Załącznik nr 2 do Zarządzenia nr R021.1.34.2026
Rektora UJD w Częstochowie z dnia 16 marca 2026 r.
w sprawie wprowadzenia wersji 2 dokumentacji bezpieczeństwa informacji: Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym w Uniwersytecie Jana Długosza w Częstochowie

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM w Uniwersytecie Jana Długosza w Częstochowie

---

Dokument do użytku wewnętrznego
marzec 2026 r.
Wersja 02

SPIS TREŚCI

WSTĘP

Niniejsza instrukcja zawiera sposób zarządzania systemem informatycznym, służącym do przetwarzania informacji, w tym danych osobowych.

Zatwierdzona przez administratora i przyjęta do stosowania, stanowi dokument obowiązujący ogół pracowników i osób, przy pomocy których administrator wykonuje swoje czynności w jednostce. Zawarte w niej procedury i wytyczne powinny być przekazane osobom odpowiedzialnym w jednostce za ich realizację stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności.

DEFINICJE

§1

Użyte w niniejszej dokumentacji bezpieczeństwa informacji definicje i pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą dokumentacją oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte przez administratora w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych. Ilekroć w niniejszej polityce bezpieczeństwa jest mowa o:

1. Administratorze danych – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W niniejszej dokumentacji przez administratora danych rozumie się Uniwersytet Jana Długosza w Częstochowie reprezentowany przez rektora, dalej zwany „administratorem". W przypadku przetwarzania danych innych niż dane osobowe przez administratora rozumie się kierownika jednostki (rektora) w kontekście ustawy o cyberbezpieczeństwie;
2. Lokalnym administratorze danych osobowych (lub „LADO") – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, której administrator przekazuje obowiązki wynikające z ogólnego rozporządzenia o ochronie danych. W niniejszej dokumentacji przez Lokalnego administratora danych osobowych rozumie się: dziekanów w zakresie działalności podległych wydziałów, prorektorów w zakresie działalności podległych jednostek, kanclerza w zakresie działalności administracji centralnej i w innych obszarach niepodlegających dziekanom i prorektorom. Podczas nieobecności obowiązki poszczególnych LADO przejmują ich zastępcy;
3. Administratorze systemów informatycznych (lub „ASI") – rozumie się przez to osobę wyznaczoną przez administratora, która odpowiada za zapewnianie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby przetwarzanie w systemach informatycznych odbywało się zgodnie z obowiązującymi przepisami prawa, w tym ogólnym rozporządzeniem o ochronie danych. Podczas nieobecności ASI obowiązki przejmuje przełożony osoby pełniącej tę funkcję;
4. Koordynatorze systemów komputerowych (lub „KSK") – rozumie się przez to informatyka, który odpowiada za zapewnianie sprawności i konserwacji sprzętu komputerowego oraz prawidłowe zabezpieczanie stanowisk komputerowych na poszczególnych wydziałach, w administracji centralnej i jednostkach ogólnouczelnianych;

5. Administratorze sieci intranetowej – rozumie się przez to pracownika administratora odpowiedzialnego za zarządzanie i bezpieczeństwo sieci intranetowej uczelni;
6. Zabezpieczeniu stanowisk komputerowych przeznaczonych do pracy w wewnętrznych systemach uczelni – rozumie się przez to instalację wspieranego systemu operacyjnego oraz stworzenie kont z odpowiednimi uprawnieniami (administrator – instalacja/ odinstalowanie oprogramowania/ blokada/ odblokowywanie zewnętrznych nośników pamięci/ zdalny dostęp do komputera użytkownika; użytkownik – praca na zainstalowanym oprogramowaniu, brak możliwości ingerencji w konfigurację systemu), zainstalowanie aktualnego oprogramowania antywirusowego, stworzenie zaszyfrowanej przestrzeni dyskowej, konfiguracja systemowego wygaszacza ekranu;
7. Zabezpieczeniu stanowisk komputerowych nieprzeznaczonych do pracy w wewnętrznych systemach uczelni (np. stanowiska komputerowe kadry dydaktycznej) – rozumie się przez to instalację wspieranego systemu operacyjnego oraz stworzenie kont z odpowiednimi uprawnieniami (administrator – instalacja/ odinstalowanie oprogramowania/ zdalny dostęp do komputera użytkownika; użytkownik – praca na zainstalowanym oprogramowaniu, brak możliwości ingerencji w konfigurację systemu), zainstalowanie aktualnego oprogramowania antywirusowego, stworzenie zaszyfrowanej przestrzeni dyskowej, konfiguracja systemowego wygaszacza ekranu;
8. Wewnętrznych systemach uczelni – rozumie się przez to systemy zlokalizowane na serwerach uczelni;
9. Danych osobowych – rozumie się przez to 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;
10. Dokumentacji bezpieczeństwa informacji — rozumie się przez to Politykę bezpieczeństwa i Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych;
11. Organie nadzorczym - rozumie się przez to prezesa Urzędu Ochrony Danych Osobowych;
12. Identyfikatorze (loginie) użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do pracy w systemie informatycznym;
13. Osobie upoważnionej – rozumie się przez to osobę, która otrzymała od administratora upoważnienie do przetwarzania danych;
14. Przetwarzaniu danych – rozumie się przez to proces przekształcania danych wejściowych w pożądane wyniki. Obejmuje to zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych;
15. Przetwarzaniu danych osobowych – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie,

wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

16. Systemie informacyjnym – rozumie się przez to system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307), wraz z przetwarzanymi w nim danymi w postaci elektronicznej;
17. Cyberbezpieczeństwie – rozumie się przez to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
18. Incydencie/ naruszeniu bezpieczeństwa informacji – rozumie się przez to zdarzenie zagrażające bezpieczeństwu informacji, naruszające poufność, integralność lub dostępność danych lub systemów informatycznych. Odnosi się do nagłego i nieoczekiwanego zdarzenia, które może mieć negatywne skutki dla osób, mienia, danych lub infrastruktury. Incydenty bezpieczeństwa mogą dotyczyć różnych aspektów organizacji, w tym danych osobowych, sprzętu, czy oprogramowania;
19. Naruszeniu ochrony danych osobowych – rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
20. Danych genetycznych – rozumie się przez to dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
21. Rozporządzeniu – rozumie się przez to 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) (Dz.U.UE.L.2016.119.1);
22. Ustawie o cyberbezpieczeństwie – rozumie się przez to ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024 poz. 1077);
23. Upoważnieniu – rozumie się przez to oświadczenie nadawane przez administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;
24. Użytkowniku uprzywilejowanym – należy przez to rozumieć osobę upoważnioną, posiadającą nadane uprawnienia administrowania danym systemem informatycznym;
25. Użytkowniku systemu – rozumie się przez to osobę upoważnioną, która otrzymała dostęp do danego systemu informatycznego w postaci loginu i hasła;
26. Zbiorze danych – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

27. Bezpośrednim przełożonym - rozumie się przez to: rektora, prorektorów, kanclerza, zastępcę kanclerza, kwestora, zastępcę kwestora, dziekanów, dyrektorów instytutów, kierowników katedr, kierowników zakładów, dyrektorów jednostek ogólnouczelnianych, redaktora naczelnego wydawnictwa, kierowników jednostek administracyjnych (działów, biur, zespołów, administracji wydziału, domu studenta), administratorów obiektów, kierownika kancelarii ogólnej.

PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

1. ZASADY OGÓLNE

§2

1. Przydzielanie uprawnień do systemu informatycznego realizowane jest w oparciu o następujące zasady:
   1) „Minimalnych przywilejów" – każdy użytkownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków;
   2) „Wiedzy koniecznej" – pracownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań;
   3) „Domniemanej odmowy" – wszystkie działania, które nie są jawnie dozwolone są zabronione.
2. Dostęp do systemu informatycznego mogą posiadać, w zależności od wykonywanych czynności służbowych lub umownych:
   1) pracownicy administratora w zakresie niezbędnym do właściwego wykonywania obowiązków służbowych;
   2) osoby, przy pomocy których administrator wykonuje swoje czynności, w szczególności:
      a) osoby zatrudnione na podstawie umowy cywilnoprawnej;
      b) pracownicy lub osoby działające w imieniu podmiotu zewnętrznego świadczącego usługi na rzecz administratora danych;
      c) studenci/ doktoranci – kierownicy projektów badawczych oraz prowadzący zajęcia dydaktyczne;
      d) stażyści, na podstawie umowy z Urzędem Pracy;
      e) praktykanci, na podstawie umowy ze szkołą wyższą;
      f) wolontariusze, na podstawie umowy o wolontariat.
3. Użytkownik systemu informatycznego jest jednoznacznie identyfikowany poprzez nadany mu indywidualny identyfikator użytkownika.
4. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika.
5. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.

6. Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień administratora (przywilejów) będzie kwalifikowane jako incydent związany z bezpieczeństwem informacji.
7. Użytkownikowi systemu informatycznego zostaje nadany dostęp po:
   1) odbyciu przez niego wstępnego szkolenia z ochrony bezpieczeństwa informacji, w tym danych osobowych celem:

      a) zapoznania z przepisami dotyczącymi ochrony danych,
      b) zapoznania z niniejszą dokumentacją przetwarzania danych;

   2) podpisaniu oświadczenia o zachowaniu informacji (w tym danych osobowych), do których użytkownik będzie miał dostęp podczas wykonywania obowiązków służbowych lub zobowiązań umownych oraz środków ich zabezpieczania w tajemnicy (również po ustaniu łączącej strony umowy);
   3) nadaniu upoważnienia do przetwarzania danych osobowych, jeśli wymagane.
8. Rejestr użytkowników wraz z uprawnieniami do systemu lub aplikacji prowadzi administrator systemu informatycznego. Rejestr prowadzony jest w postaci elektronicznej lub papierowej.
9. Administrator systemu informatycznego raz na 30 dni dokonuje przeglądu stanu aktywności kont użytkowników, jeśli nie wymaga to zbyt dużego nakładu pracy, ale nie rzadziej niż raz na 6 miesięcy.
10. Bezpośredni przełożony/ osoba upoważniona do zawarcia umowy cywilnoprawnej jest odpowiedzialny za zapewnianie przetwarzania danych przez podległych sobie pracowników/ osoby zatrudnione na podstawie umowy cywilnoprawnej zgodnie z nadanymi uprawnieniami.

2. NADANIE UPRAWNIEŃ

§3

1. Bezpośredni przełożony pracownika zobowiązany jest do złożenia wniosku o nadanie uprawnień do systemu informatycznego z dostępem do danych osobowych dotyczącego nadania uprawnień do danego systemu informatycznego administratora. Wzór wniosku stanowi załącznik nr 1 „Wniosek o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych" do niniejszej Instrukcji. Wniosek powinien zawierać poprawną informację o zakresie uprawnień zgodnym z obowiązującym „Katalogiem zakresów uprawnień" stanowiącym załącznik nr 3 do niniejszej Instrukcji.
2. W przypadku wnioskowania o nadanie uprawnień do systemu informatycznego bez dostępu do danych osobowych należy złożyć wniosek zgodnie z wzorem stanowiącym załącznik nr 2 „Wniosek o nadanie/ odebranie uprawnień do systemu informatycznego bez dostępu do danych osobowych" do niniejszej Instrukcji.
3. W przypadku osób zatrudnionych na podstawie umowy cywilnoprawnej do złożenia wniosku o nadanie uprawnień do systemu informatycznego dotyczącego nadania uprawnień do danego systemu informatycznego administratora zobowiązane są osoby upoważnione do zawierania tych umów.

4. W przypadku studentów/ doktorantów do złożenia wniosku o nadanie uprawnień do systemu informatycznego dotyczącego nadania uprawnień do danego systemu informatycznego administratora zobowiązany jest prorektor ds. kształcenia i spraw studenckich/ dziekan.
5. Bezpośredni przełożony/ osoba upoważniona do zawarcia umowy cywilnoprawnej/ prorektor ds. kształcenia i spraw studenckich/ dziekan określając zakres uprawnień, o który wnioskuje dla pracownika/ osoby zatrudnionej na podstawie umowy cywilnoprawnej/ studenta/ doktoranta obowiązany jest do stosowania zasad, o których mowa w §2 ust. 1 pkt. 1-3 niniejszej Instrukcji.
6. Po dopełnieniu powyższych wymagań „Wniosek o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych" powinien zostać przekazany w 1 egzemplarzu do Działu Kadr i Spraw Socjalnych, który po przygotowaniu upoważnienia do przetwarzania danych osobowych, przekazuje wniosek administratorowi systemu informatycznego do realizacji. W przypadku wnioskowania o nadanie uprawnień bez dostępu do danych osobowych „Wniosek o nadanie/ odebranie uprawnień do systemu informatycznego bez dostępu do danych osobowych" jest przekazywany bezpośrednio do administratora systemu informatycznego z pominięciem Działu Kadr i Spraw Socjalnych.
7. Administrator systemu informatycznego realizuje otrzymany wniosek lub odmawia nadania uprawnień do systemu informatycznego w przypadku uchybienia wymogom określonym w §2 ust. 1 pkt. 1-3 lub powzięciu przez administratora systemu informatycznego podejrzeń co do przekroczenia uprawnień wymaganych na danym stanowisku.
8. W przypadku nadania uprawnień wymagających logowania, administrator systemu informatycznego przekazuje użytkownikowi informację zawierającą wymienione z nazwy systemy informatyczne, do których użytkownik otrzymał dostęp oraz login i hasło na potrzeby pierwszego logowania. Hasło nie powinno być przekazywane przez osoby trzecie lub za pośrednictwem niechronionych wiadomości poczty elektronicznej. ASI przekazuje do Działu Kadr i Spraw Socjalnych „Wniosek o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych" uzupełniony o nazwy systemów informatycznych, do których użytkownik otrzymał dostęp oraz nadane identyfikatory.
9. Wnioski o nadanie uprawnień sporządzone wg wzoru stanowiącego załącznik nr 1 „Wniosek o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych" oraz załącznik nr 2 „Wniosek o nadanie/ odebranie uprawnień do systemu informatycznego bez dostępu do danych osobowych" do niniejszej Instrukcji mogą zostać przekazane do odpowiednio Działu Kadr i Spraw Socjalnych/ administratora systemu informatycznego także drogą elektroniczną opatrzone odpowiednimi poświadczeniami elektronicznymi.

3. MODYFIKACJA UPRAWNIEŃ (ZWIĘKSZENIE ZAKRESU UPRAWNIEŃ POPRZEZ NADANIE NOWYCH UPRAWNIEŃ)

§4

1. Bezpośredni przełożony jest zobowiązany do złożenia wniosku o nadanie nowych uprawnień do systemu informatycznego dotyczącego nadania nowych uprawnień do danego zasobu informatycznego.

