ZARZĄDZENIE NR 36
Rektora Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie
z dnia 28 czerwca 2016 r.

w sprawie ochrony danych osobowych przetwarzanych w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie

Na podstawie art. 66 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (tekst jedn. Dz. U. z 2012 r. poz. 572 z późn. zm.), art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2015 r. poz. 2135, z późn. zm.) oraz § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024), zarządza się, co następuje:

§ 1.

1. Przetwarzanie danych osobowych w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie służy realizacji zadań wynikających z art. 13 ust. 1 ustawy prawo o szkolnictwie wyższym.
2. Zarządzenie stosuje się do przetwarzania danych osobowych w systemach informatycznych, na dokumentach źródłowych, takich jak: kartoteki, skorowidze, księgi, wykazy oraz w innych zbiorach ewidencyjnych jednostek organizacyjnych uczelni.

§ 2.

Sprawy sporne związane z ochroną danych osobowych rozstrzyga rektor.

§ 3.

1. Administratorem Danych Osobowych (ADO) w rozumieniu ustawy o ochronie danych osobowych, przetwarzanych w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie jest rektor.
2. Ilekroć w niniejszym zarządzeniu jest mowa o jednostce organizacyjnej, rozumie się przez to: wydziały, jednostki pozawydziałowe (międzywydziałowe i ogólnouczelniane) oraz piony organizacyjne administracji określone w Regulaminie organizacyjnym administracji Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie.

§ 4.

Obowiązki wynikające z ustawy o ochronie danych osobowych rektor przekazuje:
1) dziekanom – w zakresie pracowników, studentów, uczestników studiów doktoranckich oraz innych osób uczestniczących w różnych formach kształcenia prowadzonych na wydziale;
2) kierownikom jednostek międzywydziałowych – w zakresie pracowników podległych im jednostek, studentów oraz innych osób uczestniczących w różnych formach kształcenia prowadzonych w tych jednostkach;
3) prorektorowi ds. kształcenia – w zakresie pracowników podległych komórek organizacyjnych oraz jednostek ogólnouczelnianych w zakresie przetwarzanych danych osobowych, uczestników studiów doktoranckich oraz uczestników studiów podyplomowych i kursów dokształcających;
4) prorektorowi ds. studenckich – w zakresie pracowników podległych komórek organizacyjnych oraz jednostek ogólnouczelnianych w zakresie przetwarzanych danych osobowych studentów;
5) prorektorowi ds. nauki – w zakresie pracowników podległych komórek organizacyjnych oraz jednostek ogólnouczelnianych;
6) prorektorowi ds. organizacyjnych i rozwoju uczelni – w zakresie pracowników podległych komórek organizacyjnych oraz jednostek ogólnouczelnianych;
7) kanclerzowi – w zakresie pracowników podległych mu i jego zastępcom komórek organizacyjnych;

8) dyrektorowi Regionalnego Centrum Innowacji i Transferu Technologii – w zakresie pracowników podległych komórek organizacyjnych;

zwanymi dalej „lokalnymi administratorami danych osobowych".

§ 5.

Lokalni Administratorzy Danych Osobowych oraz kierownicy jednostek organizacyjnych ZUT, w których przetwarzane są dane osobowe mają obowiązek bieżącego aktualizowania dokumentacji dotyczącej ochrony danych osobowych zgodnie z wymogami niniejszego zarządzenia oraz wyznaczenia Lokalnego Administratora Bezpieczeństwa Informacji, który współpracuje z Administratorem Bezpieczeństwa Informacji w ZUT.

§ 6.

1. Lokalny Administrator Danych Osobowych jest zobowiązany dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w szczególności, aby były:
   a) przetwarzane zgodnie z prawem,
   b) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddane dalszemu przetworzeniu,
   c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   d) przechowywane w postaci umożliwiającej identyfikację osób, których dane dotyczą nie dłużej, niż jest to niezbędne do osiągnięcia celu przetworzenia.
2. Do zadań Lokalnego Administratora Danych Osobowych należy w szczególności:
   1) powołanie Lokalnego Administratora Bezpieczeństwa Informacji (LABI) w podległej jednostce organizacyjnej,
   2) udzielanie/anulowanie upoważnień do przetwarzania danych osobowych.
3. Lokalny Administrator Danych Osobowych odpowiada za:
   1) nadzór i kontrolę nad przestrzeganiem zasad przetwarzania danych osobowych,
   2) dopuszczanie do przetwarzania danych wyłącznie osób przeszkolonych i posiadających stosowne upoważnienia,
   3) nadzór nad działalnością LABI w podległej jednostce organizacyjnej.
4. Lokalny Administrator Danych Osobowych zobowiązany jest do stworzenia właściwych warunków organizacyjno-technicznych zapewniających ochronę danych osobowych przetwarzanych w podległej jednostce organizacyjnej oraz ich zabezpieczenie przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 7.

1. Rektor powołuje administratora bezpieczeństwa informacji (ABI).
2. ABI w zakresie bezpieczeństwa danych osobowych podlega bezpośrednio rektorowi jako Administratorowi Danych Osobowych.
3. Do zadań Administratora Bezpieczeństwa Informacji należy nadzorowanie zasad postępowania przy przetwarzaniu danych osobowych, a w szczególności:
   1) zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w Uczelni, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, pozyskaniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem, ściśle współpracując w tym zakresie z dyrektorem Uczelnianego Centrum Informatyki – pełniącym funkcje Administratora Systemu Informatycznego w ZUT,
   2) zapewnienie kontroli nad procesem przetwarzania danych osobowych w uczelni,
   3) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
   4) wnioskowanie o usunięcie uchybień w razie stwierdzenia naruszenia przepisów o ochronie danych osobowych,
   5) prowadzenie ewidencji lokalnych administratorów bezpieczeństwa informacji,
   6) prowadzenie ewidencji zbiorów danych przetwarzanych w Uczelni,
   7) prowadzenie ewidencji miejsc przetwarzania danych osobowych i sposobu ich

zabezpieczenia,
8) prowadzenie ewidencji oprogramowania wykorzystywanego w przetwarzaniu danych osobowych,
9) prowadzenie ewidencji wniosków o udostępnianie danych osobowych instytucjom i osobom spoza Uczelni,
10) kontrola uzupełnienia zakresów czynności osób zatrudnionych przy przetwarzaniu danych o obowiązki wynikające z ustawy o ochronie danych osobowych,
11) przeprowadzanie sprawdzeń mających na celu zweryfikowania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w jednostkach organizacyjnych uczelni (sprawdzenie), na polecenie rektora lub wniosek Generalnego Inspektora Ochrony Danych Osobowych oraz opracowanie w tym zakresie sprawozdania,
12) monitorowanie zmian w przepisach prawnych dotyczących sposobu zabezpieczenia danych osobowych,
13) monitorowanie i wdrażanie zaleceń i interpretacji Generalnego Inspektora Ochrony Danych Osobowych w zakresie ochrony danych osobowych w ZUT.

§ 8.

1. Pełnomocnik Rektora ds. ochrony informacji niejawnych – kierownik Sekcji Spraw Obronnych i Kancelarii Niejawnej pełni funkcję Administratora Bezpieczeństwa Informacji (ABI).
2. Administrator Bezpieczeństwa Informacji wykonuje swoje zadania przy pomocy:
   1) dyrektora Uczelnianego Centrum Informatyki – Administratora Systemu Informatycznego w ZUT,
   2) kierownika Działu Kadr,
   3) Lokalnych Administratorów Bezpieczeństwa Informacji wyznaczonych przez Lokalnych Administratorów Danych Osobowych,
   4) Lokalnych Administratorów Systemów Informatycznych wyznaczonych przez Administratora Systemu Informatycznego w Uczelni.

§ 9.

Administrator Systemu Informatycznego (Dyrektor Uczelnianego Centrum Informatyki) opracowuje zasady:
1) zapewniania awaryjnego zasilania komputerów i innych urządzeń mających wpływ na bezpieczeństwo przetwarzania informacji,
2) korzystania z komputerów przenośnych, w których przetwarzane są dane osobowe, a w szczególności autoryzacji dostępu do zbiorów danych osobowych,
3) nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych i nośników na których znajdują się dane osobowe,
4) nadawania identyfikatorów i zarządzania hasłami użytkowników oraz częstotliwości zmian haseł, które zawiera instrukcja określająca sposób zarządzania systemami informatycznymi służącymi przetwarzaniu danych osobowych, w tym zwłaszcza mechanizmów uwierzytelniania użytkowników w tych systemach,
5) nadzoru nad sprawdzeniem systemów informatycznych pod katem obecności nieuprawnionego oprogramowania, wirusów oraz zabezpieczeń przed atakami z sieci,
6) nadzoru nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących przetwarzaniu danych osobowych oraz innymi czynnościami wykonywanymi na zbiorach danych,
7) nadzoru nad systemami komunikacyjnymi w sieci komputerowej oraz przesyłanymi danymi,
8) nadzoru nad obiegiem i przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez systemy informatyczne,
9) podejmowania działań zabezpieczających stan systemu informatycznego w przypadku naruszenia jego zabezpieczeń.

