ZARZĄDZENIE Nr 4/2016
Rektora Akademii Morskiej w Szczecinie
z dnia 17.02.2016 r.

Tekst ujednolicony z uwzględnieniem zarządzeń nr: 58/2019, 106/2020,i 46/2021, 60/2021 i 68/2022
w sprawie: **wprowadzenia „Regulaminu Informatycznego Politechniki Morskiej w Szczecinie".**

Na podstawie:

1) art. 66 ust. 2 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz.U. z 2012 r. poz. 572, z późn. zm.),
2) ustawy z dnia 17 lutego 2005 r o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U z 2014 r. poz. 1114),
3) rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2016 r. poz. 113),
4) ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2006 r., Nr 90, poz. 631, z późn. zm.)

zarządza się, co następuje:

§ 1.

1. Wprowadza się Regulamin Informatyczny Politechniki Morskiej w Szczecinie, zwany dalej Regulaminem, stanowiący załącznik do niniejszego zarządzenia.
2. Regulamin określa politykę zarządzania bezpieczeństwem informacji w systemach informatycznych oraz podstawowe zasady użytkowania zasobów i systemów informatycznych.
3. Regulamin w szczególności określa:
   1) zasady użytkowania sprzętu komputerowego i sieciowego,
   2) zasady bezpieczeństwa danych,
   3) zasady korzystania z sieci PM,
   4) zasady korzystania z elektronicznej poczty służbowej,
   5) zasady ochrony praw licencyjnych do oprogramowania komputerowego,
   6) zasady przenoszenia praw autorskich do oprogramowania opracowanego przez pracowników Uczelni,
   7) zasady przeprowadzania szkoleń informatycznych,
   8) politykę informacyjną,
   9) zasady dokonywania inwentaryzacji, przeglądu i konserwacji urządzeń i systemów informatycznych,
   10) realizację zadań i obowiązków wynikających z krajowego systemu cyberbezpieczeństwa.
4. Politykę bezpieczeństwa danych osobowych oraz instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych określają odrębne przepisy.

§ 2.

Systemy klimatyzacji, wentylacji oraz monitoringu środowiska, o których mowa w § 6 ust. 1 Regulaminu, mogą być uzupełnione w serwerowniach w miarę planów inwestycyjnych i remontowych.

§ 3.

Traci moc zarządzenie nr 30/2010 Rektora Akademii Morskiej w Szczecinie z dnia 18.10.2010 r. w sprawie wprowadzenia „Regulaminu Informatycznego Akademii Morskiej w Szczecinie" zmienione zarządzeniem nr 1/2011 Rektora Akademii Morskiej w Szczecinie z dnia 28.01.2011 r. w sprawie zmiany zarządzenia nr 30/2010 Rektora Akademii Morskiej w Szczecinie z dnia 18.10.2010 r. w sprawie wprowadzenia „Regulaminu Informatycznego Akademii Morskiej w Szczecinie" i zarządzeniem nr 27/2013 Rektora Akademii Morskiej w Szczecinie z dnia 08.07.2013 r. w sprawie zmiany zarządzenia nr 30/2010 Rektora Akademii Morskiej w Szczecinie z dnia 18.10.2010 r. w sprawie wprowadzenia „Regulaminu Informatycznego Akademii Morskiej w Szczecinie", z późn. zm.

§ 4.

Nadzór i kontrolę nad realizacją niniejszego zarządzenia powierza się kierownikom pionów wg przyznanych kompetencji.

§ 5.

Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązująca od 01.03.2016 r.

REKTOR

prof. dr hab. inż. kpt. ż.w. Stanisław Gucma

Załącznik do zarządzenia nr 4/2016
Rektora AM w Szczecinie z dnia 17.02.2016 r.

REGULAMIN INFORMATYCZNY POLITECHNIKI MORSKIEJ W SZCZECINIE

Rozdział I
Postanowienia ogólne

§ 1.

Ilekroć w Regulaminie jest mowa o:

1) Uczelni – należy przez to rozumieć Politechnikę Morską w Szczecinie,
2) UCI – należy przez to rozumieć Uczelniane Centrum Informatyczne,
3) osobach współpracujących – należy przez to rozumieć osoby fizyczne współpracujące z Uczelnią na podstawie umowy cywilnoprawnej, jeżeli Uczelnia na podstawie tej umowy udostępnia im do użytkowania własny sprzęt komputerowy,
4) użytkownikach – należy przez to rozumieć pracowników Uczelni i osoby współpracujące, posiadające możliwość użytkowania sprzętu komputerowego Politechniki Morskiej w Szczecinie lub korzystające z sieci PM,
5) obszarze Administracja – należy przez to rozumieć jednostki administracyjne, z wyłączeniem Domu Pracy Twórczej w Świnoujściu i Kancelarii Informacji Niejawnych, jednostek ogólnouczelnianych, Studium Doskonalenia Kadr Oficerskich, Ośrodka Szkoleniowego Ratownictwa Morskiego, Statku, Studium Wychowania Fizycznego i Sportu,
6) służbie informatycznej – należy przez to rozumieć pracowników UCI oraz lokalną służbę informatyczną,
7) lokalnej służbie informatycznej – należy przez to rozumieć wyznaczonych poza obszarem Administracja pracowników inżynieryjno-technicznych lub innych albo podmiot zewnętrzny, którym lokalnie powierzono wsparcie informatyczne oraz usuwanie problemów informatycznych, w tym sprzętowych,
8) sieci PM – należy przez to rozumieć komputery i urządzenia sieciowe Uczelni połączone ze sobą w celu wymiany danych, korzystania ze wspólnych urządzeń, wspólnego oprogramowania oraz baz danych,
9) urządzeniu sieciowym – należy przez to rozumieć urządzenie łączące segmenty sieci komputerowej oraz inne urządzenia pracujące w sieci PM z wyłączeniem komputerów,
10) urządzeniu mobilnym – należy przez to rozumieć urządzenie elektroniczne pozwalające na przetwarzanie, odbieranie oraz wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią, tj. m.in. urządzenia typu laptop, smartfon, tablet,.
11) przetwarzaniu mobilnym danych – należy przez to rozumieć przetwarzanie danych na urządzeniach mobilnych,
12) centralnych urządzeniach informatycznych – należy przez to rozumieć urządzenia sieciowe i serwery Uczelni wykorzystywane podczas dostępu do centralnych systemów informatycznych,
13) systemie informatycznym – należy przez to rozumieć sieć PM oraz oprogramowanie, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej,
14) centralnych systemach informatycznych – należy przez to rozumieć systemy informatyczne zainstalowane na centralnych urządzeniach informatycznych Uczelni,
15) centralnych systemach administracyjnych – należy przez to rozumieć centralne systemy informatyczne przeznaczone do użytku komórek organizacyjnych w celu przetwarzania danych i wspomagania zarządzania Uczelnią,