2. W przypadku osób zatrudnionych na podstawie umowy cywilnoprawnej do złożenia wniosku o nadanie nowych uprawnień do systemu informatycznego dotyczącego nadania nowych uprawnień do danego zasobu informatycznego zobowiązane są osoby upoważnione do zawierania tych umów.
3. W przypadku studentów/ doktorantów do złożenia wniosku o nadanie nowych uprawnień do systemu informatycznego dotyczącego nadania nowych uprawnień do danego systemu informatycznego administratora zobowiązany jest prorektor ds. kształcenia i spraw studenckich/ dziekan.
4. W przypadku, gdy wniosek dotyczy zwiększenia zakresu uprawnień o uprawnienia z dostępem do danych osobowych bezpośredni przełożony/ osoba upoważniona do zawarcia umowy cywilnoprawnej/ prorektor ds. kształcenia i spraw studenckich/ dziekan przekazuje wniosek do Działu Kadr i Spraw Socjalnych. Dział Kadr i Spraw Socjalnych po nadaniu numeru/ uzupełnieniu wniosku o numer już nadanego upoważnienia do przetwarzania danych osobowych, przekazuje wniosek administratorowi systemu informatycznego do realizacji. W przypadku wnioskowania o zwiększenie uprawnień bez dostępu do danych osobowych wniosek jest przekazywany bezpośrednio do administratora systemu informatycznego z pominięciem Działu Kadr i Spraw Socjalnych.
5. Wniosek modyfikujący uprawnienia pracownika powinien zostać złożony do Działu Kadr i Spraw Socjalnych/ administratora systemu informatycznego w możliwie najkrótszym czasie po wystąpieniu zapotrzebowania na dostęp do danego zasobu informatycznego.
6. W zależności od obszaru zmian, wniosek powinien zawierać informację o przedmiocie modyfikacji:
    1) dodanie zakresu uprawnień;
    2) nadanie indywidualnych uprawnień do systemów poza zdefiniowanym zakresem.
7. Administrator systemu informatycznego realizuje otrzymany wniosek lub odmawia nadania uprawnień do systemu informatycznego w przypadku uchybienia wymogom określonym w §2 ust. 1 pkt. 1-3 lub powzięciu przez administratora systemu informatycznego podejrzeń co do przekroczenia uprawnień wymaganych na danym stanowisku.
8. W przypadku nadania uprawnień wymagających logowania, administrator systemu informatycznego przekazuje użytkownikowi informację zawierającą wymienione z nazwy systemy informatyczne, do których użytkownik otrzymał dostęp oraz login i hasło na potrzeby pierwszego logowania. Hasło nie powinno być przekazywane przez osoby trzecie lub za pośrednictwem niechronionych wiadomości poczty elektronicznej. ASI przekazuje do Działu Kadr i Spraw Socjalnych „Wniosek o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych" uzupełniony o nazwy systemów informatycznych, do których użytkownik otrzymał dostęp oraz nadane identyfikatory.
9. Wnioski o nadanie nowych uprawnień sporządzone wg wzoru stanowiącego załącznik nr 1 „Wniosek o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych" oraz załącznik nr 2 „Wniosek o nadanie/ odebranie uprawnień do systemu informatycznego bez dostępu do danych osobowych" do niniejszej Instrukcji mogą zostać przekazane do odpowiednio Działu Kadr i Spraw Socjalnych/ administratora systemu informatycznego także drogą elektroniczną opatrzone odpowiednimi poświadczeniami elektronicznymi.

4. ODEBRANIE UPRAWNIEŃ

§5

1. Bezpośredni przełożony jest zobowiązany do złożenia wniosku o odebranie uprawnień do systemu informatycznego dotyczącego odebrania użytkownikowi uprawnień do danego zasobu informatycznego.
2. W przypadku osób zatrudnionych na podstawie umowy cywilnoprawnej do złożenia wniosku o odebranie uprawnień do systemu informatycznego dotyczącego odebrania użytkownikowi uprawnień do danego zasobu informatycznego zobowiązane są osoby upoważnione do zawierania tych umów.
3. W przypadku studentów/ doktorantów do złożenia wniosku o odebranie uprawnień do systemu informatycznego dotyczącego odebrania uprawnień do danego systemu informatycznego administratora zobowiązany jest prorektor ds. kształcenia i spraw studenckich/ dziekan.
4. Terminami obowiązującymi przy składaniu wniosku są w szczególności:
    1) w przypadku urlopów na wniosek zatrudnionego, z wyłączeniem urlopów wypoczynkowych i naukowych – wniosek odbierający wszystkie uprawnienia – od 1 dnia urlopu;
    2) w przypadku długotrwałego zwolnienia lekarskiego – wniosek odbierający wszystkie uprawnienia – natychmiast po upływie 30 dni kalendarzowych zwolnienia lekarskiego;
    3) w przypadku zmiany stanowiska pracy – wniosek odbierający część uprawnień – natychmiast, najpóźniej ostatniego dnia pracy przed zmianą stanowiska na stanowisko wymagające zmniejszenia uprawnień.
5. Po spełnieniu powyższych wymagań „Wniosek o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych” powinien zostać przekazany do Działu Kadr i Spraw Socjalnych. Dział Kadr i Spraw Socjalnych bezzwłocznie przekazuje wniosek administratorowi systemu informatycznego do realizacji. „Wniosek o nadanie/ odebranie uprawnień do systemu informatycznego bez dostępu do danych osobowych” jest przekazywany bezpośrednio do administratora systemu informatycznego z pominięciem Działu Kadr i Spraw Socjalnych.
6. Administrator systemu informatycznego przyjmuje wniosek o odebranie uprawnień do systemu informatycznego spełniający wymogi opisane powyżej.
7. Administrator systemu informatycznego dokonuje weryfikacji poprawności wniosku o odebranie uprawnień do systemu informatycznego.
8. Administrator systemu informatycznego bezzwłocznie realizuje otrzymany wniosek. Po uzupełnieniu „Wniosku o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych” o nazwy systemów informatycznych, do których uprawnienia zostały odebrane, administrator systemu informatycznego przekazuje wniosek do Działu Kadr i Spraw Socjalnych.
9. Wnioski o odebranie uprawnień sporządzone wg wzoru stanowiącego załącznik nr 1 „Wniosek o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych” oraz załącznik nr 2 „Wniosek o nadanie/ odebranie uprawnień do systemu informatycznego bez dostępu do danych osobowych” do niniejszej Instrukcji mogą zostać

przekazane do Działu Kadr i Spraw Socjalnych/ administratora systemu informatycznego także drogą elektroniczną opatrzone odpowiednimi poświadczeniami elektronicznymi.

5. ZARZĄDZANIE PRZYWILEJAMI

§6

1. Nadawane przywileje (większe uprawnienia niż wynika to z realizowanych rutynowych zadań użytkownika) podlegają ścisłej ewidencji prowadzonej przez administratora systemu informatycznego.
2. Przywileje w systemie nadaje administrator systemu informatycznego na podstawie „Wniosku o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych" stanowiącego załącznik nr 1 do niniejszej Instrukcji.
3. Uprzywilejowane konto nie może służyć do realizacji przez użytkownika rutynowych zadań.
4. Przywileje podlegają cofnięciu niezwłocznie po ustaniu potrzeby uzasadniającej ich nadanie.
5. Nadawane przywileje podlegają regularnym przeglądom i kontroli.