§ 10.

Lokalny Administrator Danych Osobowych przekazuje Administratorowi Bezpieczeństwa Informacji kopię powołania lub odwołania Lokalnego Administratora Bezpieczeństwa Informacji.

§ 11.

Lokalny Administrator Bezpieczeństwa Informacji zobowiązany jest do:

1) gromadzenia oryginałów upoważnień do przetwarzania danych osobowych,
2) przekazywania kopii pisemnych upoważnień osób, które mogą być dopuszczone do przetwarzania danych osobowych do Działu Kadr celem włączenia do akt osobowych,
3) sporządzania wykazu osób upoważnionych do przetwarzania danych osobowych w danej jednostce organizacyjnej,
4) zaznajomienia osób zatrudnionych przy przetwarzaniu danych osobowych z obowiązującymi przepisami,
5) przestrzegania obowiązujących ustaleń w zakresie udostępniania danych osobowych instytucjom i osobom spoza Uczelni,
6) analizy sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych,
7) współdziałania z administratorami sieci komputerowych w zakresie nadzorowania i kontroli funkcjonowania i dostępu do systemów informatycznych wykorzystywanych do przetwarzania danych osobowych.

§ 12.

1. Udostępnianie danych osobowych w celach innych niż włączenie do zbioru odbiorcom danych może nastąpić wyłącznie na pisemny wniosek, chyba że przepis innej ustawy stanowi inaczej.
2. Udostępnianie instytucjom lub osobom spoza Uczelni danych osobowych może odbywać się wyłącznie zgodnie z przepisami prawa oraz za zgodą rektora.

§ 13.

1. Niezastosowanie się do prowadzonej przez Administratora Danych Osobowych polityki bezpieczeństwa informacji, której założenia określa niniejszy dokument i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie przepisów Kodeksu Pracy.
2. Niezależnie od rozwiązania stosunku pracy osoby nieprzestrzegające przepisów w zakresie ochrony danych osobowych podlegają odpowiedzialności karnej na podstawie przepisów rozdziału 8 ustawy o ochronie danych osobowych.

§ 14.

1. Zobowiązuje się Administratora Bezpieczeństwa Informacji do corocznych przeglądów polityki bezpieczeństwa informacji oraz jej aktualizowania stosownie do potrzeb.
2. W razie istotnych zmian dotyczących przetwarzania danych osobowych Administrator Bezpieczeństwa Informacji wnioskuje do rektora o przeprowadzenie przeglądu polityki bezpieczeństwa stosownie do potrzeb.
3. Administrator Bezpieczeństwa Informacji analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych odpowiadają przeprowadzonym zmianom:
   1) w systemie informatycznym,
   2) organizacji administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
   3) w obowiązującym prawie.
4. Administrator Bezpieczeństwa Informacji może w porozumieniu z Administratorem Danych Osobowych przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych.
5. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z osobami objętymi audytem.
6. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym zarówno przez Administratora Bezpieczeństwa Informacji, jak i Administratora Danych Osobowych.

7. Rektor może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowaną instytucję.

§ 15.

Sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych regulują:

1) „Polityka Bezpieczeństwa Danych Osobowych" stanowiąca załącznik nr 1 do niniejszego zarządzenia,
2) „Instrukcja Zarządzania Systemami Informatycznymi" stanowiąca załącznik nr 2 do niniejszego zarządzenia.
3) „Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych" stanowiąca załącznik nr 3 do niniejszego zarządzenia.

§ 16.

Lokalni Administratorzy Danych Osobowych w terminie do dnia 30 stycznia każdego roku, przekazują w formie elektronicznej do Administratora Bezpieczeństwa Informacji następujące informacje :

1) dane kontaktowe Lokalnych Administratorów Bezpieczeństwa Informacji;
2) wykaz zbiorów danych osobowych przetwarzanych w jednostce organizacyjnej z określeniem:
   - miejsc przetwarzania danych osobowych,
   - sposobu zabezpieczenia miejsc przetwarzania,
   - wykazu osób przetwarzających dane osobowe;
3) informacje powyższe przekazywane są według wzorów określonych w Polityce Bezpieczeństwa Danych Osobowych.

§ 17.

Sprawdzenie zgodności przetwarzania danych osobowych z przepisami prawa, przeprowadza Administrator Bezpieczeństwa Informacji przy pomocy Administratora Systemu Informatycznego.

§ 18.

Ochronę danych osobowych w zakresie monitoringu wizyjnego w obiektach uczelni, reguluje odrębne zarządzenie rektora uczelni.

§ 19.

Tracą moc:

1) zarządzenie nr 38 Rektora ZUT z dnia 20 maja 2010 r. w sprawie ochrony danych osobowych,
2) zarządzenie nr 17 Rektora ZUT z dnia 18 marca 2011 r. w sprawie wprowadzenia „Polityki bezpieczeństwa przetwarzania danych osobowych w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie",
3) zarządzenie nr 23 Rektora ZUT z dnia 29 kwietnia 2015 r. w sprawie powołania administratora bezpieczeństwa informacji w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie.

Rektor

prof. dr hab. inż. Włodzimierz Kiernożycki

Załącznik nr 1
do zarządzenia nr 36 Rektora ZUT z dnia 28 czerwca 2016 r.

POLITYKA
BEZPIECZEŃSTWA DANYCH OSOBOWYCH

I Podstawa prawna

1. Dane osobowe w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie, przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:
   1) przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2015 r. poz. 2135, z późn. zm.) oraz przepisów wykonawczych wydanych z upoważnienia tej ustawy,
   2) innych przepisów prawnych normujących przetwarzanie danych osobowych określonych kategorii.
2. Dane osobowe w ZUT przetwarzane są w celu realizacji statutowych celów szkoły wyższej. W szczególności dane osobowe przetwarza się:
   1) dla zabezpieczania prawidłowego toku realizacji zadań dydaktycznych, naukowych i organizacyjnych Uczelni wynikających z przepisów ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (tekst jedn. Dz. U. z 2012 r. poz. 572, z późn. zm.),
   2) dla zapewnienia prawidłowej, zgodnej z prawem i celami Uczelni polityki personalnej oraz bieżącej obsługi stosunków pracy nawiązywanych przez Uczelnię,
   3) dla realizacji innych celów i zadań ZUT – z poszanowaniem praw i wolności osób powierzających ZUT swoje dane.

II Podstawowe definicje

Przez użyte w dokumencie określenia rozumie się:

1) **jednostka** – jednostka organizacyjna ZUT: wydział, jednostka pozawydziałowa (międzywydziałowa i ogólnouczelniana) oraz pion organizacyjny administracji określony w Regulaminie organizacyjnym administracji Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie;
2) **jednostka prowadząca zbiór danych** – jednostka odpowiedzialna merytorycznie za wdrożenie i utrzymywanie struktury zbioru, zgodnie z poleceniem administratora danych osobowych oraz zgodnie z wymaganiami ustaw. Jednostka odpowiedzialna za prowadzenie zbioru danych może korzystać z pomocy innych jednostek, w szczególności jednostek odpowiedzialnych za wdrożenie i utrzymanie oprogramowania i baz danych oraz za wdrożenie i utrzymanie serwerów i sieci;
3) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) **dane wrażliwe** – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;
5) **odbiorca danych** – każdy, komu udostępnia się dane osobowe z wyłączeniem osoby, której dane dotyczą;
6) **administrator zbioru** – kierujący jednostką prowadzącą zbiór albo osoba wskazana przez niego, odpowiadająca za bieżące funkcjonowanie i bezpieczeństwo zbioru danych osobowych;
7) **Administrator Danych Osobowych (ADO)** – rektor;
8) **Lokalny Administrator Danych Osobowych (LADO)** – prorektorzy, dziekani, kanclerz, kierownicy jednostek międzywydziałowych, dyrektor RCIiTT;
9) **Administrator Bezpieczeństwa Informacji (ABI)** – osoba powołana przez rektora, nadzorująca przestrzeganie zasad ochrony przetwarzania danych osobowych w Uczelni;