16) centralnym dysku sieciowym – należy przez to rozumieć przestrzeń dyskową na serwerze Uczelni przeznaczoną do zapisywania danych jednostek organizacyjnych Uczelni, objętą systemem bezpieczeństwa w zakresie obowiązkowego tworzenia kopii zapasowych,
17) dysku lokalnym – należy przez to rozumieć dysk twardy w komputerze użytkownika oraz nośniki elektroniczne (np. dysk przenośny, płyta CD, pendrive),
18) usłudze katalogowej – należy przez to rozumieć scentralizowane zarządzanie informacją o komputerach pracujących w systemach operacyjnych Windows, kontami użytkowników oraz sposobem i zasadami organizacji pracy w sieci PM,
19) PPD – należy przez to rozumieć dedykowane węzłowe pomieszczenia zwane Pośrednimi Punktami Dystrybucyjnymi sieci komputerowej Uczelni,
20) serwerowni – należy przez to rozumieć PPD, w którym znajdują się serwery Uczelni,
21) licencji – należy przez to rozumieć umowę zawieraną pomiędzy podmiotem, któremu przysługują majątkowe prawa autorskie do programu komputerowego a osobą, która zamierza z danej aplikacji lub programu korzystać lub inny dokument potwierdzający prawo korzystania z aplikacji lub programu komputerowego,
22) Spamie – należy przez to rozumieć niezamawianą ofertę handlową oraz niezamawianą pocztę masową, w formie listu elektronicznego,
23) formie elektronicznej – należy przez to rozumieć e-mail wysłany za pośrednictwem służbowej poczty elektronicznej lub zeskanowany dokument papierowy z podpisem odręcznym,
24) „Serwis PM" – należy przez to rozumieć elektroniczny system obsługi zgłoszeń serwisowych, tj. usterek i problemów informatycznych,
25) punkt elektryczno-logiczny (PEL) – należy przez to rozumieć wewnętrzne instalacje teleinformatyczne i elektryczne przeznaczone do podłączania komputerów i telefonów.

§ 2.

1. Utrzymanie standardów wynikających z niniejszego Regulaminu należy odpowiednio do służby informatycznej i użytkowników.
2. Na komputerach niepracujących w usłudze katalogowej i niezarządzanych przez służbę informatyczną, użytkownicy są zobowiązani we własnym zakresie do zapewnienia przestrzegania następujących standardów:
   1) uprawnienia dostępowe do komputerów,
   2) profilaktyka antywirusowa,
   3) bezpieczeństwo poczty elektronicznej,
   4) inwentaryzacja, przegląd i konserwacja urządzeń i systemów informatycznych.

Rozdział II
Zasady użytkowania sprzętu komputerowego i sieciowego.

§ 3.

Użytkowanie i ochrona sprzętu

1. Przełożeni mają obowiązek zapewnić podległym pracownikom prawidłowe warunki bezpieczeństwa i higieny pracy przy obsłudze monitorów ekranowych, w szczególności warunki ergonomiczne wynikające z rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz. U. nr 148, poz. 973).
2. Użytkownicy powinni chronić sprzęt komputerowy przed zniszczeniem lub nadmiernym zabrudzeniem, w szczególności przy spożywaniu posiłków lub napojów.

3. Obsługa urządzeń peryferyjnych (monitory, drukarki, urządzenia wielofunkcyjne, itd.) i wymiana materiałów eksploatacyjnych, takich jak papier czy toner, należy do użytkownika po wcześniejszym zapoznaniu się z instrukcją obsługi dostępną w formie papierowej bądź na stronie internetowej producenta.
4. Nie wolno zostawiać otwartych pomieszczeń, w których znajdują się komputery, sprzęt peryferyjny (monitory, drukarki, skanery, urządzenia wielofunkcyjne, rzutniki itd.) i urządzenia mobilne bez nadzoru upoważnionych pracowników.
5. Urządzenia mobilne powinny być chronione przed kradzieżą lub nieuprawnionym dostępem poprzez na przykład:
   1) zapewnienie ochrony osobistej,
   2) zamykanie na klucz w szafach służbowych,
   3) zamykanie w niedostępnych dla innych osób pomieszczeniach.
6. Kradzież, zniszczenie lub ślady włamania do komputerów lub miejsc, w których były przechowywane należy niezwłocznie zgłosić przełożonemu i odpowiednio służbie informatycznej lub osobie materialnie odpowiedzialnej za ten sprzęt.
7. Użytkownicy mają obowiązek stosowania się do zaleceń służby informatycznej w sprawach dotyczących bezpieczeństwa i efektywności eksploatacji komputerów służbowych.

§ 4.

Bezpieczeństwo przeciwpożarowe i zasady zakończenia pracy ze sprzętem komputerowym

1. Komputery i sprzęt peryferyjny muszą być podłączone do sieci elektrycznej przy użyciu listwy zasilającej z bezpiecznikiem zabezpieczającym i filtrem przepięciowym.
2. Nie należy podłączać do komputerowej (wydzielonej) sieci elektrycznej urządzeń innych niż informatyczne o dużym poborze mocy, np.: czajników elektrycznych, niszczarek, odkurzaczy, itp.
3. Kable przy komputerze i sprzęcie peryferyjnym powinny być uporządkowane i nie przeszkadzać w pracy, w szczególności nie powinny być narażone na najeżdżanie fotelem i wyrywanie ze ścian.
4. Użytkownicy, po zakończeniu pracy, zobowiązani są do bezwzględnego wyłączania sprzętu elektrycznego i elektronicznego na swoich stanowiskach pracy oraz w pomieszczeniach znajdujących się pod ich pieczą.
5. Zobowiązanie wyłączenia sprzętu nie dotyczy urządzeń podtrzymujących zasilanie (UPS), serwerowni oraz innych niezbędnych urządzeń, których wyłączenie spowodowałoby zakłócenie bieżącego funkcjonowania Uczelni, a także realizacji procesu dydaktycznego lub naukowego.

§ 5.

Serwis

1. Komputery służbowe powinny pracować w usłudze katalogowej Uczelni. Odstępstwo od tej zasady można zastosować w uzasadnionych przypadkach, w których praca w usłudze katalogowej jest niemożliwa ze względów technicznych bądź z innego ważnego powodu. Odstępstwo to wymaga uzyskania od przełożonego pracownika i kierownika UCI zgody w formie pisemnej bądź elektronicznej.
2. Realizacja zgłoszeń serwisowych i usuwanie problemów odbywa się poprzez właściwą służbę informatyczną w możliwie najszybszym czasie.
3. W celu prawidłowej realizacji funkcji serwisowych służba informatyczna ma prawo do uruchamiania skryptów, programów sieciowych dokonujących sprawdzenia legalności oprogramowania, odpowiedniego zabezpieczania oprogramowania, dostępności miejsca na dyskach oraz analizy parametrów technicznych sprzętu w sieci i na komputerach służbowych użytkowników. Lokalna służba informatyczna ograniczona jest w tych uprawnieniach do administrowanego przez siebie obszaru.