6. ZASADY POSTĘPOWANIA Z HASŁAMI ADMINISTRACYJNYMI

§7

[…]

STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. ZASADY OGÓLNE

§8

1. Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.
2. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
3. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez administratora systemu informatycznego) i jego przechowywanie.
4. Użytkownik systemu ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła.
5. Osoba pełniąca funkcję administratora systemu informatycznego powinna posiadać dodatkowo odrębne konto służące tylko i wyłącznie do administracji danym systemem informatycznym, o ile dany system udostępnia taką funkcjonalność.

2. POLITYKA HASEŁ

§9

Każdy użytkownik posiadający dostęp do systemów informatycznych administratora jest obowiązany do:

1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez administratora systemu informatycznego;
4) poinformowania administratora o podejrzeniu lub rzeczywistym ujawnieniu hasła, na formularzu zgłoszenia, wzór zgłoszenia incydentu stanowi załącznik nr 8 „Zgłoszenie wystąpienia incydentu" do Polityki bezpieczeństwa;
5) stosowania haseł o wysokim stopniu złożoności;
6) stosowania haseł nieposiadających w swojej strukturze części loginu;
7) stosowania haseł niebędących zbliżonymi do poprzednich (np. Tadeusz$2013 - Tadeusz$2014);
8) zmiany wykorzystywanych haseł nie rzadziej niż raz na kwartał.

§10

1. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
2. Zabronione jest:
   a) zapisywanie haseł w sposób jawny i umieszczanie ich w miejscach dostępnych dla innych osób;
   b) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
   c) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
   d) udostępnianie haseł innym użytkownikom;
   e) przeprowadzanie prób łamania haseł;
   f) wpisywanie haseł „na stałe" (np. w skryptach logowania) oraz wykorzystywania opcji auto-zapamiętywania haseł (np. w przeglądarkach internetowych).

§11

1. Administrator systemu informatycznego obowiązany jest do skonfigurowania systemu tak, aby próby dostępu do tego systemu były limitowane zarówno w ujęciu ilościowym, jak i czasowym jeżeli system umożliwia wymienioną konfigurację.
2. W przypadku, gdy system umożliwia limitowanie wprowadzenia błędnego hasła, należy przyjąć próg ilości wprowadzonych błędnych haseł na 3, po czym ustanowić blokadę konta.
3. Należy ograniczyć możliwość wielokrotnego logowania, gdzie użytkownik loguje się na kilku komputerach równocześnie wykorzystując ten sam identyfikator.

4. Administrator systemu informatycznego odblokowuje/ zresetuje hasło do danego systemu informatycznego w przypadku przekroczenia przez użytkownika ustalonej ilości prób logowania.
5. Po dokonaniu czynności przez administratora systemu informatycznego stosowna informacja o odblokowaniu dostępu do konta użytkownika zostanie przekazana użytkownikowi.

3. ZASADY POSTĘPOWANIA Z KLUCZAMI KRYPTOGRAFICZNYMI

§12

1. W systemach obsługujących transmisję danych osobowych wrażliwych lub informacji poufnych administratora powinny być wykorzystywane klucze kryptograficzne służące do zabezpieczenia danych.
2. Za generowanie, przechowywanie i bezpieczną dystrybucję kluczy kryptograficznych odpowiada administrator systemu informatycznego.
3. Przekazywanie kluczy użytkownikom powinno odbywać się w sposób protokolarny.
4. Obowiązkiem użytkownika jest zabezpieczenie kluczy (prywatnych) przed dostępem osób nieupoważnionych.
5. Dane osobowe wrażliwe lub informacje poufne administratora, do których nie stosuje się kluczy kryptograficznych, można przesyłać wyłącznie pocztą elektroniczną po uaktywnieniu funkcji podpisywania i szyfrowania pliku.
6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.
7. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza, ujawnienia klucza osobie nieupoważnionej lub podejrzenia jego ujawnienia fakt ten należy niezwłocznie zgłosić do administratora na formularzu zgłoszenia, wzór zgłoszenia incydentu stanowi załącznik nr 8 „Zgłoszenie wystąpienia incydentu” do Polityki bezpieczeństwa.

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY

§13

1. Rozpoczęcie przez użytkownika pracy w systemie następuje po wprowadzeniu unikalnego identyfikatora i hasła.
2. Zawieszenie pracy w systemie tj. brak wykonywania jakichkolwiek czynności przez okres 5 minut w systemie informatycznym powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu wygaszaczem chronionym hasłem po odejściu od stanowiska.
3. Przed zakończeniem pracy należy upewnić się czy dane zostały zapisane, aby uniknąć utraty danych.
4. Po zakończeniu pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.

5. W sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
6. Użytkownik systemu informatycznego przetwarzającego dane niezwłocznie powiadamia administratora systemu informatycznego w przypadku, gdy:
    1) wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;
    2) niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne;
    3) nie ma możliwości zalogowania się na swoje konto.

ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ

§14

1. Pracownikowi/ osobie zatrudnionej na podstawie umowy cywilnoprawnej/ innej osobie, przy pomocy której administrator wykonuje swoje czynności w jednostce zostaje nadany unikalny adres skrzynki poczty elektronicznej działający w domenie administratora.
2. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym jest dostępna na łamach witryny internetowej administratora w postaci książki adresowej.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych administratora danych podlega logowaniu, może być rejestrowana i monitorowana. Informacje przesyłane za pośrednictwem sieci administratora (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
4. Wszelka korespondencja elektroniczna niezwiązana z działalnością administratora, powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
5. Użytkownicy dokonujący wysyłki korespondencji masowej na zewnątrz, obowiązani są do ukrywania odbiorców w kopii (pole BCC lub UDW).
6. Zabronione jest:
    1) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu);
    2) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi administratora;
    3) odbieranie przesyłek z nieznanych źródeł;
    4) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
    5) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe;
    6) ukrywanie lub dokonywanie zmian tożsamości nadawcy;

7) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;

8) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją administratorowi systemu informatycznego;

9) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;

10) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb administratora lub do poszukiwania dodatkowego zatrudnienia.

7. Dostęp do nadanego użytkownikowi imiennego adresu skrzynki poczty elektronicznej jest blokowany w momencie ustania stosunku pracy, następnie skasowany po upływie minimalnie 90 maksymalnie 100 dni. Po zablokowaniu dostępu tworzona jest dla przychodzących wiadomości automatyczna odpowiedź o przesyłaniu wiadomości na skrzynkę funkcyjną jednostki/ inny imienny adres skrzynki poczty elektronicznej.
8. Dostęp do nadanego użytkownikowi imiennego adresu skrzynki poczty elektronicznej może być zachowany po ustaniu stosunku pracy w sytuacji, jeśli wynika to z innych regulacji wewnętrznych jednostki.
9. Dostęp do skrzynki funkcyjnej/ jednostki dla pracownika zastępującego następuje:

   1) w przypadku ustania stosunku pracy/ zmiany stanowiska pracy – natychmiast, najpóźniej ostatniego dnia pracy zatrudnionego na stanowisku na wniosek jego bezpośredniego przełożonego składany do administratora;

   2) w przypadku urlopów na wniosek zatrudnionego/ zwolnienia lekarskiego – ewentualny dostęp do skrzynki funkcyjnej/ jednostki na okres nieobecności pracownika następuje na wniosek jego bezpośredniego przełożonego składany do administratora.