10) **Administrator Systemu Informatycznego (ASI)** – osoba odpowiedzialna za przetwarzanie danych osobowych w systemie informatycznym, opiniowanie wniosków o nadawanie/cofanie zakresu uprawnień dostępu do systemu i sposobu zabezpieczenia tego dostępu, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tym systemie;
11) **Lokalny Administrator Bezpieczeństwa Informacji (LABI)** – osoba powołana przez **LADO**, odpowiedzialna za prowadzenie spraw związanych z udzielaniem upoważnień w zakresie przetwarzania danych osobowych w jednostce organizacyjnej ZUT oraz ich ochroną;
12) **Lokalny Administrator Systemów Informatycznych (LASI)** - osoba odpowiadającą za funkcjonowanie i bezpieczeństwo systemu informatycznego, zawierającego programy lub bazy danych zastosowane do przetwarzania danych osobowych, również w przypadku dostępu zdalnego i mobilnego do systemu, w szczególności z użyciem sieci Internet lub radiowej sieci bezprzewodowej, w tym z użyciem prywatnych urządzeń użytkowników, w sytuacjach gdy zostało to dozwolone przez administratora danych osobowych;
13) **zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
14) **przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
15) **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
16) **zabezpieczenie danych osobowych** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
17) **użytkownik systemu** – osoba posiadająca upoważnienie do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu wydanym przez LADO;
18) **identyfikator użytkownika/login** – ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym;
19) **hasło** – ciąg znaków literowych, cyfrowych lub innych specjalnych znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
20) **dostępność** – cecha zapewniająca użytkownikowi dostępność zasobów informacyjnych w wymaganym miejscu, czasie i formie;
21) **poufność** (danych) – właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
22) **integralność** (danych) – właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
23) **rozliczalność** – cecha zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
24) **sieć telekomunikacyjna** – sieć telekomunikacyjna w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (tekst jedn. Dz. U. z 2014 r. poz. 243, z późn. zm.);
25) **publiczna sieć telekomunikacyjna** – publiczna sieć telekomunikacyjna w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
26) **teletransmisja** –przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
27) **integralność danych** – właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
28) **raport** –przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
29) **poufność danych** – właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
30) **uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

III Cel i zakres stosowania dokumentu Polityka bezpieczeństwa danych osobowych

1. Celem Polityki Bezpieczeństwa Danych Osobowych, zwanej dalej Polityką Bezpieczeństwa, jest:
   1) zapewnienie właściwego poziomu bezpieczeństwa danych osobowych w ZUT poprzez wdrożenie odpowiedniego systemu ochrony przed zagrożeniami wewnętrznymi i zewnętrznymi,
   2) podniesienie poziomu świadomości pracowników ZUT co do istoty problemu bezpieczeństwa danych osobowych.
2. Polityka Bezpieczeństwa ma zastosowanie do wszystkich informacji zawierających dane osobowe: dokumentów papierowych, zapisów elektronicznych i innych będących własnością ZUT lub administrowanych przez ZUT i przetwarzanych w systemach informatycznych oraz tradycyjnych (papierowych).
3. Polityka bezpieczeństwa ma zastosowanie do wszystkich pracowników, studentów i doktorantów ZUT jak również osób trzecich mających dostęp do danych osobowych w ZUT.
4. Ochrona danych osobowych wynikająca z Polityki Bezpieczeństwa jest realizowana na każdym etapie przetwarzania informacji.
5. Przetwarzanie danych osobowych pracowników, studentów i doktorantów oraz innych osób służy realizacji zadań wynikających z art. 13 ust. 1 ustawy Prawo o szkolnictwie wyższym.
6. Przetwarzanie danych osobowych może odbywać się zarówno w systemach informatycznych, jak i w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.
7. Pracownicy ZUT, studenci i doktoranci oraz inne osoby, których dane są przetwarzane w jednostkach organizacyjnych ZUT, mają prawo do ochrony danych ich dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualnienia lub poprawiania jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.
8. Osoby zatrudnione w Uczelni przetwarzające dane osobowe każdego rodzaju, niezależnie od systemu przetwarzania:
   1) mogą przetwarzać dane osobowe wyłącznie w zakresie udzielonego upoważnienia, o którym mowa w pkt 10, i tylko w celu wykonywania nałożonych na nich obowiązków; zakres dostępu do danych przypisany jest do identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie; rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych,
   2) muszą zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania; przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia w Uczelni, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji,
   3) zapoznają się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
   4) zabezpieczają dane przed ich udostępnieniem osobom nieupoważnionym.
9. Indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych powinien określać także zakres odpowiedzialności za ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem – w stopniu odpowiednim do zadań.
10. Do przetwarzania danych osobowych i obsługi zbiorów informatycznych zawierających te dane mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez lokalnego administratora danych osobowych wraz z oświadczeniem potwierdzającym znajomość przepisów dotyczących ochrony danych osobowych, których wzory stanowią odpowiednio załączniki nr 1 i 2 do Polityki Bezpieczeństwa.
11. Upoważnienia mogą być wydawane bezterminowo lub na czas określony.
12. Lokalny Administrator Bezpieczeństwa Informacji zobowiązany do niezwłocznego przekazywania Administratorowi Bezpieczeństwa Informacji danych o wydanych przez LADO upoważnieniach do przetwarzania danych osobowych.
13. Lokalny Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w danej jednostce organizacyjnej zgodnie ze worem stanowiącym załącznik nr 3 do Polityki Bezpieczeństwa,
14. Kierownik jednostki organizacyjnej ZUT zobowiązany jest do uzupełnienia zakresu obowiązków pracowników w podległej jednostce o odpowiedzialność za ochronę danych osobowych.

15. Infrastrukturę przetwarzania danych osobowych obejmują rejestry i kartoteki prowadzone poza systemem informatycznym w formie dokumentów oraz sprzęt, urządzenia i oprogramowanie służące do przetwarzania danych w systemach informatycznych.
16. Wykaz obszarów przetwarzania danych osobowych i sposobu ich zabezpieczenia, wykaz zbiorów danych osobowych oraz programów wykorzystywanych do ich przetwarzania sporządza Lokalny Administrator Bezpieczeństwa Informacji w ramach danej jednostki i przekazuje Administratorowi Bezpieczeństwa Informacji w Uczelni, zgodnie z wzorami stanowiącymi odpowiednio załączniki nr 4 i 5 do Polityki Bezpieczeństwa.
17. Administrator Bezpieczeństwa Informacji prowadzi ewidencję Lokalnych Administratorów Danych Osobowych oraz Lokalnych Administratorów Bezpieczeństwa Informacji, zgodnie z załącznikiem nr 6 do Polityki Bezpieczeństwa.
18. Zbiory danych, używane podczas przetwarzania danych osobowych, są zbiorami pojedynczymi lub zbiorami stanowiącymi część bazy danych.
19. Przepływ danych w zintegrowanym systemie opisują instrukcje obsługi systemów.
20. Przepływ danych pomiędzy zintegrowanymi systemami następuje albo za pomocą mechanizmów eksportu/importu danych, albo w drodze współdziałania systemów na zasadzie użytkownik – serwer, kiedy to system użytkownik uzyskuje dane od systemu serwera automatycznie na życzenie.
21. Bezpieczeństwo osobowe – zachowanie poufności następuje w szczególności poprzez:
    a) dobór pracowników z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych; zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań,
    b) minimalizowanie ryzyka utraty bezpieczeństwa danych osobowych pojawiające się ze strony osób trzecich, mających dostęp do danych osobowych, przez podpisanie umów powierzenia przetwarzania danych osobowych.
22. Szkolenia w zakresie ochrony danych osobowych należy przeprowadzać dla:
    a) każdej osoby, która ma zostać upoważniona do przetwarzania danych osobowych,
    b) wszystkich osób upoważnionych do przetwarzania danych osobowych w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych,
    c) osób innych, jeżeli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.
23. Tematyka szkoleń obejmuje:
    a) przepisy i procedury dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
    b) sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą,
    c) obowiązki osób upoważnionych do przetwarzania danych osobowych i innych,
    d) odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych,
    e) zasady i procedury określone w polityce bezpieczeństwa informacji.