4. Zgłoszenia nieprawidłowego funkcjonowania sprzętu bądź innych problemów informatycznych do UCI powinny odbywać się przez elektroniczny system zgłoszeń serwisowych „Serwis PM". W sytuacjach, gdy nie jest to technicznie możliwe dopuszcza się zgłoszenia np. osobiste, telefoniczne lub pisemne.
5. Instrukcję użytkowania sytemu „Serwis PM" ustala kierownik UCI.
6. Tryb zgłaszania usterek i problemów oraz organizację serwisu informatycznego w Uczelni poza dniami i godzinami pracy administracji, głównie dla potrzeb procesu dydaktycznego, ustala kierownik UCI.

Rozdział III
Zasady bezpieczeństwa danych.

§ 6.

Ochrona fizyczna i dostęp fizyczny do centralnych urządzeń informatycznych.

1. Sieć komputerowa Uczelni posiada dedykowane węzłowe pomieszczenia zwane Pośrednimi Punktami Dystrybucyjnymi (PPD), zabezpieczone przed dostępem fizycznym przez osoby nieupoważnione.
2. PPD, w których umiejscowione są serwery Uczelni, zwane są serwerowniami i wyposażone są w system klimatyzacji, chronione są przed pożarem oraz wyposażone w system monitoringu środowiska.
3. Dostęp do PPD mają wyznaczeni przez kierownika UCI pracownicy lub inne upoważnione osoby.
4. Centralne urządzenia informatyczne powinny być zabezpieczone zasilaczem awaryjnym UPS pozwalającym na podtrzymanie ich pracy w przypadku braku zasilania.

§ 7.

Uprawnienia dostępowe do centralnych zasobów informatycznych

1. Centralne systemy informatyczne są zabezpieczane przed ingerencją z sieci na poziomie komunikacji sieciowej.
2. Systemy operacyjne serwerów, na których przetwarzane są dane, oraz centralne systemy administracyjne muszą być zabezpieczone za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora użytkownika i hasła.
3. Dostęp do serwerów i systemów, o których mowa w ust. 2, mogą posiadać tylko uprawnieni użytkownicy.
4. Kierownik UCI zapewnia opracowanie systemów dostępu, o których mowa ust. 3, w tym sposób prowadzenia wykazu obszarów dostępowych (serwery, centralne systemy administracyjne), procedury nadawania i cofania uprawnień dostępowych oraz sposób prowadzenia wykazu udzielonych praw dostępowych i ich zakresu.

§ 8.

Uprawnienia dostępowe do komputerów i systemów

1. Każdy użytkownik, będący pracownikiem Uczelni lub osobą współpracującą otrzymuje dane dostępowe do:
   1) usługi katalogowej,
   2) imiennego konta poczty służbowej,
   3) innych systemów zgodnie z przydzielonymi uprawnieniami.

2. Wszystkie komputery winny być chronione przed dostępem osób nieuprawnionych poprzez stosowanie bezpiecznych haseł zabezpieczających, okresową ich zmianę oraz ochronę tych haseł przed osobami postronnymi.
3. Bezpieczne hasło powinno być kombinacją małych i dużych liter, cyfr oraz znaków specjalnych oraz spełniać dodatkowo następujące wymagania:
   1) powinno składać się z co najmniej 8 znaków,
   2) jego zmiana następuje nie rzadziej niż co 90 dni.
4. Użytkownikowi zabrania się udostępniania haseł osobom nieupoważnionym, w jakiejkolwiek formie, w całości lub w części oraz przechowywania ich w publicznie dostępnych miejscach lub w sieci w sposób niezabezpieczony.
5. Komputery powinny być zabezpieczone mechanizmem blokowania dostępu po określonym czasie bezczynności, z wyjątkiem sprzętu wykorzystywanego do prezentacji audiowizualnych na zajęciach dydaktycznych lub innych szczególnie uzasadnionych przypadków.
6. Kierownik UCI ustala szczegółowe zasady stosowania bezpiecznych haseł, mechanizmów blokowania dostępu oraz poziomu uprawnień użytkowników.
7. Zasady nadawania, cofania i ograniczania uprawnień dostępowych określone w „Polityce bezpieczeństwa w zakresie przetwarzania danych osobowych Politechniki Morskiej w Szczecinie" stosuje się odpowiednio do pozostałych centralnych systemów informatycznych.

§ 9.

Bezpieczeństwo dostępu zdalnego

1. Dostęp do centralnych systemów informatycznych w sposób zdalny możliwy jest wyłącznie w oparciu o technologie szyfrowanej transmisji danych.
2. W celu zachowania tego standardu UCI stosuje na poziomie zarządzania odpowiednie protokoły zabezpieczeń oraz szyfrowania.

§ 10.

Profilaktyka antywirusowa

1. Komputery, zawarte w nich dane i systemy informatyczne chronione są przed nieuprawnionym dostępem oraz utratą danych przez system ochrony antywirusowej, antyspamowej i zapór sieciowych (firewall).
2. Konfiguracja programu antywirusowego powinna zapewnić:
   1) bieżący monitoring systemu,
   2) aktualizację względem najnowszej bazy wirusów, wykonywaną automatycznie niezwłocznie po uruchomieniu komputera (w przypadku m/s Nawigator XXI powyższe realizowane jest ręcznie tylko podczas cumowania w Szczecinie),
   3) ochronę działania aplikacji i dysków twardych komputera w czasie rzeczywistym poprzez skanowanie plików zawierających potencjalnie niebezpieczne kody w trakcie pracy komputera w tle działania aplikacji,
3. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, właściwa służba informatyczna 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 zapasowej po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
   3) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych narzędzi i oprogramowania.

§ 11.

Zapisywanie i bezpieczeństwo danych

1. W celu ochrony przed utratą danych pracownicy powinni zapisywać dane i dokumenty elektroniczne na centralnych dyskach sieciowych.
2. Zapisywanie danych lub dokumentów na dyskach lokalnych i urządzeniach mobilnych jest dopuszczalne pod warunkiem zabezpieczenia ich przed utratą np. poprzez m.in. dodatkowe zapisanie ich na centralnym dysku sieciowym lub na innym nośniku lokalnym.
3. Istnieje możliwość zabezpieczenia plików przed dostępem osób trzecich poprzez m.in. szyfrowanie danych lub opcje zabezpieczeń dostępne w programie użytkowym.
4. W szczególności zabezpieczenia, o których mowa w ust. 3, należy stosować przy przetwarzaniu mobilnym.
5. Zaleca się zachowanie ostrożności podczas używania urządzeń do przetwarzania mobilnego w miejscach publicznych, salach spotkań i innych niechronionych miejscach poza terenem Uczelni.
6. Utrata danych lub dokumentów, spowodowana nieprzestrzeganiem przepisów ust. 1, 2, 4 lub 5, traktowana jest jako narażenie Uczelni na szkody i grozi pociągnięciem do odpowiedzialności służbowej, dyscyplinarnej lub materialnej.
7. UCI zapewnia wsparcie merytoryczne w kwestii doboru odpowiedniej metody zabezpieczenia danych. Na stronie Uczeni zamieszczone są instrukcje konfiguracji popularnych metod szyfrowania danych
8. Pracownicy mogą korzystać z centralnych dysków sieciowych wyłącznie do celów służbowych.
9. Kierownik UCI ustala szczegółowe zasady korzystania z dysków sieciowych.