9. Użytkownicy zobowiązani są do regularnej retencji danych na poczcie elektronicznej, czyli usuwania danych po określonym czasie, nie dłuższym niż istnienie celów, dla których te dane są przetwarzane, w tym usuwania e-maili zawierających nieaktualne informacje, usuwania nieistotnych e-maili, usuwania kopii roboczych wiadomości. Należy kierować się generalną zasadą dotyczącą okresów przechowywania: „przechowuj tak krótko, jak to możliwe oraz tak długo, jak to konieczne".
10. Użytkownicy zobowiązani są do używania klientów poczty internetowej do prowadzenia korespondencji służbowej poprzez serwer UJD. Wymagana jest konfiguracja klienta poczty tak, aby pozostawiał wiadomości e-mail na serwerze nie dłużej niż 30 dni.
11. Usuwanie nadmiarowych danych ze skrzynek poczty elektronicznej oraz wiadomości starszych niż 30 dni, zgodnie z obowiązującymi zasadami konfiguracji klienta poczty wskazanymi w pkt. 10 niniejszego paragrafu, podlega okresowym kontrolom przeprowadzanym raz na kwartał poprzez losowe sprawdzenie zawartości 10% aktywnych kont poczty elektronicznej. Dostęp do wytypowanych do sprawdzenia skrzynek poczty elektronicznej jest blokowany dla użytkowników na czas kontroli.

ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET)

§15

1. […]
2. […]
3. […]
4. Systemy informatyczne powinny korzystać z szyfrowanych protokołów wymiany danych, w szczególności połączeń sftp i https.
5. Prowadzony jest ciągły monitoring ruchu sieciowego z możliwością wyciągnięcia konsekwencji służbowych.
6. Wprowadza się całkowite ograniczenia w dostępie do treści uznanych za pornograficzne, rasistowskie, traktujące o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.
7. Dostęp do protokołu wymiany plików możliwy jest w uzasadnionych przypadkach, po nadaniu odpowiednich uprawnień.
8. Dalsze ograniczenia dostępu do sieci Internet mogą być rekomendowane przez administratora systemów informatycznych oraz inspektora ochrony danych.

ZASADY KORZYSTANIA Z SIECI WEWNĘTRZNEJ (INTRANET)

§16

1. Sieć wewnętrzna administratora podlega segmentacji logicznej. Nadzór nad bezpieczeństwem i prawidłowym działaniem sieci wewnętrznej administratora sprawuje administrator sieci intranetowej.
2. Każdy segment sieci jest odseparowany od pozostałych.
3. Sprzęt pracownika w zależności od przydzielonych mu zadań musi znajdować się w odpowiednim segmencie sieci. Za prawidłowe przypisanie urządzenia pracownika do odpowiedniego segmentu sieci odpowiada jednostka nadzorująca sieć intranetową administratora.
4. Do segmentów, w których znajdują się systemy informatyczne administratora mogą mieć dostęp jedynie urządzenia zarejestrowane, będące własnością administratora, przekazane odpowiednim pracownikom administratora w celu ich prawidłowego zabezpieczenia.
5. Urządzenia prywatne pracowników, studentów i gości mogą mieć dostęp jedynie do specjalnego segmentu wewnętrznej sieci administratora. Segment ten nosi nazwę Eduroam. Dostęp do tego segmentu sieci odbywa się na podstawie poświadczeń przechowywanych w systemie rejestracji toków nauczania USOS lub innych dopuszczonych metod autoryzacji przez Eduroam. Tylko aktywne konta studentów, pracowników i gości mają możliwość zalogowania się do tej sieci. Ruch w tej sieci podlega monitorowaniu.
6. Firmy posiadające aktywne umowy serwisowe systemów/ urządzeń administratora mogą mieć dostęp do tych systemów/ urządzeń tylko poprzez specjalnie na ten cel przygotowywane tunele VPN.

7. Za złożenie wniosku o dostęp dla firmy zewnętrznej do wewnętrznych systemów urządzeń administratora odpowiada użytkownik uprzywilejowany danego systemu informatycznego lub kierownik danego projektu badawczego. Pełne zasady współpracy z firmami zewnętrznymi znajdują się w załączniku nr 10 „Zapisy do umów zawieranych z UJD dotyczących zdalnego serwisowania urządzeń będących własnością i znajdujących się w budynkach UJD" do niniejszej Instrukcji.

ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH

§17

1. Każdy użytkownik wymiennych nośników elektronicznych, użytkownicy zdalnych dostępów do sieci służbowej administratora (VPN) oraz użytkownicy elektronicznych kart dostępu ponoszą całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz są obowiązani do stosowania się do poniższych zasad:
    1) dane przechowywane są na zaszyfrowanej przestrzeni dyskowej nośników elektronicznych;
    2) zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje administratora;
    3) komputery przenośne należy przewozić jako bagaż podręczny i w miarę możliwości je maskować;
    4) użytkownik wykonując czynności zawodowe lub umowne w domu powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;
    5) zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem;
    6) zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością administratora;
    7) w przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do administratora na formularzu zgłoszenia, wzór zgłoszenia incydentu stanowi załącznik nr 8 „Zgłoszenie wystąpienia incydentu" do Polityki bezpieczeństwa. Administrator dokumentuje wszelkie naruszenia w rejestrze, wzór rejestru stanowi załącznik nr 9 „Rejestr naruszeń bezpieczeństwa informacji" do Polityki bezpieczeństwa;
    8) problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać Koordynatorowi systemów komputerowych.
2. Pracownik w celu uzyskania zdalnego dostępu do wewnętrznych systemów informatycznych administratora przekazuje do administratora systemów informatycznych podpisany odpowiednio przez rektora/prorektora/dziekana/kanclerza oraz Lokalnego administratora danych osobowych wniosek na wzorze stanowiącym załącznik nr 7 „Wniosek o przydzielenie zdalnego dostępu do wewnętrznego systemu informatycznego" do niniejszej Instrukcji. Wniosek powinien zawierać poprawną informację o zakresie uprawnień zgodnym z obowiązującym „Katalogiem zakresów uprawnień" stanowiącym załącznik nr 3 do niniejszej Instrukcji.

3. Administrator systemów informatycznych po akceptacji wniosku o przydzielenie zdalnego dostępu przekazuje pracownikowi imienny klucz i certyfikat dla aplikacji OpenVPN wraz z plikami konfiguracyjnymi. W tym celu wnioskujący pracownik osobiście zgłasza się do administratora systemów informatycznych z nośnikiem danych, np. pendrive. Zabronione jest przesyłanie ww. kluczy, certyfikatów i plików konfiguracyjnych za pośrednictwem poczty elektronicznej, usług ftp, itp.
4. Administrator systemów informatycznych prowadzi rejestr przydzielonych pracownikom na podstawie kluczy VPN dostępów zdalnych.
5. Przydział dostępu zdalnego do systemów wewnętrznych administratora może zostać cofnięty w następujących przypadkach:
    1) na wniosek pracownika;
    2) na wniosek odpowiednio rektora/prorektora/dziekana/kanclerza;
    3) w związku z zaprzestaniem pełnienia funkcji przez pracownika, na podstawie której dostęp został pierwotnie przyznany;
    4) w wyniku nieprzestrzegania procedur bezpieczeństwa zawartych w niniejszej Instrukcji.
6. Użytkownicy VPN obowiązani są do stosowania się do poniższych zasad:
    1) użytkownik uzyskujący zdalny dostęp do systemów wewnętrznych administratora samodzielnie pobiera, instaluje i konfiguruje aplikację OpenVPN według instrukcji: [...]