IV Zbiory danych osobowych

1. ABI przy współpracy z ASI prowadzi wykaz zbiorów danych osobowych obejmujący następujący zakres informacji o zbiorach danych:
    1) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych,
    2) programy komputerowe zastosowane do przetwarzania tych danych,
    3) powiązania między polami informacyjnymi,
    4) przepływ danych pomiędzy poszczególnymi systemami.
2. LABI oraz LASI są zobowiązani do przekazywania i aktualizacji informacji dotyczących zbiorów danych do ABI. Sposób przekazywania informacji ustala ABI przy współpracy z ASI.

V Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i dostępności przetwarzanych danych osobowych

1. Zarządzanie bezpieczeństwem danych osobowych jest procesem ciągłym, realizowanym przy współdziałaniu wszystkich uczestników tego procesu, którymi są: ADO, LADO, ABI, ASI, LABI, LASI oraz użytkownicy systemów.
2. LADO powołują Lokalnych Administratorów Bezpieczeństwa Informacji. Wzór dokumentu powołania LABI określa załącznik nr 7.

3. Kopię dokumentu powołania LABI ewidencjonuje i przechowuje ABI.
4. ADO powołuje Administratora Systemu Informatycznego (ASI). Administratorowi Systemu Informatycznego podlegają LASI. Wzór powołania ASI i LASI stanowią odpowiednio załączniki nr 8 i 9 do Polityki Bezpieczeństwa..
5. W celu organizacji zasad ochrony, zabezpieczenia i kontroli przetwarzania danych osobowych w ZUT, rektor wyznacza Administratora Bezpieczeństwa Informacji (ABI).
6. Politykę bezpieczeństwa w zakresie ochrony danych osobowych realizuje się w wyznaczonych budynkach, pomieszczeniach, tworzących obszar uczelni, w którym przetwarzane są dane osobowe.
7. Za obszar przetwarzania danych uznaje się obszar, w którym wykonywana jest choćby jedna z czynności wymienionych w rozdz. II pkt 14.
8. ABI prowadzi wykaz budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe w uczelni.

VI Dostęp do pomieszczeń ZUT, w których przetwarzane są dane osobowe

1. Dostęp do pomieszczeń ZUT, w których przetwarzane są dane osobowe podlega całodobowej kontroli.
2. Kontrola dostępu polega na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia lub budynku oraz godzinę pobrania lub zdania klucza. Funkcję kontrolną w tym zakresie wypełnia LADO.
3. Kierownicy jednostek organizacyjnych ZUT, w których przetwarzane są dane osobowe, zobowiązani są do niezwłocznego przekazywania do ABI wiadomości o zmianie lub powstaniu nowej lokalizacji miejsc przetwarzania danych osobowych.
4. Uczelnia na potrzeby polityki bezpieczeństwa w zakresie ochrony danych osobowych może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.
5. W przypadku gdy w pomieszczeniu znajduje się część ogólnodostępna oraz część, w której przetwarzane są dane osobowe – część, w której są przetwarzane dane osobowe powinna być wyraźnie oddzielona od ogólnodostępnej.
6. Wydzielenie części pomieszczenia, w której przetwarza się dane osobowe może być w szczególności realizowane poprzez montaż barierek, lad lub odpowiednie ustawienie mebli biurowych, uniemożliwiające lub co najmniej ograniczające niekontrolowany dostęp osób niepowołanych do zbiorów danych osobowych przetwarzanych w danym pomieszczeniu.
7. Opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających używane aktualnie zbiory danych osobowych. W szczególności w razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzana danych osobowych, obowiązany jest on umieścić zbiory występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiającym dostęp do danych osobowych osobom niepowołanym.
8. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne, i jako takie traktowane będzie, jako naruszenie podstawowych obowiązków pracowniczych.

VII Dostęp do danych osobowych

1. Dostęp do danych osobowych następuje na podstawie upoważnienia do przetwarzania danych osobowych, o którym mowa w rozdziale III pkt 11.
2. Administrator Bezpieczeństwa Informacji prowadzi:
   a) ewidencję osób upoważnionych do przetwarzania danych osobowych w ZUT,
   b) wykaz podmiotów i osób, którym udostępniono dane zgodnie z określonymi wzorami stanowiącymi załączniki nr 10 i 11 do Polityki Bezpieczeństwa.
   c) wykaz podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych osobowych w rozumieniu art. 31 ustawy zgodnie z określonym wzorem stanowiącym załącznik nr 12 do Polityki Bezpieczeństwa.
3. Z chwilą ustania stosunku pracy wygasa upoważnienie do przetwarzania danych osobowych.

VIII Dostęp do danych przetwarzanych tradycyjnie lub w systemach informatycznych

1. Każdy użytkownik posiadający upoważnienie do przetwarzania danych osobowych w systemie informatycznym otrzymuje od LASI jednoznaczny i niepowtarzalny identyfikator do systemu oraz ustala hasło o złożoności zgodnej z obowiązującym poziomem bezpieczeństwa.
2. Sposób uwierzytelnienia użytkownika w systemie informatycznym określa Instrukcja Zarządzania Systemami Informatycznymi, stanowiąca załącznik nr 2 do zarządzenia nr 36 Rektora ZUT z dnia 28 czerwca 2016 r. w sprawie ochrony danych osobowych przetwarzanych w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie.
3. Użytkownicy zobowiązani są do:
   a) ścisłego przestrzegania zakresu nadanego upoważnienia;
   b) przetwarzania i ochrony danych osobowych zgodnie z przepisami;
   c) zachowania w tajemnicy loginów i haseł uwierzytelniających użytkownika w systemie do przetwarzania danych osobowych;
   d) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
   e) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa ochrony danych osobowych oraz niewłaściwym funkcjonowaniem systemu przetwarzania danych.
4. Pod szczególną ochroną przed niepowołanym dostępem do danych osobowych pozostają urządzenia wchodzące w skład systemu informatycznego ZUT. W szczególności stacje robocze (poszczególne komputery) wchodzące w skład tego systemu, powinny być umiejscawiane w sposób uniemożliwiający osobom nieuprawnionym, bezpośredni i niekontrolowany dostęp do ekranów oraz urządzeń służących do przetwarzania, a zwłaszcza kopiowania danych.
5. Dane w rejestrach papierowych przetwarzane tradycyjnie przechowuje się w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.

IX Przetwarzanie danych osobowych z wykorzystaniem systemów informatycznych

1. Dane osobowe w ZUT są przetwarzane przy zastosowaniu systemów informatycznych, w zbiorach ewidencyjnych oraz poza zbiorami.
2. ABI oraz ASI zatwierdzają poziom bezpieczeństwa systemów informatycznych do przetwarzania danych osobowych zgodnie ze wzorem określonym w załączniku nr 13.
3. Za zabezpieczenie systemu informatycznego zgodnie z zatwierdzonym poziomem bezpieczeństwa odpowiada ASI.
4. ASI stosuje wszelkie dostępne mu mechanizmy ochrony celem właściwego zabezpieczenia systemu do przetwarzania danych.
5. Dla każdego systemu przetwarzania danych osobowych ASI przygotowuje procedurę zgodnie z Instrukcją Zarządzania Systemami Informatycznymi i przekazują je do ABI.
6. Systemy informatyczne służące do przetwarzania danych osobowych zabezpieczone są przed działaniami niepożądanymi na bieżąco aktualizowanymi systemami antywirusowymi.
7. Zbiory danych osobowych zlokalizowane są w przedmiotowych bazach danych umieszczonych na serwerach bazodanowych.
8. Dane osobowe w zbiorach są przetwarzane tylko w aplikacjach (programach) dostosowanych do merytorycznych potrzeb jednostek organizacyjnych ZUT.
9. Zawartość pól informacyjnych, występujących w aplikacjach (programach) zastosowanych do przetwarzania danych, musi być zgodna z przepisami prawa. Opisy wykonywane są w postaci wydruków zrzutów ekranowych lub struktur tablic bazy prezentujących zawartość pól informacyjnych i powiązań pomiędzy nimi. W przypadku braku możliwości uzyskania wydruku zrzutu ekranowego ASI sporządza inne dostępne opisy struktury zbioru.
10. Opisy struktur zbiorów danych wskazujące zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi wykonują ASI na podstawie aplikacji zastosowanych do przetwarzania tych danych, jeżeli opisów nie uzyskano od dostawców oprogramowania.
11. Schematy przepływu danych pomiędzy systemami informatycznymi przetwarzającymi dane osobowe wykonują poszczególni LASI, w uzgodnieniu z użytkownikami tych systemów i integratorem systemów w uczelni Uczelnianego Centrum Informatyki.

12. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (w szczególności płyty CD i DVD, taśmy streamera, dysku wymiennego, pamięci flash) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu (importu) danych za pomocą teletransmisji (w szczególności poprzez wewnętrzną sieć komputerową).

X Archiwizowanie danych osobowych, niszczenie wydruków i zapisów na nośnikach magnetycznych

1. Kopie bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych wykonywane są zgodnie z Instrukcją Zarządzania Systemem Informatycznym dla każdego z systemów przetwarzania danych.
2. Harmonogram archiwizacji danych osobowych zawiera Instrukcja Zarządzania Systemami Informatycznymi dla każdego z systemów przetwarzania danych.
3. Za prawidłowe wykonanie kopii bezpieczeństwa odpowiada właściwy LASI.
4. Sposoby przechowywania, oznaczania i niszczenia nośników kopii bezpieczeństwa zawiera Instrukcja Zarządzania Systemami Informatycznymi dla danego systemu przewarzania.
5. Uszkodzone nośniki magnetyczne, przed ich wyrzuceniem, są fizycznie niszczone w sposób uniemożliwiający ich odczytanie. Skuteczność zniszczenia jest potwierdzana przez LASI oraz LABI.
6. Nośniki magnetyczne przekazywane na zewnątrz nie mogą zawierać zapisów z danymi osobowymi. Sposób postępowania z nośnikami magnetycznymi określa Instrukcja Zarządzania Systemami Informatycznymi.
7. Po wykorzystaniu dokumenty w formie papierowej, zawierające dane osobowe, niszczone są w sposób uniemożliwiający ich odczytanie.

XI Szkolenia

1. Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych ZUT zapewnia zaznajomienie osób upoważnionych do przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi w uczelni, a także z ich zmianami, w szczególności poprzez:
   a) instruktaż na stanowisku pracy,
   b) szkolenie wewnętrzne realizowane na terenie Uczelni (także e-learning),
   c) szkolenie zewnętrzne.
2. W przypadku dostępu do danych osobowych przetwarzanych w systemie informatycznym, podstawowe szkolenie w zakresie procedur rozpoczęcia, zawieszenia i zakończenia pracy w systemie oraz mechanizmów zabezpieczenia stanowiska roboczego przeprowadza LABI wraz z LASI.

XII Zapewnienie ciągłości działania systemów

1. Pomieszczenia, w których znajdują się kluczowe dla ZUT elementy systemów informatycznych posiadają dwa źródła zasilania.
2. Kluczowe urządzenia są podłączone do urządzeń podtrzymujących napięcie (UPS) w celu umożliwienia bezpiecznego wyłączenia systemu w przypadku awarii zasilania oraz przełączenia źródła zasilania, np. na agregat prądotwórczy.
3. W czasie gdy kluczowy dla funkcjonowania ZUT sprzęt informatyczny uległ awarii Uczelniane Centrum Informatyki zapewnia sprzęt o właściwościach identycznych lub przewyższających go funkcjonalnością.
4. Serwisowanie urządzeń i sprzętu związanego z bezpieczeństwem przetwarzania informacji powinno następować w możliwie krótkim czasie od wykrycia jego awarii.
   Szybkie przywrócenie właściwego stanu technicznego urządzeń ma na celu wyeliminowanie z użycia sprzętu, który nie spełnia parametrów określonych przez szczegółowe instrukcje dotyczące elementów systemu przetwarzania danych osobowych. W szczególności oznacza to, iż nie jest dopuszczalne rezygnowanie z zabezpieczeń z powodu ich wadliwego działania spowodowanego awarią.

5. Dla każdego systemu przetwarzania danych osobowych ASI opracowuje procedury związane z ciągłością działania zawarte w Instrukcji Zarządzania Systemem Informatycznym.
6. ABI wraz z ASI inicjują, nadzorują i przekazują do zatwierdzenia przez Rektora dokumenty uzupełniające proces zarządzania ciągłością działania uczelni, w zakresie przetwarzania zbiorów danych osobowych.

XIII Dostęp osób trzecich do danych osobowych przetwarzanych w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie

1. Dane osobowe mogą być udostępnione na pisemny, umotywowany wniosek zawierający informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazuje zakres i sposób wykorzystania danych osobowych.
2. Podstawą udzielania osobom trzecim dostępu do danych osobowych przetwarzanych w ZUT są:
   a) obowiązek udzielania dostępu wynikający z przepisów prawa,
   b) umowa zawarta pomiędzy ZUT a osobami trzecimi.
3. Umowy o współpracy Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie z instytucjami i podmiotami gospodarczymi powinny zawierać zapisy dotyczące ochrony danych osobowych.
4. Udostępnianie danych osobowych instytucjom i osobom spoza Uczelni odbywa się według procedury:
   a) wniosek opiniuje odpowiedni LADO,
   b) LADO przekazuje wniosek do ABI, który rejestruje wniosek i wydaje opinię,
   c) na wniosek odpowiada LADO zgodnie z opinią ABI.
5. Umowy zawierane przez uczelnię z osobami trzecimi związane z dostępem tych osób do danych osobowych przetwarzanych w ZUT, muszą zawierać klauzule określające bezpieczeństwo danych osobowych zgodne z Polityką Bezpieczeństwa Danych Osobowych oraz zobowiązanie do zachowania poufności.
6. Umowy z osobami trzecimi, związane z dostępem tych osób do danych osobowych przetwarzanych w ZUT zawierają, w szczególności:
   l) cel i zakres udzielonych praw dostępu do danych osobowych przetwarzanych w ZUT,
   2) prawa i obowiązki związane z udzielonym dostępem oraz okres ich obowiązywania,
   3) oświadczenie o znajomości:
      a) ustawy z dnia 6 czerwca 1997 r. Kodeks Karny rozdział XXXIII (Dz. U. Nr 88, poz. 553 z późn. zm.),
      b) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2015 r. poz. 2135, z późn. zm.),
      c) Polityki Bezpieczeństwa Danych Osobowych w ZUT,
   4) zasady związane ze zmianą składu personelu świadczącego usługi,
   5) tryb rozwiązywania kwestii spornych dotyczących bezpieczeństwa danych osobowych przetwarzanych w ZUT.
7. Przed zawarciem umowy, oraz okresowo w trakcie jej realizacji, ABI może przeprowadzić analizę następujących elementów związanych z dostępem osoby trzeciej do danych osobowych przetwarzanych w ZUT:
   1) aktualnego stanu zasadności (powodów, konieczności) udzielenia dostępu,
   2) rodzaju wymaganego dostępu (np. fizyczny, logiczny),
   3) aktualnego stanu wymagań bezpieczeństwa związanego z dostępem osób trzecich,
   4) ryzyka związanego z faktem przebywania osób trzecich na terenie ZUT oraz z ich dostępem do danych osobowych przetwarzanych w ZUT.
8. W przypadku stwierdzenia braku odpowiedniego poziomu ochrony ADO może rozwiązać umowę.
9. Przed wyborem dostawcy systemów i usług związanych z przetwarzaniem danych ABI zobowiązany jest do określenia wymagań bezpieczeństwa wobec:
   1) dostawcy,
   2) elementów systemu przetwarzania związanych z przedmiotem umowy.

XIV Postanowienia końcowe

1. Integralną część niniejszej Polityki Bezpieczeństwa stanowią:
   1) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe,
   2) wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
   3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
   4) sposób przepływu danych pomiędzy systemami do przetwarzania danych osobowych.
2. Informacje, o których mowa w ust. 1, są przechowywane i aktualizowane przez Administratora Bezpieczeństwa Informacji w ZUT i wyłączone są z publikacji w bazie aktów prawnych ZUT.

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Panią/Pana
   .....
   zatrudnioną/-ego na stanowisku .....
   w .....

   do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:
   – .....
   – .....
   – .....
   – .....
   – .....

2. Identyfikator/Login: .....

3. Okres trwania upoważnienia: .....

Wystawił: .....
(podpis i pieczątka
Lokalnego Administratora Danych Osobowych)

Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....

Załącznik nr 2
do Polityki Bezpieczeństwa Danych Osobowych

OŚWIADCZENIE

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz .....

Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2015 r. poz. 2135, z późn. zm.), w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

.....
(data i podpis osoby oświadczającej)

Załącznik nr 3
do Polityki Bezpieczeństwa Danych Osobowych

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Imię i nazwisko	Stanowisko/komórka organizacyjna	Zakres *(określenie, do jakich zbiorów dana osoba ma dostęp)*	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator/Login w danym systemie informatycznym
1.						
2.						
3.						
4.						
5.						
6.						
7.						