§ 12.

Kopie zapasowe

1. UCI dąży do zapewnienia maksymalnej ochrony danych zgromadzonych na centralnych dyskach sieciowych poprzez m.in. ograniczanie uprawnień do odczytu plików i tworzenie kopii zapasowych.
2. Kopie zapasowe danych z centralnego dysku sieciowego oraz w centralnych systemów administracyjnych powinny być przechowywane w pomieszczeniu oddalonym od serwera, z którego zostały pobrane, w sposób chroniący przed jednoczesną utratą tych danych na serwerze i ich kopii.
3. System wykonywania kopii zapasowych powinien być automatyczny i pozwalać na szybki dostęp do kopii zapasowych.
4. Kopie zapasowe danych z centralnego dysku sieciowego oraz w centralnych systemów administracyjnych tworzone są w dni robocze, co najmniej raz dziennie.
5. Kierownik UCI ustala szczegółowe zasady tworzenia kopii zapasowych.

§ 13.

Zakres uprawnień

1. UCI jest odpowiedzialne za zarządzanie, administrowanie oraz koordynację działań zapewniających sprawne funkcjonowanie centralnych systemów informatycznych.
2. W celu prawidłowej realizacji funkcji zapewnienia bezpieczeństwa danych służba informatyczna ma prawo do pełnego dostępu administracyjnego do wszystkich komputerów służbowych Uczelni oraz plików w nich zawartych, z wyłączeniem zasobów kancelarii tajnych. Lokalna służba informatyczna ograniczona jest w tych uprawnieniach do administrowanego przez siebie obszaru.
3. Służba informatyczna zobowiązana jest do zachowania w tajemnicy informacji służbowych i osobistych innych użytkowników, które posiadła z racji wykonywania przydzielonych zadań i uprawnień. Szczególnej ochronie podlegają dane związane z realizacją procesu dydaktycznego

(np. tematy egzaminacyjne) oraz nieopublikowane treści związane z prowadzonymi badaniami i przygotowywanymi publikacjami.

4. Użytkownikom zabrania się:
   1) podejmowania prób dostępu do kont oraz danych innych użytkowników,
   2) uruchamiania oprogramowania deszyfrującego hasła dostępu,
   3) prowadzenia działań mających na celu podsłuchiwanie lub przechwytywanie danych transmitowanych w sieci PM.

Rozdział IV
Zasady korzystania z sieci PM

§ 14.

Status sieci PM

1. Sieć komputerowa Politechniki Morskiej w Szczecinie połączona jest z polskim i światowym Internetem.
2. UCI zapewnia lub organizuje realizację obowiązków Uczelni związanych z funkcjonowaniem sieci PM, a wynikających z prawa telekomunikacyjnego.
3. Dostęp do sieci PM nie stanowi publicznie dostępnych usług telekomunikacyjnych i skierowany jest wyłącznie do użytkowników w rozumieniu § 1 pkt 4 Regulaminu.
4. Uczelnia nie ponosi odpowiedzialności za skutki ewentualnej przerwy w pracy sieci PM, wynikłej z przyczyn od niej niezależnych, np. przerwy w dostawie energii elektrycznej, awarii na łączach poza jej obszarem administrowania itp.

§ 15.

Dostęp zdalny do sieci PM

1. Użytkownik ma możliwość uzyskania dostępu zdalnego do zasobów sieci PM.
2. Dostęp zdalny przyznawany jest na podstawie analizy możliwości technicznych.
3. Uprawnienia do zdalnego podłączenia się do sieci przyznawane są przez kierownika UCI na wniosek przełożonego pracownika lub kierownika jednostki merytorycznej dla osoby współpracującej, za wyłączeniem użytkowników, o których mowa w ust. 4.
4. Użytkownik będący nauczycielem akademickim uprawniony jest do łączenia się z zasobami sieci PM poprzez VPN na podstawie poświadczeń domenowych, po pisemnym zgłoszeniu do UCI zapotrzebowania na zdalny dostęp.
5. Wzór wniosku, o którym mowa w ust. 3, określa kierownik UCI.
6. Uprawnienia do zdalnego podłączenia się do sieci mogą być przyznawane dla podmiotów gospodarczych współpracujących z Uczelnią w zakresie obsługi systemów informatycznych, dla których sprawują opiekę serwisową na mocy umowy cywilnoprawnej. W przypadku podmiotów gospodarczych, nie posiadających aktywnej umowy cywilnoprawnej z Uczelnia, dostęp do zdalnego podłączenia się do sieci w celach diagnostycznych może zostać udzielony każdorazowo na okres nie dłuży niż 7 dni kalendarzowych.
7. Uprawnienia dostępu zdalnego, o którym mowa w ust. 6, przyznawane są i cofane przez kierownika UCI. Przepisy § 16 stosuje się odpowiednio.

§ 16.

Bezpieczeństwo sieci

1. Sieć PM nie może być wykorzystywana do jakiejkolwiek działalności niezgodnej z prawem.
2. Cały ruch wychodzący i przychodzący w sieci PM jest monitorowany i logowany.