       W przypadku pracy zdalnej na komputerze służbowym aplikację pobiera, instaluje i konfiguruje dla użytkownika KSK.
    2) komputer użytkownika, na którym jest zainstalowana aplikacja OpenVPN musi mieć ustawione hasło do kont, zgodnie z obowiązującą u administratora polityką haseł, przedstawioną w § 9 i 10 niniejszej Instrukcji;
    3) użytkownik nie może zainstalowanego klucza VPN przekazywać ani przesyłać żadnej innej osobie;
    4) klucza VPN nie należy przesyłać za pośrednictwem poczty elektronicznej, nawet na swoje konto pocztowe;
    5) otrzymanego klucza VPN nie wolno kopiować, przenosić na inne komputery w miejscu pracy jak i poza miejscem pracy. Wyjątkiem jest sytuacja, w której komputer użytkownika jest niesprawny, wówczas tymczasowo klucz VPN może być skopiowany na inny komputer osobisty użytkownika który musi spełniać wymagania bezpieczeństwa wymienione w pkt. 6 ust. 2 niniejszego paragrafu. Po odzyskaniu sprawności uszkodzonego komputera, klucze VPN powinny zostać usunięte z tymczasowo wykorzystywanego komputera;
    6) po zestawieniu połączenia VPN cały ruch sieciowy pomiędzy komputerem zestawiającym połączenie, a siecią, do której zostało zestawione połączenie jest monitorowany i logowany;

7) po zestawieniu połączenia VPN zabronione jest skanowanie sieci, poszczególnych komputerów czy narażanie sieci na jakiekolwiek inne niebezpieczeństwo, w tym utratę danych;

8) użytkownik po nawiązaniu zdalnego połączenia i zalogowaniu się do wewnętrznych systemów administratora bierze pełną odpowiedzialność za wszelkie dokonane zmiany;

9) wszelkie problemy i naruszenia związane z otrzymanym kluczem VPN, w tym użycie klucza przez osobę trzecią, kradzież lub zaginięcie komputera, na którym jest zainstalowany klucz VPN należy bezzwłocznie zgłosić do administratora na formularzu zgłoszenia, wzór zgłoszenia incydentu stanowi załącznik nr 8 „Zgłoszenie wystąpienia incydentu" do Polityki bezpieczeństwa.

10) użytkownik, któremu z różnych przyczyn nie jest już potrzebny dostęp zdalny do wewnętrznych systemów administratora powinien jak najszybciej poinformować o tym administratora systemów informatycznych w celu unieważnienia przydzielonego klucza i certyfikatu.

PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. ZASADY OGÓLNE

§18

[…]

2. ZASADY TWORZENIA KOPII BEZPIECZEŃSTWA I KOPII ARCHIWALNYCH

§19

[…]

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§20

1. Koordynator systemów komputerowych prowadzi ewidencję przenośnych nośników informacji zawierających dane osobowe wraz z wyszczególnieniem użytkownika. Wszelkiego rodzaju przenośne nośniki informacji zawierające dane osobowe powinny być odpowiednio zabezpieczone kryptograficznie: KSK (stworzenie zaszyfrowanej przestrzeni dyskowej) lub sprzętowo (urządzenie posiadające odpowiednią funkcjonalność – uniemożliwiające zdjęcie fabrycznego szyfrowania) przed podłączeniem do stacji roboczej.
2. Użytkownicy zobowiązani są do przechowywania wszelkiego rodzaju nośników informacji (płyty CD, taśmy magnetyczne, pendrive) zawierających dane w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. Nośniki powinny być przechowywane w zamykanych szafach.
3. Nośniki przenośne z danymi archiwalnymi powinny być składowane w sposób bezpieczny. Dotyczy to zarówno zapewnienia właściwych warunków środowiskowych (temperatura, wilgotność,

ochrona przed wpływem pól elektromagnetycznych itp.), jak i zabezpieczenia przed dostępem osób nieupoważnionych.

4. Nośniki z danymi archiwalnymi składowane są u administratora w dedykowanym odpowiednio zabezpieczonym pomieszczeniu, do którego dostęp mają tylko upoważnieni pracownicy.
5. Nośniki informacji przechowywane są u administratora maksymalnie przez okres 3 miesięcy do czasu likwidacji.
6. Nośniki magnetyczne w celu zniszczenia poddawane są procesowi demagnetyzacji lub fizycznemu zniszczeniu. Płyty CD/DVD zostają uszkodzone mechanicznie przy użyciu niszczarki do płyt spełniającej wymagania normy DIN 66399 na poziomie bezpieczeństwa nie niższym niż 3.
7. Nośniki danych przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie. Nośniki te niszczone są komisyjnie, z czynności zniszczenia sporządzany jest protokół przechowywany u ASI/ KSK.

UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH

§21

1. Do sprzętu komputerowego zalicza się między innymi:
   1) komputery stacjonarne,
   2) komputery przenośne,
   3) tablety,
   4) smartphony,
   5) drukarki,
   6) monitory,
   7) routery,
   8) switch-e,
   9) inny sprzęt służący do przetwarzania danych,
   10) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.
2. Administrator systemu informatycznego/ Koordynator systemów komputerowych odpowiada za poprawne działanie sprzętu komputerowego. Czynność ta może być wykonywana przez współpracowników administratora lub poprzez podmioty zewnętrzne.
3. W przypadku wykorzystywania urządzeń mobilnych (m.in. laptop, tablet, smartphone) wymaga się zastosowania następujących środków bezpieczeństwa:
   1) blokada ekranu (pin/hasło/symbol graficzny),
   2) szyfrowanie pamięci/karty pamięci,
   3) program antywirusowy (aktualizacja sygnatur wirusów min. raz na dobę),
   4) wyłączanie nieużywanych usług (wi-fi, gprs/lte, bluetooth, nfc),

5) instalowanie oprogramowania z zaufanego źródła (np. iStore, Google Play).

4. Zakup i przekazanie sprzętu służbowego odbywa się wyłącznie za wiedzą ASI/KSK. Każdy sprzęt komputerowy mający dostęp do zasobów uczelni znajdujących się w Intranecie, jak również komputer korzystający z dostępu do Internetu poprzez sieć wewnętrzną uczelni musi być zabezpieczony przez ASI/KSK zgodnie z zapisami niniejszej Instrukcji. Przekazanie sprzętu jest to czynność polegająca na dostarczeniu użytkownikowi sprzętu komputerowego wraz z odpowiednim oprogramowaniem oraz kartą komputera zgodną ze wzorem stanowiącym załącznik nr 4 „Kartoteka komputera" do niniejszej Instrukcji. Karta wydawana jest w 2 egzemplarzach – jeden dla użytkownika komputera, drugi dla ASI/ KSK.
5. ASI/ KSK odpowiedzialny jest za przygotowanie sprzętu komputerowego do prawidłowej i zgodnej z przeznaczeniem pracy, czyli odpowiednie zabezpieczenie stanowiska komputerowego:

   a) przeznaczonego do pracy w wewnętrznych systemach uczelni poprzez: instalację wspieranego systemu operacyjnego oraz stworzenie kont z odpowiednimi uprawnieniami (administrator – instalacja/ odinstalowanie oprogramowania/ blokada/ odblokowywanie zewnętrznych nośników pamięci/ zdalny dostęp do komputera użytkownika; użytkownik – praca na zainstalowanym oprogramowaniu, brak możliwości ingerencji w konfigurację systemu), zainstalowanie aktualnego oprogramowania antywirusowego, stworzenie zaszyfrowanej przestrzeni dyskowej, konfiguracja systemowego wygaszacza ekranu;

   b) nieprzeznaczonego do pracy w wewnętrznych systemach uczelni (stanowiska komputerowe kadry dydaktycznej) poprzez: instalację wspieranego systemu operacyjnego oraz stworzenie kont z odpowiednimi uprawnieniami (administrator – instalacja/ odinstalowanie oprogramowania/ zdalny dostęp do komputera użytkownika; użytkownik – praca na zainstalowanym oprogramowaniu, brak możliwości ingerencji w konfigurację systemu), zainstalowanie aktualnego oprogramowania antywirusowego, stworzenie zaszyfrowanej przestrzeni dyskowej, konfiguracja systemowego wygaszacza ekranu;
6. ASI/ KSK jest zobowiązany do prowadzenia spisu wraz ze specyfikacją posiadanego pod opieką sprzętu komputerowego oraz oprogramowania z wyszczególnieniem użytkownika.
7. ASI/ KSK ma obowiązek przechowywać karty gwarancyjne, klucze i licencje do oprogramowania.
8. ASI/ KSK udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania.
9. Zabrania się bez wiedzy i zgody administratora podłączania urządzeń typu: switch, router i innych urządzeń sieciowych.
10. Zabrania się bez wiedzy i zgody administratora tworzenia własnych sieci bezprzewodowych.
11. Pracownik używający danego komputera bierze pełną odpowiedzialność za treści pobierane z sieci Internet. Prowadzony jest ciągły monitoring ruchu sieciowego z możliwością wyciągnięcia konsekwencji służbowych.
12. W przypadku korzystania z narzędzi wykorzystujących sztuczną inteligencję użytkownik jest zobowiązany zapewnić zgodność przetwarzania danych z niniejszą dokumentacją bezpieczeństwa informacji. Przede wszystkim powinien posiadać akceptację prawną umowy, na podstawie której przetwarzane są dane za pomocą tych narzędzi.

13. W przypadku niepoprawnego i niezgodnego z przeznaczeniem użytkowania przez użytkownika sprzętu komputerowego, ASI/ KSK informuje o powyższym administratora.
14. Administrator instaluje wyłącznie licencjonowane oprogramowanie lub oprogramowanie, które nie wymaga opłaty licencyjnej, zgodnie z warunkami licencji.
15. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także jest odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz za ochronę przed kradzieżą lub zagubieniem.
16. Użytkownik nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować lub usuwać oprogramowania, w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.
17. Użytkownik nie może udostępniać powierzonego mu sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.
18. Wykorzystywanie sprzętu prywatnego do celów służbowych odbywa się na własną odpowiedzialność pracownika.

KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ I WIZYJNEJ

§22

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany danych osobowych lub informacji poufnych u administratora, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
2. Odczytanie wiadomości z systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych”) haseł dla ww. urządzeń.
4. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających informacje wrażliwe.

MONITORING WIZYJNY

§23

1. Osoby znajdujące się w miejscu prowadzonych czynności wideo monitoringu muszą być tego świadome. Administrator podaje swoją nazwę, adres, obszar oraz cel monitorowania. Tablice informujące o zainstalowanym monitoringu powinny być widoczne, syntetyczne, umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc. Wymiary tablic muszą być proporcjonalne do miejsca, gdzie są umieszczone. Stosowane mogą być dodatkowo piktogramy informujące o objęciu dozorem kamer.
2. Wideo monitoring realizowany jest zgodnie z tzw. zasadą adekwatności. Przewiduje ona, że pozyskiwać można jedynie te dane, które są niezbędne dla osiągnięcia wyznaczonego z góry, zgodnego z prawem celu. Celem administratora jest zapewnienie bezpieczeństwa i porządku publicznego oraz ochrony osób i mienia, wideo monitoring stanowi element systemu

zabezpieczenia budynków, pomieszczeń i mienia (ciągi komunikacyjne, serwerownie, parkingi) oraz kontroli ruchu osobowego.

3. Dostęp do nagrań wideo mają wyłącznie osoby do tego upoważnione.
4. Nagrania są odpowiednio zabezpieczone, odczyt danych bieżących oraz zapis danych bieżących i archiwalnych możliwy jest po dokonaniu autoryzacji osoby poprzez wprowadzenie identyfikatora i hasła.
5. Nagrania przechowywane są w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
6. Informacje z monitoringu przechowywane są jedynie przez czas niezbędny dla celów monitorowania, tj. maksymalnie 90 dni. Nagrania dotyczące incydentów mogą być przechowywane dłużej – do czasu wyjaśnienia sprawy/ zakończenia odpowiednich postępowań.
7. Pracownicy wykonujący pracę w pomieszczeniach monitorowanych powinni zostać poinformowani o tym, że znajdują się w zasięgu kamer.

ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO PRZED UTRATĄ DANYCH SPOWODOWANĄ AWARIĄ ZASILANIA LUB ZAKŁÓCENIAMI W SIECI ZASILAJĄCEJ

§24

1. Wszystkie krytyczne systemy informatyczne powinny być zasilane z wydzielonej sieci oraz zabezpieczone przed krótkotrwałymi zanikami napięcia, przepięciami itp., przy pomocy zasilaczy awaryjnych (UPS).
2. Minimalny czas podtrzymywania zasilania za pomocą zasilaczy awaryjnych nie może być dla serwerów krótszy niż 30 minut. Dopuszcza się krótszy czas jeśli serwery posiadają funkcje automatycznego zamknięcia i uruchomienia po przywróceniu zasilania.

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

§25

1. Zidentyfikowanymi obszarami systemu informatycznego administratora narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.
2. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.
3. […]
4. Do sieci wewnętrznej „LAN” administratora, mającej dostęp do systemów wewnętrznych przetwarzających dane osobowe, dostęp posiadają urządzenia znajdującej się w ewidencji KSK, po ich odpowiednim zabezpieczeniu.
5. Za prawidłowe funkcjonowanie oprogramowania antywirusowego odpowiada Koordynator systemów komputerowych.

6. Oprogramowanie antywirusowe uruchamiane jest przy starcie systemu, a użytkownik nie posiada uprawnień do jego wyłączenia.
7. Konfiguracja programu antywirusowego zapewnia ciągłe monitorowanie otrzymywanych i wysyłanych, a także uruchamianych plików pod kątem występowania oprogramowania złośliwego.
8. Stacje robocze i komputery przenośne przynajmniej raz w miesiącu skanowane są pod kątem występowania na nich oprogramowania złośliwego.
9. Serwery plikowe podlegają skanowaniu pod kątem występowania na nich oprogramowania złośliwego przynajmniej raz w tygodniu.
10. Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
11. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik powinien skontaktować się odpowiednio z KSK.
12. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, KSK podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

    1) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego;

    2) odtworzenie plików z kopii zapasowych, po uprzednim sprawdzeniu, czy dane zapisane na kopiach zapasowych nie są zainfekowane;

    3) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z odpowiednim serwisem.

PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

§26

1. Konserwacja sprzętu komputerowego, systemów informatycznych oraz nośników informacji administratora ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy tych systemów, zapobieganie utracie, uszkodzeniu lub naruszeniu bezpieczeństwa.
2. Sprzęt podlega konserwacji w terminach wynikających z zapisów na karcie komputera stanowiącej załącznik nr 4 „Kartoteka komputera” do niniejszej Instrukcji.
3. Sprzęt podlega okresowym kontrolom pod kątem zastosowanych na nim zabezpieczeń technicznych. Okresowe kontrole przeprowadzone są przez KSK nie rzadziej niż raz na dwa lata. Okresowe kontrole odnotowywane są w kartotece komputera.
4. Wszelkie naprawy oraz konserwacje urządzeń komputerowych oraz zmiany w systemie informatycznym administratora przeprowadzane są – o ile to możliwe – przez upoważnionych pracowników administratora.
5. Naprawy, konserwacje i zmiany w systemie informatycznym administratora przeprowadzane przez serwisanta zewnętrznego prowadzone są pod nadzorem administratora systemu informatycznego

w siedzibie administratora (jeśli to możliwe) lub poza siedzibą administratora, po uprzednim usunięciu elementów zawierających dane osobowe i informacje poufne, o ile nie wiąże się to z nadmiernymi utrudnieniami.

6. Wszelkie prace, o których mowa powyżej, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie pomiędzy administratorem a tymże podmiotem, z uwzględnieniem odpowiednio w zależności od przedmiotu umowy: klauzuli powierzenia przetwarzania danych, klauzuli dotyczącej zachowania w poufności przez wykonawcę wszelkich informacji, do których ma dostęp w czasie wykonywania usługi lub/ oraz zapisów załącznika nr 10 „Zapisy do umów zawieranych z UJD dotyczących zdalnego serwisowania urządzeń będących własnością i znajdujących się w budynkach UJD" do niniejszej Instrukcji.
7. W przypadku zdalnej obsługi serwisowej systemów informatycznych administratora, porty komunikacyjne powinny być włączane jedynie na wyraźne żądanie dostawcy takich usług, za zgodą ASI i muszą być ponownie odłączone tuż po zakończeniu prac serwisowych.
8. Jeśli nośnik danych (dysk, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie w niszczarce spełniającej wymagania normy DIN 66399 na poziomie bezpieczeństwa nie niższym niż 3.

§27

1. Sprzęt komputerowy wykorzystywany przez wydziały uczelni w procesie rekrutacji na studia podlega dodatkowym sprawdzeniom.
2. KSK jest odpowiedzialny za przygotowanie stanowisk komputerowych i poprawne działanie sprzętu wykorzystywanego w procesie rekrutacji.
3. KSK odpowiedzialny jest za przygotowanie sprzętu komputerowego do prawidłowej i zgodnej z przeznaczeniem pracy, czyli odpowiednie zabezpieczenie stanowiska komputerowego:
   a) przeznaczonego do pracy dla członków Wydziałowej Komisji Rekrutacyjnej poprzez: instalację wspieranego systemu operacyjnego oraz stworzenie kont z odpowiednimi uprawnieniami (administrator – instalacja/ odinstalowanie oprogramowania/ blokada/ odblokowywanie zewnętrznych nośników pamięci/ zdalny dostęp do komputera użytkownika; użytkownik – praca na zainstalowanym oprogramowaniu, brak możliwości ingerencji w konfigurację systemu), zainstalowanie aktualnego oprogramowania antywirusowego, stworzenie zaszyfrowanej przestrzeni dyskowej, konfiguracja systemowego wygaszacza ekranu;
   b) przeznaczonego dla kandydatów ubiegających się o przyjęcie na studia poprzez: instalację wspieranego systemu operacyjnego oraz stworzenie konta z minimalnymi odpowiednimi uprawnieniami typu „gość" nie dającymi możliwości ingerencji w konfigurację systemu operacyjnego, zainstalowanie aktualnego oprogramowania antywirusowego.
4. System komputerowy przed oddaniem do pracy dla Wydziałowej Komisji Rekrutacyjnej powinien być sprawdzony przez KSK pod kątem obecności zbędnych plików i innych kont użytkowników oraz przeskanowany zainstalowanym oprogramowaniem antywirusowym.
5. KSK po przygotowaniu jednostki komputerowej dla Wydziałowej Komisji Rekrutacyjnej zobowiązany jest wypełnić załącznik nr 8 „ Przygotowanie stanowiska komputerowego do pracy w WKR" do niniejszej Instrukcji i przedłożyć go do podpisu dziekanowi wydziału oraz odnotować fakt oddelegowania komputera w kartotece komputera, której wzór stanowi załącznik nr 4 „Kartoteka komputera" do niniejszej Instrukcji.

6. Po zakończeniu rekrutacji, a przed oddaniem sprzętu do pracy na wydziale, KSK czyści dyski komputerów wykorzystywanych w rekrutacji z plików, które powstały podczas prac komisji oraz uzupełnia załącznik nr 8 „ Przygotowanie stanowiska komputerowego do pracy w WKR" do niniejszej Instrukcji i przedkłada do podpisu dziekanowi wydziału oraz uzupełnia kartotekę komputera, której wzór stanowi załącznik nr 4 „Kartoteka komputera" do niniejszej Instrukcji.
7. KSK jest zobowiązany przechowywać dla jednostki wykorzystywanej w procesie rekrutacji wraz z kartoteką komputera załącznik nr 8 „Przygotowanie stanowiska komputerowego do pracy w WKR" do niniejszej Instrukcji.

POSTANOWIENIA KOŃCOWE

§28

1. Dokumentacja bezpieczeństwa informacji stanowi wewnętrzną regulację administratora i obowiązuje wszystkich pracowników i współpracowników administratora.
2. Dokumentacja bezpieczeństwa informacji jest poufna i nie może być udostępniana podmiotom trzecim bez uprzedniej zgody administratora, z możliwością wyciągnięcia konsekwencji służbowych.
3. Dokumentacja bezpieczeństwa informacji obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u administratora. Wszelkie jej zmiany obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u administratora.
4. Każdy kto przetwarza dane posiadane przez administratora zobowiązany jest do stosowania przy przetwarzaniu danych postanowień zawartych w niniejszej dokumentacji.
5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
6. W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy.

WYKAZ ZAŁĄCZNIKÓW:

Załącznik nr 1 *„Wniosek o nadanie/ zmianę/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych"*

Załącznik nr 2 *„Wniosek o nadanie/ odebranie uprawnień do systemu informatycznego bez dostępu do danych osobowych"*

Załącznik nr 3 *„Katalog zakresów uprawnień w poszczególnych systemach"*

Załącznik nr 4 *„Kartoteka komputera"*

Załącznik nr 5 *„Wykaz tworzonych kopii zapasowych"*

Załącznik nr 6 *„Rejestr odtworzenia systemu z kopii zapasowej"*

Załącznik nr 7 *„Wniosek o przydzielenie zdalnego dostępu do wewnętrznego systemu informatycznego"*

Załącznik nr 8 *„Przygotowanie stanowiska komputerowego do pracy w WKR"*

Załącznik nr 9 *„Procedury odtwarzania systemów informatycznych w Uniwersytecie Jana Długosza w Częstochowie”*

Załącznik nr 10 *„Zapisy do umów zawieranych z UJD dotyczących zdalnego serwisowania urządzeń będących własnością i znajdujących się w budynkach UJD”*