Załącznik nr 4
do Polityki Bezpieczeństwa Danych Osobowych

WYKAZ POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

(wszystkie miejsca, pomieszczenia, pokoje, w których dokonuje się operacji na danych osobowych)

Lp.	Lokalizacja – adres	Precyzyjne określenie pomieszczenia	Dział/osoba użytkująca pomieszczenie	Zabezpieczenie pomieszczenia
1.				
2.				
3.				
4.				
5.				
6.				
7.				

(S) - serwer, (K) - miejsce przechowywania kopii bezpieczeństwa, (P) – pomieszczenie, w którym przetwarza się dane osobowe, (AP) - archiwum zbiorów papierowych (KR) - kraty w oknach, (A) - alarm, (W) - wzmocnione drzwi, (B) – brak

Załącznik nr 5
do Polityki Bezpieczeństwa Danych Osobowych

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

Lp.	Nazwa zbioru danych osobowych	Podstawa prawna upoważniająca do prowadzenia zbioru	Cel przetwarzania danych w zbiorze	Opis kategorii osób, których dane są przetwarzane	Zakres danych przetwarzanych w zbiorze	Sposób zbierania danych	Sposób udostępniania danych	Oznaczenie odbiorcy danych	Historia zmian
1.									
2.									
3.									
4.									
5.									
6.									
7.									
8.									
9.									

Załącznik nr 6
do Polityki Bezpieczeństwa Danych Osobowych

EWIDENCJA LOKALNYCH ADMINISTRATORÓW DANYCH OSOBOWYCH ORAZ LOKALNYCH ADMINISTRATORÓW BEZPIECZEŃSTWA INFORMACJI

Lp.	Nazwisko i imię	Jednostka	Funkcja (LADO/LABI)	Podstawa powołania
1.				
2.				
3.				
4.				
5.				
6.				

Załącznik nr 7
do Polityki Bezpieczeństwa Danych Osobowych

Szczecin, ...

.....
(pieczęć jednostki)

POWOŁANIE
LOKALNEGO ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI – (LABI)

Nr .....*

Celem spełnienia wymogów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. 2015 r. poz. 2135, z późn. zm.)

Powołuję Panią/Pana .....
(imię i nazwisko)

zatrudnioną/nego na stanowisku .....

w .....
(nazwa jednostki / komórki organizacyjnej)

do pełnienia funkcji **Lokalnego Administratora Bezpieczeństwa Informacji.**

na okres od ..... do .....

.....
podpis LADO

otrzymują:

1. oryginał – LABI
2. kopie: Dział Kadr, ABI

Załącznik nr 8
do Polityki Bezpieczeństwa Danych Osobowych

.....
miejscowość, data

UPOWAŻNIENIE DLA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO (ASI)

Na podstawie rozdziału V pkt 4 Polityki Bezpieczeństwa Danych Osobowych, stanowiącej załącznik nr 1 do zarządzenia nr 36 Rektora ZUT z dnia 28 czerwca 2016 r. w sprawie ochrony danych osobowych przetwarzanych w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie, z dniem ..... wyznaczam Administratora Systemu Informatycznego (ASI), powierzając tę funkcję Panu/Pani ..... posługującemu/-ej się numerem PESEL: ..... .

.....
podpis i pieczątka
Administratora Danych Osobowych (ADO)

Ja, niżej podpisany/-a, zobowiązuję się do pełnienia obowiązków Administratora Systemu Informatycznego w oparciu o obowiązujące przepisy dotyczące ochrony danych osobowych, ze szczególnym uwzględnieniem przepisów wewnętrznych w sprawie ochrony danych osobowych przetwarzanych w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie.

.....
podpis i pieczątka ASI

Załącznik nr 9
do Polityki Bezpieczeństwa Danych Osobowych

Szczecin, ...

.....
(pieczęć jednostki)

POWOŁANIE
LOKALNEGO ADMINISTRATORA SYSTEMU INFORMATYCZNEGO – (LASI)
Nr .....*

Celem spełnienia wymogów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2015 r. poz. 2135, z późn. zm.)

Powołuję Panią/Pana .....
(imię i nazwisko)

zatrudnioną/nego na stanowisku .....

w .....
(nazwa jednostki / komórki organizacyjnej)

do pełnienia funkcji **Lokalnego Administratora Systemu Informatycznego.**

na okres od ..... do .....

.....
podpis i pieczątka ASI

.....
(podpis Administratora Bezpieczeństwa Informacji)

Otrzymują:
1. oryginał – LASI
2. kopie: ASI, ABI

Załącznik nr 10
do Polityki Bezpieczeństwa Danych Osobowych

WYKAZ UDOSTĘPNIEŃ DANYCH INNYM PODMIOTOM

Lp.	**Imię i Nazwisko/ Nazwa zbioru** *(możliwie najpełniejszy opis osoby, której dane zostały udostępnione lub całego zbioru)*	**Data udostępnienia**	**Nazwa podmiotu, któremu udostępniono dane** *(np. upoważniony organ, instytucja lub inny, który wykazał uprawnienie do udostępnienia mu danych)*	**Cel udostępnienia** *(podstawa prawna/numer umowy)*	**Zakres udostępnionych danych** *(jakie dane zostały udostępnione)*	**Rodzaj zbioru/zasobu i jego lokalizacja** *(np. papierowy wydruk, dane w formie elektronicznej)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						

Załącznik nr 11
do Polityki Bezpieczeństwa Danych Osobowych

WYKAZ UDOSTEPNIEŃ DANYCH OSOBOWYCH OSOBOM KTÓRYCH DOTYCZĄ

Lp.	Nazwa podmiotu, któremu powierzono dane	Data powierzenia	Cel powierzenia oraz numer umowy powierzenia	Zakres powierzonych danych *(jakie dane zostały powierzone)*	Określenie zbioru/zasobu
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Załącznik nr 12
do Polityki Bezpieczeństwa Danych Osobowych

WYKAZ PODMIOTÓW, Z KTÓRYMI ZAWARTO UMOWY POWIERZENIA PRZETWARZANIA.

L.p.	Imię i nazwisko osoby, której dane są udostępniane	Data udostępnienia	Rodzaj zbioru/zasobu i jego lokalizacja *(np. papierowy wydruk danych zawartych w określonym zbiorze)*
1.			
2.			
3.			
4.			
5.			
6.			
7.			

Załącznik nr 13
do Polityki Bezpieczeństwa Danych Osobowych

Szczecin, dnia .....

POZIOM BEZPIECZEŃSTWA SYSTEMU PRZETWARZANIA DANYCH OSOBOWYCH

Dla systemu przetwarzania danych osobowych
..... [1)]

w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie
obowiązuje ..... [2)]

poziom bezpieczeństwa

zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

ZATWIERDZAM

(ABI-ASI)

1) - nazwa systemu informatycznego
2) - poziom bezpieczeństwa: *podstawowy, podwyższony, wysoki*

załącznik nr 2
do zarządzenia nr 36 Rektora ZUT z dnia 28 czerwca 2016 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH W ZACHODNIOPOMORSKIM UNIWERSYTECIE TECHNOLOGICZNYM W SZCZECINIE

I Wprowadzenie

1. Instrukcja Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie (ZUT) zwana dalej Instrukcją, określa zasady zarządzania każdym systemem informatycznym, w którym przetwarzane są dane osobowe.
2. Podstawą prawną powstania Instrukcji jest ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jedn. Dz. U z 2015 r. poz. 2135, z późn. zm.), zwana dalej ustawą, oraz rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), zwane dalej rozporządzeniem.
3. Instrukcja obowiązuje wszystkie osoby korzystające z zasobów informatycznych ZUT, w których przetwarzane są dane osobowe.