3. Dostęp do treści internetowych uznanych za kontrowersyjne, niepożądane, niebezpieczne lub niezwiązane z wykonywaniem obowiązków służbowych, dydaktyką i badaniami naukowymi może być blokowany.
4. Sieć PM jest zabezpieczana przed ingerencją z sieci Internet na poziomie komunikacji sieciowej.
5. Urządzenia sieciowe i komputery muszą być, w ramach możliwości technicznych, zabezpieczone bezpiecznym hasłem oraz mechanizmem blokowania dostępu po określonym czasie bezczynności.
6. Każdy komputer pracujący w sieci PM powinien spełniać poniższe, minimalne wymagania programowe:
   1) zainstalowany program antywirusowy posiadający aktualne bazy sygnatur wirusów,
   2) włączona zapora sieciowa,
   3) zainstalowane najnowsze aktualizacje systemu.
7. Użytkownik jest zobowiązany do:
   1) stosowania nazwy użytkownika i hasła podczas pracy z komputerem podłączonym do sieci,
   2) zgłaszania administratorowi zauważonych nadużyć i nieprawidłowości w pracy sieci PM,
   3) podporządkowania się bieżącym zaleceniom służby informatycznej w zakresie użytkowania sieci PM.
8. Zabrania się jednoczesnego korzystania z sieci PM oraz:
   1) z modemu sieci komórkowych,
   2) z podłączonego do komputera bezprzewodowego urządzenia dostępowego typu access point,
   3) z sieci bezprzewodowej innego dostawcy.
9. W przypadku konieczności korzystania z usług lub urządzeń, wymienionych w ust. 8, należy najpierw odłączyć komputer od sieci PM.
10. Zabronione jest wykonywanie przez użytkowników czynności mogących zakłócić funkcjonowanie sieci PM, takich jak rozłączanie okablowania oraz wyłączanie, wymiana lub rekonfiguracja urządzeń sieciowych.
11. Zabronione jest umieszczanie w sieci PM oraz w sieci Internet za pośrednictwem sieci PM nielegalnych informacji, oprogramowania, używanie obelżywego języka, jak również podejmowanie jakichkolwiek innych działań niezgodnych z prawem obowiązującym w Polsce lub prawem międzynarodowym.
12. W szczególności do działań zabronionych należy:
    1) używanie, udostępnianie i rozpowszechnianie treści chronionych prawami autorskimi i pokrewnymi oraz uruchamianie programów komputerowych, które w tym pośredniczą,
    2) rozpowszechnianie i udostępnianie materiałów sprzecznych z prawem, dobrymi obyczajami oraz etyką,
    3) podszywanie się pod innych użytkowników lub inne komputery,
    4) monitorowanie łącz, podsłuchiwanie i skanowanie ruchu sieciowego lub portów,
    5) podejmowanie prób korzystania z zasobów chronionych bez zezwolenia,
    6) celowe i nieuzasadnione obciążanie łącza,
    7) rozsyłanie Spamu,
    8) prowadzenie z wykorzystaniem sieci PM działalności komercyjnej, innej niż na rzecz Uczelni, bez pisemnej zgody Rektora wydanej po pozytywnej opinii technicznej kierownika UCI,
    9) utrudnianie lub uniemożliwianie innym użytkownikom korzystania z sieci PM lub dostępu do jej zasobów, dezorganizowanie pracy innych użytkowników sieci PM,
    10) wprowadzanie samowolnych, nieuzgodnionych z UCI zmian we właściwościach połączenia sieciowego komputera lub urządzenia pośredniczącego (w szczególności nazwa sieciowa komputera, adresu IP, adres MAC),
    11) nieuprawniona rozbudowa sieci PM bez konsultacji z UCI poprzez m.in. instalacje punktów sieci bezprzewodowej, uruchamianie urządzeń i programów świadczących usługę typu DHCP, DNS, itd.,
    12) zmiana w lokalizacji aktywnych urządzeń sieciowych bez poinformowania UCI.

§ 17.

Prawa i obowiązki UCI

1. UCI jest odpowiedzialne za zarządzanie, administrowanie oraz koordynację działań zapewniających sprawne funkcjonowanie sieci PM.
2. UCI ma prawo zablokować dostęp do sieci PM użytkownikowi, który narusza postanowienia Regulaminu.
3. UCI jest uprawnione do:
   1) zmiany adresu IP ze względów technicznych i ze względów bezpieczeństwa,
   2) wglądu w konfigurację sieciowych urządzeń aktywnych oraz nadzór nad tą konfiguracją,
   3) prowadzenia kontroli przekazywanych w sieci informacji.
4. UCI jest zobowiązane do:
   1) stałego zabiegania o właściwy poziom bezpieczeństwa sieci,
   2) przydzielania adresów IP oraz przydzielania nazw w usłudze katalogowej,
   3) zapewnienia ciągłości pracy sieci PM,
   4) reagowania, w miarę technicznych możliwości, na powstałe w sieci PM problemy,
   5) zabezpieczania dowodów wszelkich prób nieautoryzowanego dostępu do sieci PM,
   6) nadzorowania majątku związanego z funkcjonowaniem sieci PM,
   7) usuwania lokalnych usterek i zakłóceń działania sieci PM.
   8) opracowywania rozwiązań i standardów, których celem jest optymalizacja kosztów eksploatacji sprzętu i oprogramowania**.**

Rozdział V
Zasady korzystania z elektronicznej poczty służbowej.

§ 18.

Oprogramowanie

1. Uczelnia stosuje jednolitą aplikację programową do obsługi elektronicznej poczty służbowej.
2. Wykorzystywanie innej aplikacji przez użytkownika odbywa się wyłącznie na jego własną odpowiedzialność i aplikacja taka nie jest objęta serwisem służby informatycznej.
3. Kierownik UCI podaje do wiadomości użytkowników informację na temat stosowanej jednolitej aplikacji programowej do obsługi elektronicznej poczty służbowej.

§ 19.

Konta pocztowe

1. Użytkownicy po odbyciu instruktarzu podstawowego otrzymują imienne konto pocztowe w określonym formacie. Konto pocztowe przydzielone użytkownikowi jest aktywne nie dłużej niż do ostatniego dnia odpowiednio okresu zatrudnienia lub współpracy.
2. W celu usprawnienia komunikacji między użytkownikami w Uczelni wprowadzona jest standaryzacja personalnych adresów elektronicznej poczty służbowej w formacie:
   <pierwsza_litera_imienia>.<nazwisko>@pm.szczecin.pl
   (np. j.kowalski @pm.szczecin.pl).
3. W sytuacjach szczególnych dopuszczony jest odmienny format adresu.
4. Oprócz adresów personalnych mogą być ustalane także adresy funkcjonalne dla jednostek organizacyjnych (z wykorzystaniem symboli organizacyjnych tych jednostek), zespołów tematycznych, komitetów organizacyjnych itp. (np. dla potrzeb organizacji konferencji) oraz

w uzasadnionych przypadkach aliasy do kont personalnych w innych formatach, niż określone w ust. 2. Adresy takie tworzone są na wniosek użytkowników i w formacie przez nich określanym.

§ 20.

Przeglądanie i sygnowanie poczty

1. Pracownicy administracyjni mają obowiązek co najmniej raz dziennie (w dni pracy) przejrzeć elektroniczną pocztę służbową na swoich komputerach.
2. Pozostali pracownicy powinni przeglądać kierowaną do nich pocztę elektroniczną systematycznie, z częstotliwością zapewniającą terminowy odbiór przesyłanych informacji i komunikatów.
3. Korespondencja elektroniczna winna być podpisywana imieniem i nazwiskiem pracownika, z podaniem co najmniej jego stanowiska służbowego lub funkcji, telefonu kontaktowego i adresu elektronicznej poczty służbowej.
4. W przypadku planowanej nieobecności w pracy należy dokonać ustawienia mechanizmu automatycznej odpowiedzi (autorespondera), w której winien być podany co najmniej czas nieobecności, kontakt telefoniczny i e-mail do osoby upoważnionej do działania w zastępstwie w celu zapewnienia ciągłości realizacji zadań służbowych.
5. Kierownik UCI podaje do wiadomości użytkowników instrukcję użytkowania elektronicznej poczty służbowej, w tym korzystania z autorespondera.
6. Dział Promocji:
   1) w uzgodnieniu z Rektorem ustala zawierający elementy graficzne wzór podpisu w elektronicznej poczcie służbowej (dalej: wzór podpisu),
   2) informuje użytkowników elektronicznej poczty służbowej za jej pośrednictwem o obowiązującym wzorze podpisu i miejscu, z którego może być pobrany,
   3) zamieszcza do pobrania wzór podpisu w Intranecie Uczelni, w sekcji „Dokumenty formalne”.
7. Kierownik UCI ustala Instrukcję samodzielnego skonfigurowania podpisu w elektronicznej poczcie służbowej. Przepis ust. 6 pkt. 2 i 3 stosuje się odpowiednio.

