ze zdarzeniem:……

……

(data)……..

(czytelny podpis)……..

Rejestr incydentów bezpieczeństwa informacji

Rejestr incydentów bezpieczeństwa informacji										
Lp.	Krótki opis incydentu	Czy incydent mniejszej wagi, czy większej wagi/ fałszywy alarm (M/W/F)	Data, godzina zgłoszenia	Kto zgłosił	Czy incydent naruszył ochronę danych osobowych (T/N)	Czy powiadomiono o incydencie instytucje zewnętrzne (cert.gov.pl, PUODO)	Kiedy i w jaki sposób usunięto skutki incydentu	Podjęte działania korygujące - zmiany w zasadach bezpieczeństwa	Data, godzina zamknięcia obsługi incydentu	Uwagi

Zarządzanie danymi badawczymi

Dla zapewnienia ochrony danych badawczych przetwarzanych w Politechnice Białostockiej (w tym również powstałych we współpracy z innymi podmiotami), określa się sformułowane niżej wymagania dotyczące ich bezpieczeństwa. W przypadku danych wytworzonych w wyniku badań finansowanych ze środków zewnętrznych lub we współpracy z innym podmiotem – prawa własności, zasady dostępu do danych oraz zasady ich przetwarzania powinny być jasno i precyzyjnie opisane w umowie na finansowanie badań. Przyjęte w umowie ustalenia obowiązują wszystkich partnerów.

Określa się następujące wymagania dotyczące bezpieczeństwa informacyjnego danych badawczych:

sposoby pozyskiwania i zarządzania danymi badawczymi muszą być zgodne z obowiązującymi przepisami prawa, wewnętrznymi regulacjami uczelni, normami oraz dobrymi praktykami, przyjętymi przez europejską społeczność naukową;

zaleca się przechowywanie wszystkich danych badawczych w centralnych systemach gromadzenia informacji, utworzonych w jednostkach organizacyjnych Uczelni, gdyż przechowywanie danych w pamięciach masowych, komputerach przenośnych itp. może spowodować ich utratę;

zgodnie z dobrymi praktykami archiwizacji danych badawczych, zaleca się tworzenie trzech kopi zapasowych danych, na dwóch odrębnych nośnikach, w tym jednej kopii w innej lokalizacji fizycznej, np. inny budynek lub „chmura” (tzw. reguła 3-2-1);

dostęp do danych badawczych powinien być ograniczony do osób uprawnionych, przy jednoczesnym zapewnieniu okresowego, uzasadnionego dostępu do tych danych pracownikom, realizującym zadania kontroli lub rozliczania projektu;

dane przeznaczone do powszechnego udostępnienia powinny być w trakcie trwania lub po zakończeniu badań (ale nie później, niż w momencie ukazania się publikacji odwołujących się do tych danych) zdeponowane w wybranym otwartym repozytorium; repozytorium powinno być oznakowane unikalnym i trwale przypisanym do niego identyfikatorem, np. DOI;

dane udostępniane w otwartych repozytoriach danych badawczych, powinny być przechowywane w jednym z formatów pozwalających na

interoperacyjność oraz zachowanie jak najlepszej jakości i długotrwałej, technologicznej przydatności danych badawczych (tzw. formaty otwarte);

w umowach projektowych, zawieranych z podmiotami (partnerami) zewnętrznymi powinny być jasno określone, przysługujące Politechnice Białostockiej prawa do dysponowania danymi badawczymi powstałymi w wyniku projektu;

dane badawcze, wytworzone w wyniku realizacji projektu finansowanego ze środków zewnętrznych, powinny być przechowywane przez okres 10 lat od daty podpisania umowy projektowej;

o usunięciu danych badawczych po założonym okresie przechowywania lub we wcześniejszym terminie decyduje kierownik projektu lub inny upoważniony pracownik Politechniki Białostockiej (np. dziekan, kierownik jednostki organizacyjnej) na podstawie wniosku złożonego przez kierownika projektu. Usunięcie danych powstałych w wyniku prac naukowo-badawczych jest dopuszczalne wyłącznie wtedy, kiedy nie stanowią już one materiału badawczego o dużym znaczeniu, wykazują się niskim wykorzystaniem lub nie będę podlegać kontroli przez instytucję finansującą projekt.

Oświadczenie pracownika Uczelni o zapoznaniu się z Polityką Bezpieczeństwa Informacji w Politechnice Białostockiej

Białystok,…….. 202.. r.

(nazwisko i imię).....

(aktualne stanowisko).....

(jednostka organizacyjna).....

Oświadczenie o zapoznaniu się z polityką bezpieczeństwa informacji w Politechnice Białostockiej

Ja – niżej podpisana/y- oświadczam, że zapoznałam/em się z Polityką Bezpieczeństwa Informacji w Politechnice Białostockiej oraz zobowiązuję się stosować procedury i zasady w niej określone, w szczególności:

chronić przetwarzane w Politechnice Białostockiej informacje, w tym dane osobowe przed utratą ich poufności, dostępności i integralności;

nie wykorzystywać do celów prywatnych powierzonego sprzętu oraz służbowej skrzynki pocztowej;

używać do celów służbowych wyłącznie służbowych urządzeń i służbowej skrzynki pocztowej;

nie wynosić poza teren Politechniki Białostockiej sprzętu komputerowego i/lub elektronicznych nośników danych, niezabezpieczonych środkami ochrony kryptograficznej, zawierających informacje, w tym dane osobowe;

informować o każdym przypadku wystąpienia bądź podejrzenia naruszenia bezpieczeństwa informacji i danych osobowych.

Jestem świadoma/y, że naruszenie procedur określonych w Polityce Bezpieczeństwa Informacji Politechniki Białostockiej może skutkować odpowiedzialnością karną, dyscyplinarną lub odszkodowawczą na zasadach i w trybie przewidzianym w przepisach prawa, w tym w ustawie z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2023 r., poz. 1465 z późn. zm.).

(data, czytelny podpis)…….