II Definicje podstawowych pojęć

1) dane osobowe – wszystkie informacje dotyczące zidentyfikowanej lub możliwej do identyfikacji osoby fizycznej,
2) przetwarzanie danych osobowych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie,
3) Administrator Danych Osobowych (ADO) – osoba, która decyduje o celach i środkach przetwarzania danych osobowych. Obowiązki administratora danych osobowych wykonuje rektor,
4) Lokalny Administrator Danych Osobowych (LADO) – osoba wyznaczona przez rektora, która wykonuje obowiązki administratora danych osobowych w podległych jej jednostkach,
5) Administrator Bezpieczeństwa Informacji (ABI) – osoba powołana przez rektora, która odpowiada za bezpieczeństwo danych osobowych na uczelni,
6) Lokalny Administrator Bezpieczeństwa Informacji (LABI) – osoba powołana przez Lokalnego Administratora Danych Osobowych odpowiadająca za bezpieczeństwo danych osobowych na terenie jednostki organizacyjnej uczelni,
7) system informatyczny – zespół współpracujących ze sobą, urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
8) Administrator Systemu Informacyjnego (ASI) – osoba upoważniona przez Administratora Danych Osobowych zarządzająca systemem informatycznym,
9) użytkownik systemu – osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym,
10) stacja komputerowa – komputer lub terminal wraz z urządzeniami peryferyjnymi, z którego korzysta użytkownik systemu,
11) identyfikator użytkownika (login) – ciąg znaków identyfikujący w sposób jednoznaczny użytkownika systemu,
12) hasło – ciąg znaków znany użytkownikowi systemu służący do uwierzytelniania użytkownika w systemie,
13) logowanie – proces uwierzytelniania polegający na podaniu identyfikatora i hasła,
14) duże zbiory danych osobowych – zbiory danych, które dotyczą więcej niż 500 osób.

III Ogólne zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych w systemach informatycznych

1. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób zatrudnionych w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
2. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym przetwarzane są dane osobowe, dozwolone jest tylko w obecności osób upoważnionych do ich przetwarzania.
3. Wydruki zawierające dane osobowe należy przechowywać w miejscach, w których niemożliwe jest ich odczytanie przez osoby nieuprawnione. Nieprzydatne wydruki należy niezwłocznie niszczyć w stopniu uniemożliwiającym ich odczyt.
4. Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby nieuprawnione, a na których przetwarzane są dane osobowe, należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w te dane.
5. Duże zbiory danych osobowych powinny być przetwarzane w systemach działających w oparciu o architekturę klient – serwer. To znaczy, że dane powinny być umieszczone w bazach danych na dedykowanych serwerach.

IV Procedury nadawania i zmiany uprawnień do przetwarzania danych oraz ich rejestrowania w systemach informatycznych

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych ma obowiązek zapoznania się z niniejszą instrukcją.
2. Podstawą nadania uprawnień jest upoważnienie do przetwarzania danych osobowych wystawione przez Lokalnego Administratora Danych Osobowych.
3. Na podstawie upoważnienia, o którym mowa w pkt 2, ASI dokonuje rejestracji użytkownika w systemie informatycznym, nadając mu odpowiednie uprawnienia.
4. Podczas rejestracji nadawany jest identyfikator użytkownika oraz hasło.
5. Hasło musi spełniać wymogi opisane w dziale V.
6. O dokonaniu rejestracji ASI informuje w formie elektronicznej użytkownika systemu, LADO oraz ABI.
7. ABI ma prawo zablokować nadanie uprawnień użytkownikowi systemu, w przypadku jeśli zakres tych uprawnień może zagrozić bezpieczeństwu systemu. W takim przypadku informuje niezwłocznie odpowiedniego ASI i LADO o zaistniałej sytuacji.
8. Hasło powinno być przekazanie bezpośrednio użytkownikowi systemu pisemnie w zaklejonej kopercie lub ustnie.
9. Użytkownik systemu ma obowiązek niezwłocznej zmiany hasła, zgodnie z wymogami opisanymi w dziale V.
10. Zmiany/cofnięcia uprawnień dokonuje ASI na pisemny wniosek LADO. Informację o tym fakcie LADO przesyła również do ABI.
11. ASI ma obowiązek przechowywania kopii wszystkich upoważnień do przetwarzania danych osobowych w danym systemie oraz wniosków o zmianę uprawnień użytkowników systemu.
12. ABI prowadzi rejestr użytkowników oraz ich uprawnień.

V Metody i środki uwierzytelniania w systemach informatycznych.

1. Dostęp do danych osobowych następuje wyłącznie po podaniu identyfikatora użytkownika i hasła.
2. W przypadku dużych zbiorów danych stosuje się uwierzytelnienie dwustopniowe na poziomie dostępu do sieci komputerowej oraz dostępu do aplikacji przetwarzającej dane osobowe.
3. Identyfikator użytkownika systemu nie powinien być zmieniany bez uzasadnienia.
4. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.
5. Hasło użytkownika musi być zmieniane przynajmniej raz w miesiącu.
6. Przy wyborze hasła obowiązują następujące zasady:
   - hasło musi składać się z co najmniej 8 znaków,
   - nie może być utworzone ze słowa znajdującego się w słownikach, identyfikatora użytkownika nazwiska lub imienia, innej nazwy własnej, ogólnie dostępnych danych o użytkowniku,

- nie może być złożone z łatwo przewidywalnego ciągu znaków np. qwerty lub 123456,
- powinno zawierać litery duże i małe oraz cyfry lub znaki specjalne.

7. Użytkownik systemu ma obowiązek utrzymywania swojego hasła w tajemnicy, również po upływie jego ważności.
8. W przypadku gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik systemu zobowiązany jest do natychmiastowej zmiany hasła lub w razie problemów powiadomienia o tym fakcie ASI lub ABI.
9. Hasła wpisywane z klawiatury nie mogą się pojawiać w formie jawnej na ekranie monitora.
10. W przypadku przetwarzania danych osobowych na komputerach przenośnych, dyskach twardych oraz innych cyfrowych nośnikach informacji, dane muszą być zabezpieczone w sposób uniemożliwiający dostęp do tych danych poprzez zastosowanie metod i środków kryptograficznych.

VI Procedury rozpoczęcia i zakończenia pracy w systemie

1. Rozpoczęcie pracy w systemie musi być poprzedzone procedurą uwierzytelniania (należy zalogować się do systemu, podając identyfikator i hasło).
2. W przypadku dużych zbiorów danych osobowych dostęp do aplikacji musi być poprzedzony dodatkową procedurą uwierzytelniania.
3. W sytuacji opuszczenia stanowiska na odległość uniemożliwiającą jego obserwację należy wylogować się z systemu lub uruchomić wygaszacz ekranu zabezpieczony hasłem.
4. System po upływie 5 minut braku aktywności ze strony użytkownika powinien uruchomić samoczynnie wygaszacz ekranu zabezpieczony hasłem.
5. W przypadku zastosowania dwustopniowej metody uwierzytelniania po zakończeniu pracy z aplikacją przetwarzającą dane osobowe należy bezwzględnie wykonać proces wylogowania się z niej. Po zakończeniu pracy w systemie komputerowym należy wylogować się oraz prawidłowo zamknąć system operacyjny komputera.
6. W przypadku zastosowania jednostopniowej metody uwierzytelniania proces wylogowania należy przeprowadzić po zakończeniu pracy na stacji komputerowej, a następnie prawidłowo zamknąć system operacyjny.

VII Procedury tworzenia kopii zapasowych danych

1. Kopie zapasowe baz danych oraz aplikacji przetwarzających duże zbiory danych osobowych są tworzone oddzielnie w postaci kopii przyrostowych (to znaczy zawierających tylko te informacje, które uległy zmianie podczas ostatniej doby). Raz w tygodniu tworzona jest natomiast pełna kopia. Czas rotacji nośników nie powinien być krótszy niż 3 miesiące.
2. W stosunku do systemów informatycznych przetwarzających dane osobowe, które nie są sklasyfikowane jako duże zbiory danych osobowych, należy stosować - w miarę możliwości technicznych i organizacyjnych - zasadę umieszczania danych na serwerach. W takim przypadku procedura wykonywania kopii zapasowych jest identyczna jak w pkt 1. W przypadku gdy umieszczenie danych na serwerze jest niemożliwe (na przykład w sytuacji gdy system informatyczny nie jest podłączony do sieci komputerowej) kopie zapasowe wykonuję się na nośnikach wymiennych (np. płyty CD, DVD).
3. Za tworzenie kopii zapasowej danych osobowych odpowiedzialny jest ASI.
4. Szczególnie istotne dla funkcjonowania ZUT dane powinny być kopiowane dodatkowo na serwer znajdujący się w innym budynku niż ten, w którym znajduje się podstawowy system archiwizujący dane. Dane te powinny być zabezpieczone przed nieuprawnionym odczytem metodami kryptograficznymi, przy czym długość klucza szyfrującego nie powinna być krótsza niż 1024 bity.
5. Nośniki kopi zapasowych przeznaczone do likwidacji powinny być pozbawione zapisu danych. W przypadku gdy jest to niemożliwe, należy je uszkodzić w sposób uniemożliwiający ich odczytanie.
6. Procedura likwidacji nośników powinna być zatwierdzona odpowiednim protokołem.