§ 21.

Bezpieczeństwo poczty elektronicznej

1. Zaleca się okresową zmianę hasła dostępu do służbowego konta pocztowego.
2. Użytkownik zobowiązany jest do przestrzegania tajemnicy swojego hasła do konta pocztowego.
3. Użytkownikom zabrania się:
   1) udostępniania swojego hasła lub konta pocztowego innym osobom,
   2) wykorzystywania konta pocztowego do rozsyłania Spamu.
4. W celu ograniczenia Spamu stosuje się odpowiednie zabezpieczenia.
5. Kierownik UCI podaje do wiadomości użytkowników szczegółowe informacje na temat stosowanych metod zabezpieczania elektronicznej poczty służbowej przed Spamem oraz instrukcje konfiguracyjne tej poczty.

§ 22.

Dystrybucja zbiorowych wiadomości do wszystkich pracowników

1. W celu ochrony przed nadużyciami elektroniczna poczta służbowa adresowana do wszystkich użytkowników Uczelni wysyłana jest za pośrednictwem UCI.
2. Wiadomości elektronicznej poczty służbowej adresowane „do wszystkich” wysyła się na specjalnie w tym celu wyznaczony adres pocztowy: wszyscy@pm.szczecin.pl. Wiadomości tego typu wysłane na inne adresy nie są rozsyłane.
3. Nadawcą wiadomości rozsyłanych „do wszystkich” jest „System poczty Politechniki Morskiej”.
4. Jednostka organizacyjna przygotowująca wiadomość odpowiada za jej treść.

5. Wiadomość jest rozsyłana w takiej samej formie, w jakiej zostanie przesłana. UCI nie dokonuje korekt, modyfikacji lub edycji wiadomości.
6. Wiadomość musi posiadać temat, który powinien również zawierać nazwę jednostki organizacyjnej wysyłającej wiadomość.
7. Korespondencja w ramach elektronicznej poczty służbowej winna być podpisywana imieniem i nazwiskiem pracownika, z podaniem co najmniej jego stanowiska służbowego lub funkcji, nazwy jednostki organizacyjnej, telefonu kontaktowego i adresu elektronicznej poczty służbowej.
8. Załącznik do rozsyłanej wiadomości nie powinien być większy niż 1 MB.
9. W uzasadnionych sytuacjach UCI może odmówić rozesłania wiadomości, powiadamiając o tym nadawcę, lub cofnąć wiadomość do uzupełnienia.

Rozdział VI
Zasady ochrony praw licencyjnych do oprogramowania komputerowego.

§ 23.

Zasady ogólne

Ochrona praw licencyjnych do oprogramowania komputerowego w Uczelni realizowana jest poprzez:

1) określenie indywidualnego i bezpośredniego modelu odpowiedzialności użytkowników za legalność użytkowanego oprogramowania,
2) powołanie Administratora Legalności, opiniującego prawo do posiadania konkretnych wersji oprogramowania,
3) wskazanie osób – Skarbników Licencji – odpowiedzialnych za przechowywanie dowodów legalności oprogramowania (kopie faktur, nośniki, licencje – EULA, dokumentacja, certyfikaty) – o ile nie jest to sprzeczne z wymogami licencyjnymi,
4) wprowadzenie w Uczelni centralnego rejestru legalnego oprogramowania,
5) kontrole i audyty legalności oprogramowania.

§ 24.

Legalność oprogramowania

1. Użytkownicy mogą wykorzystywać do celów służbowych lub na komputerach służbowych jedynie legalne oprogramowanie informatyczne.
2. Przez legalne oprogramowanie rozumie się:
   1) oprogramowanie nabyte przez Uczelnię z legalnego źródła i wykorzystywane zgodnie z warunkami udzielonej licencji,
   2) oprogramowanie bezpłatne,
   3) oprogramowanie opracowane przez pracowników Uczelni, do którego Uczelnia nabyła prawa autorskie,
   4) oprogramowanie opracowane w ramach realizowanych przez Uczelnię projektów (europejskich, krajowych), po uzyskaniu pozytywnej opinii odpowiednio opiekuna projektu (projekty europejskie) lub kierownika jednostki wsparcia (projekty krajowe) o możliwości jego wykorzystania na potrzeby własne Uczelni.

§ 25.

Zakup i powierzanie programów informatycznych

1. Dział Administracyjno-Gospodarczy przekazuje dowody legalności zakupionych przez tę jednostkę programów informatycznych do UCI wraz z kopią faktury zakupu.
2. Administrator Legalności:

1) odnotowuje zakupiony program w centralnym rejestrze programów,
2) skanuje dowody legalności i fakturę i umieszcza pliki w bazie danych w sposób zapewniający powiązanie programu z określonym obszarem, o którym mowa w § 28 ust. 1,
3) przekazuje dowody legalności za pokwitowaniem do właściwego Skarbnika Licencji.

3. Uczelnia powierzając użytkownikowi nowo zakupiony sprzęt komputerowy, powierza mu legalne oprogramowanie komputerowe.
4. Każdy użytkownik w ramach wstępnego szkolenia informatycznego:
   1) zostaje poinformowany o prawach i obowiązkach wynikających z posiadania oprogramowania;
   2) podpisuje porozumienie zobowiązujące go do przestrzegania zasad legalności oprogramowania; wzór porozumienia z pracownikiem stanowi załącznik nr 1 do Regulaminu, wzór porozumienia z osobą współpracującą stanowi załącznik nr 2 do Regulaminu;
   3) zostaje poinformowany o wykazie standardowego legalnego oprogramowania Uczelni, zamieszczonym i aktualizowanym na stronie intranetu pod adresem: **https://samszczecin.sharepoint.com/sites/UczelnianeCentrumInformatyczne**.

§ 26.

Instalacja samodzielna

1. Ze względu na zawiłości licencyjne użytkownikom nie wolno instalować ani umieszczać na jakimkolwiek nośniku Uczelni albo innym nośniku do celów służbowych żadnego oprogramowania bez zgody Administratora Legalności wyrażonej w formie pisemnej bądź elektronicznej.
2. Użytkownik może samodzielnie zainstalować program na użytkowanym komputerze służbowym po uprzednim zgłoszeniu takiego zamiaru Administratorowi Legalności i wyrażeniu przez niego zgody.
3. Administrator Legalności przed wyrażeniem zgody może zażądać okazania dowodów legalności oprogramowania. Przepisy § 25 ust. 2 pkt. 1 i 2 stosuje się odpowiednio.
4. Po uzyskaniu akceptacji użytkownik jest zobowiązany niezwłocznie przekazać odpowiednio zabezpieczone i oznakowane dowody legalności programów informatycznych właściwemu Skarbnikowi Licencji.
5. Administrator Legalności udziela użytkownikowi zgody w formie pisemnej bądź elektronicznej na instalację oprogramowania i rejestruje je w centralnym rejestrze legalnego oprogramowania.
6. Zgoda Administratora Legalności nie jest wymagana do zainstalowania:
   1) oprogramowania udostępnianego w systemie MSDNaa przez użytkowników zarejestrowanych w tym systemie,
   2) oprogramowania darmowego, które umieszczone jest na prowadzonej przez Administratora Legalności liście oprogramowania darmowego,
   3) oprogramowania próbnego/testowego na okres nie dłuższy niż 30 dni kalendarzowych,
   4) oprogramowania związanego z układami specjalizowanymi zamontowanymi w komputerze.

§ 27.

Administrator Legalności

1. Kierownik UCI wyznacza spośród podległych sobie pracowników odpowiednio przeszkolonego Administratora Legalności. W przypadku braku takiego wyznaczenia, sam pełni tę funkcję.
2. Do zadań Administratora Legalności należy:
   1) analizowanie treści licencji,
   2) wydawanie opinii co do legalności i zakresu korzystania z oprogramowania informatycznego,
   3) wyrażanie zgody na użytkowanie programów informatycznych,
   4) prowadzenie centralnego rejestru legalnego oprogramowania Uczelni,
   5) prowadzenie wykazu oprogramowania standardowego,
   6) prowadzenie listy oprogramowania, na instalację którego nie jest wymagana każdorazowo

zgoda Administratora Legalności.

3. W przypadku przyjmowania do użytkowania oprogramowania opracowanego w ramach projektów Administrator Legalności jest zobowiązany przed zarejestrowaniem takiego oprogramowania do uzyskania pozytywnej opinii odpowiednio opiekuna projektu (projekty europejskie) lub kierownika jednostki wsparcia (projekty krajowe).
4. W zakresie składanych wniosków, formułowanych zapytań oraz wydawanych przez Administratora Legalności opinii obowiązuje forma pisemna lub elektroniczna do celów dowodowych.

§ 28.

Skarbnicy Licencji

1. W obszarze Administracja, obszarach dziekanatów, instytutów, katedr, Biblioteki Głównej, jednostek międzywydziałowych, jednostek pozawydziałowych, pozostałych jednostek organizacyjnych oraz dla projektów europejskich i krajowych wyznacza się Skarbników Licencji, odpowiedzialnych za przechowywanie dowodów legalności oprogramowania zainstalowanego na komputerach w danych obszarach.
2. Skarbników Licencji wyznaczają spośród podległych pracowników, wprowadzając odpowiednie zapisy do zakresów czynności:
   1) kierownik UCI – dla obszaru Administracja, z wyłączeniem dziekanatów i Statku,
   2) kierownicy katedr, kierownicy wydziałowych centrów kształcenia, kierownicy jednostek ogólnouczelnianych, międzywydziałowych, pozawydziałowych i innych nie wymienionych wyżej – dla podległych obszarów organizacyjnych,
   3) kierownicy projektów – spośród etatowych pracowników projektu – dla obszarów poszczególnych projektów.
3. W razie niewyznaczenia Skarbnika Licencji, jego funkcję przejmuje:
   1) kierownik UCI – dla obszaru Administracja, z wyłączeniem dziekanatów i Statku,
   2) kierownicy dziekanatów, kierownik Domu Pracy Twórczej, kapitan Statku, kierownicy jednostek ogólnouczelnianych i pozawydziałowych poza obszarem Administracja – dla podległych obszarów organizacyjnych,
   3) pracownicy administracyjni, którym powierzono prowadzenie sekretariatu jednostki – w obszarach wydziałowych centrów kształcenia i jednostek międzywydziałowych,
   4) pracownicy administracyjni lub inżynieryjno-techniczni, którym powierzono prowadzenie sekretariatu jednostki – w obszarach katedr, a w przypadku braku takich pracowników – kierownicy katedr,
   5) kierownik projektu – dla obszaru danego projektu.
4. Do zadań Skarbnika Licencji należy:
   1) przypisywanie użytkowników do komputerów w ramach podległego obszaru, w systemie obsługującym centralny rejestr środków trwałych,
   2) prowadzenie magazynu dowodów legalności oprogramowania posiadanego w podległym obszarze (zwanych dalej DLO), w tym m.in.:
      a) przejęcie odpowiedzialności materialnej za powierzoną DLO,
      b) dbałość o stan techniczny i bezpieczeństwo przechowywania DLO,
      c) wypożyczanie DLO osobom uprawnionym,
      d) zabezpieczenie DLO przed dostępem osób nieuprawnionych,
      e) rzetelne prowadzenie ewidencji magazynowej DLO,
      f) prowadzenie dokumentacji przyjęcia/wydania DLO oraz innych zdarzeń dot. DLO,
   3) powiadamianie Administratora Legalności i przełożonego o brakach DLO,
   4) konsultowanie z Administratorem Legalności stanu prawnego DLO (zwłaszcza ilości i typu posiadanych DLO),

5) niezwłoczna realizacja zaleceń wydanych przez Administratora Legalności i przełożonych.

§ 29.

Dokumentacja legalności

1. W uzasadnionych wypadkach użytkownik może wypożyczyć od Skarbnika Licencji nośnik lub dokumentację do powierzonego mu oprogramowania. Jednak nie wolno mu naruszać warunków licencji.
2. Wypożyczone dowody legalności muszą zostać zwrócone Skarbnikowi Licencji w ciągu 30 dni kalendarzowych. W szczególnie uzasadnionych przypadkach istnieje możliwość przedłużenia okresu wypożyczenia.

§ 30

Kontrola legalności oprogramowania

1. Użytkownik może na swój wniosek otrzymać wykaz zainstalowanego na użytkowanym przez siebie komputerze oprogramowania wraz z oceną jego legalności wg stanu na dany dzień. Wykaz przygotowuje właściwa służba informatyczna, a oceny legalności dokonuje Administrator Legalności.
2. UCI dokonuje okresowo kontroli legalności oprogramowania. Zalecane jest, by rocznie poddać kontroli ok. 1-1,5 % losowo wybranych komputerów.
3. Uczelnia może zlecić w określonym zakresie audyt legalności oprogramowania firmie zewnętrznej, w szczególności gdy wyniki kontroli, o których mowa w ust. 1- 2 wskazują na powstanie poważnych ryzyk. Działania w tym zakresie w szczególności proponuje UCI.
4. W przypadku, gdy wyniku działań, o których mowa w ust. 1-3, okaże się, iż na komputerze zainstalowane było nielegalne oprogramowanie, Administrator legalności zleca właściwej służbie informatycznej postępowanie wyjaśniające, a po jego zakończeniu – usunięcie niezgodności.