VIII Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Wszelkie nośniki danych, które zawierają dane osobowe, powinny być przechowywane w sposób zabezpieczający je przed nieuprawnionym przejęciem, odczytem, skopiowaniem lub zniszczeniem.
2. Nośniki, o których mowa powyżej, powinny być oznaczone w sposób umożliwiający ich identyfikacje.
3. Kopie zapasowe danych osobowych, które przetwarzane są na serwerach, przechowywane są w serwerowni Uczelnianego Centrum Informatyki.
4. Kopie zapasowe danych osobowych należy bezzwłocznie usuwać po ustaniu ich użyteczności.
5. Dyski twarde w warunkach gwarancji muszą posiadać opcję zachowania dysku podczas wymiany uszkodzonego.

IX Udostępnienia danych

1. Udostępnianie danych może nastąpić w następujących przypadkach:
   a) w celu innym niż włączenie do zbioru – ADO udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa,
   b) dane osobowe, z wyłączeniem danych, o których mowa w art. 27 ust 1 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r., mogą być także udostępnione w celach innych niż włączenie do zbioru, innym osobom lub podmiotom niż wyżej wymienione jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą
2. Dane osobowe udostępnia się wyłącznie na pisemny umotywowany wniosek, chyba że przepisy prawa stanowią inaczej. Zgodę na udostępnienie danych wyraża ADO.
3. Dla każdego systemu, w którym przetwarzane są dane osobowe prowadzony jest elektroniczny rejestr, w którym odnotowywane są informacje o odbiorcach danych z tego systemu.
4. Odnotowanie obejmuje informacje o:
   a) nazwie podmiotu lub imieniu i nazwisku osoby, której udostępniono dane;
   b) zakresie udostępnionych danych;
   c) dacie udostępnienia.
5. Obowiązek odnotowywania ww. informacji w rejestrze spoczywa na ABI.

X Środki i zasady ochrony systemów informatycznych

1. System informatyczny powinien być zabezpieczony przed:
   - działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do niego,
   - utratą danych spowodowanych awarią zasilania lub zakłóceniami w sieci zasilającej.
2. W celu zabezpieczania systemu przed skutkami działania oprogramowania, o którym mowa w pkt 1, ASI instaluje na stacjach komputerowych oprogramowanie antywirusowe i antyszpiegowskie.
3. Konfiguracja oprogramowania antywirusowego i antyspyware powinna być następująca:
   - aktualizacja oprogramowania powinna odbywać się nie rzadziej niż co 2 godziny,
   - rezydentny monitor antywirusowy powinien być stale włączony,
   - powinna być zablokowana możliwość ingerencji użytkownika w ustawienia programu antywirusowego.
4. System operacyjny stacji komputerowej powinien być tak skonfigurowany aby automatycznie pobierał i instalował aktualizacje.
5. System poczty elektronicznej ZUT musi posiadać zabezpieczenie antyspamowe i antywirusowe.
6. W systemach przetwarzających dane osobowe powinno być zainstalowane oprogramowanie typu ściana ogniowa. Konfiguracja tego oprogramowania powinna zabezpieczać system przed nieautoryzowanym dostępem.
7. Segmenty sieci komputerowej, w których funkcjonują systemy informatyczne przetwarzające duże zbiory danych osobowych, powinny być logicznie odseparowane za pomocą urządzeń typu ściana ogniowa od reszty sieci komputerowej.

8. Serwery, na których funkcjonują bazy danych osobowych powinny być zabezpieczone przed utratą zasilania przez podłączenie zasilaczy awaryjnych.
9. Czas pracy systemu na zasilaniu awaryjnym nie może być krótszy niż 10 minut.
10. Główna serwerownia Uczelnianego Centrum Informatyki, w której znajdują się serwery ze szczególnie istotnymi danymi dla funkcjonowania ZUT, powinna być wyposażona w sprawny agregat prądotwórczy.

XI Procedury wykonywania przeglądów i konserwacji systemów

1. Wszelkie prace związane z naprawami lub konserwacją systemu informatycznego mogą być wykonywane wyłącznie przez upoważnionych pracowników uczelni lub upoważnionych przedstawicieli wykonawców.
2. W przypadku konieczności dokonania naprawy poza miejscem przetwarzania danych osobowych z systemu informatycznego należy usunąć wszelkie nośniki danych.
3. Przeglądy i konserwacje systemów powinny być wykonywane w terminach określonych przez producentów sprzętu. Jeśli producent nie przewidział dla danego urządzenia przeglądów eksploatacyjnych lub nie określił ich częstotliwości, to o dokonaniu przeglądu decyduje ASI.
4. Przegląd i konserwacja urządzeń może być wykonana na żądanie przełożonego.
5. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
   c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

Załącznik nr 3
do zarządzenia nr 36 Rektora ZUT z dnia 28 czerwca 2016 r.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH W ZUT

1. Instrukcja niniejsza ma zastosowanie w sytuacjach podejrzenia lub stwierdzenia naruszenia danych osobowych w systemie informatycznym lub innym zbiorze danych.
2. Naruszenie zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych stwierdza się, gdy wystąpiły między innymi:
   1) nieuprawniony dostęp do danych osobowych,
   2) udostępnienie danych osobowych osobom nieupoważnionym,
   3) zmiana, kopiowanie lub uszkodzenie danych osobowych dokonane przez osoby nieuprawnione,
   4) kradzież lub zgubienie nośników informacji zawierających dane osobowe (w szczególności dysków, pamięci flash, płyt CD, płyt DVD, wydruków komputerowych).
3. Za okoliczności, które wskazują na naruszenie zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych, uważa się między innymi:
   1) nieuzasadnione korzystanie z zasobów systemu informatycznego lub innego zbioru danych,
   2) nieuzasadnione ujawnienie danych osobowych,
   3) ujawnienie wirusów komputerowych lub innych programów, które mogą mieć negatywny wpływ na funkcjonowanie systemu informatycznego,
   4) wydarzenia obniżające stan bezpieczeństwa systemu informatycznego lub innego zbioru danych (np. awaria zasilania).
4. Osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym lub innym zbiorze danych, która stwierdzi lub podejrzewa naruszenie zabezpieczenia danych zobowiązana jest do:
   1) niezwłocznego poinformowania o tym fakcie swojego bezpośredniego przełożonego, a ten informuje ASI w przypadku systemu informatycznego oraz ABI,
   2) zaprzestania pracy w systemie informatycznym lub innym zbiorze danych do momentu otrzymania od ASI decyzji o możliwości wznowienia pracy.
5. ABI po uzyskaniu informacji, o której mowa w pkt 4 podejmuje działania (jeśli dotyczy to systemu informatycznego – wraz z ASI) w celu rozpoznania naruszenia zabezpieczenia danych, a w szczególności ustala, czy miało miejsce naruszenie ochrony danych osobowych.
6. ABI w przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych:
   1) podejmuje działania służące ograniczeniu szkód wywołanych naruszeniem ochrony danych osobowych,
   2) zabezpiecza dane wskazujące na naruszenie zabezpieczenia danych osobowych,
   3) ustala okoliczności naruszenia ochrony danych osobowych,
   4) analizuje rodzaj, zakres i źródło naruszenia ochrony danych osobowych,
   5) podejmuje działania naprawcze,
   6) bada przyczyny naruszenia ochrony danych osobowych i podejmuje działania mające na celu wyeliminowanie podobnych zdarzeń zagrażających bezpieczeństwu danych.
7. ABI po przeprowadzeniu czynności, o których mowa w pkt 5 i 6, sporządza i przedstawia ADO oraz LADO raport o stwierdzeniu naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych w ciągu 14 dni od daty jego zaistnienia. Raport zawiera w szczególności następujące dane i informacje:
   1) imię i nazwisko, stanowisko oraz miejsce zatrudnienia osoby, która zgłosiła naruszenie zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych,
   2) datę i godzinę powiadomienia o naruszeniu,
   3) opis podjętych działań mających na celu ustalenie zakresu podejrzewanego naruszenia,
   4) opis podjętych działań naprawczych.
8. ABI odpowiedzialny jest za przechowywanie materiałów, o których mowa w pkt 7, dokumentujących naruszenie oraz podejrzenie naruszenia zabezpieczenia danych w systemie informatycznym lub innym zbiorze danych.