Rozdział VII

Zasady przenoszenia praw autorskich do oprogramowania opracowanego przez pracowników Uczelni.

§ 31.

Nabycie praw

1. Prawa majątkowe do programu komputerowego stworzonego przez pracownika w wyniku wykonywania obowiązków ze stosunku pracy przysługują Uczelni, o ile umowa nie stanowi inaczej.
2. Pracownicy, którzy opracowali program informatyczny dla potrzeb użytkowych Uczelni, zgłaszają ten fakt niezwłocznie do Administratora Legalności oraz składają oświadczenie dotyczące potwierdzenia majątkowych praw autorskich Uczelni do programu. Wzór zgłoszenia stanowi załącznik nr 3 do Regulaminu.
3. Kierownik pionu, w którym ma być użytkowany ten program, potwierdza jego przydatność.
4. Dalsze postępowanie prowadzone jest zgodnie z Rozdziałem VI Regulaminu, przy czym zgłoszenie wraz z oświadczeniem, o którym mowa w ust. 2, stanowi dowód legalności oprogramowania w zakresie danego programu.
5. Niedopełnienie czynności, o których mowa w ust. 2 przez pracownika – twórcę programu i przekazanie go Uczelni lub jej pracownikom do użytkowania jest jednoznaczne z potwierdzeniem majątkowych praw autorskich Uczelni do tego programu i wyłącza dochodzenie od Uczelni jakichkolwiek roszczeń finansowych.

§ 32.

Obrót komercyjny

1. Programy, które mają być przekazane do użytku Uczelni odpłatnie, wymagają uprzedniego zawarcia z Uczelnią odpowiedniej umowy. W takich przypadkach stosuje się przepisy rozdziału VI Regulaminu.
2. Komercyjne dysponowanie prawami autorskimi Uczelni do programów komputerowych stworzonych przez pracowników regulują odrębne przepisy.

Rozdział VIII
Zasady przeprowadzania szkoleń informatycznych.

§ 33.

Szkolenie pracowników

1. Użytkownicy podlegają wstępnym i okresowym szkoleniom informatycznym.
2. Szkoleniom informatycznym podlegają pracownicy:
   1) nauczyciele akademiccy,
   2) pracownicy administracyjni,
   3) pracownicy Biblioteki Głównej,
   4) pracownicy inżynieryjno-techniczni i inżynieryjno-naukowi,
   5) pracownicy ochrony mienia.
3. Za wskazanie pracowników niewymienionych w ust. 2, a będących użytkownikami, odpowiadają ich przełożeni. Informacja w tym zakresie powinna być niezwłocznie przekazana do UCI.
4. Za wskazanie osób współpracujących odpowiadają właściwi kierownicy komórek lub kierownicy projektów, odpowiadający merytorycznie za umowę, na podstawie której następuje użytkowanie sprzętu informatycznego Uczelni. Informacja w tym zakresie powinna być niezwłocznie przekazana do UCI.

§ 34.

Szkolenie wstępne

1. Szkolenie informatyczne wstępne musi odbyć się nie później niż w ciągu 2 tygodni od momentu rozpoczęcia zatrudnienia lub udostępnienia sprzętu informatycznego do użytkowania, chyba że w ciągu ostatnich 5 lat użytkownik odbył w Uczelni szkolenie informatyczne wstępne lub okresowe, potwierdzone odpowiednimi dla tych szkoleń wymaganymi Regulaminem dokumentami.
2. Szkolenie wstępne powinno obejmować co najmniej tematykę:
   1) obsługa stanowiska komputerowego,
   2) logowanie do sieci,
   3) obsługę służbowej poczty elektronicznej,
   4) dysków sieciowych,
   5) serwera www i ftp,
   6) pracy zdalnej (VPN),
   7) legalności oprogramowania,
   8) ochrony danych osobowych w systemach informatycznych,
   9) zagrożeń bezpieczeństwa informacji, w tym zgłaszania incydentów,
   10) skutków naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialności prawnej,
   11) stosowania środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowań minimalizujących ryzyko błędów ludzkich,
   12) zadań UCI.

3. Szkolenie informatyczne wstępne może być przeprowadzane poprzez formie e-learningu, tj. kursu multimedialnego zakończonego testem wiedzy.
4. Szczegółową (rozszerzoną) tematykę i program szkolenia informatycznego określa kierownik UCI.
5. Szkolenie wstępne poprzedzone jest instruktażem podstawowym przeprowadzonym przez wyznaczonego pracownika UCI.
6. W ramach instruktażu podstawowego krótko omówione są zasady bezpiecznego użytkowania sprzętu informatycznego oraz przekazywana jest informacja o obowiązujących przepisach w zakresie polityki bezpieczeństwa informatycznego, ochrony praw licencyjnych do oprogramowania, ochrony danych osobowych i ochrony baz danych oraz wskazywany jest sposób dostępu do tych przepisów.
7. Odbycie instruktażu podstawowego upoważnia do założenia użytkownikowi przez pracownika UCI kont systemowych oraz nadania uprawnień dostępowych do pracy w sieci PM.
8. Instruktaż podstawowy przechodzą również pracownicy Uczelni wchodzący w skład załogi statku Uczelni.

§ 35.

Dokumentowanie szkoleń wstępnych

1. Odbycie instruktażu podstawowego i szkolenia informatycznego wstępnego potwierdzane jest przez użytkownika i osobę szkolącą na „Karcie szkolenia informatycznego wstępnego", zwanej dalej Kartą, której wzór stanowi załącznik nr 4 do Regulaminu. Potwierdzenie przez użytkownika odbycia szkolenia wstępnego przeprowadzonego w formie e-learningu nie jest na Karcie wymagane.
2. W przypadku nowo zatrudnianych pracowników Karta jest wystawiana przez UCI.
3. W przypadku pozostałych pracowników, Dział Kadr wystawia i wręcza pracownikowi Kartę po uzyskaniu informacji od przełożonego.
4. W przypadku osób współpracujących Kartę wystawia UCI po uzyskaniu informacji odpowiednio od kierownika komórki lub kierownika projektu, o których mowa w § 33 ust. 4.
5. Po przeprowadzeniu szkolenia informatycznego wstępnego Karta potwierdzająca przeszkolenie:
   1) pracownika – przekazywana jest do Działu Kadr w celu włączenia do akt osobowych pracownika,
   2) osoby współpracującej – pozostaje w UCI.
6. Jednostki wymienione w ust. 5 są odpowiedzialne za archiwizowanie dokumentów potwierdzających odbycie szkolenia co najmniej przez okres ich ważności.
7. Ewidencję szkoleń informatycznych pracowników prowadzi się w systemie informatycznym obsługującym kadry, w sposób zapewniający generowanie raportów zbiorczych zawierających informacje o terminach ważności szkoleń.
8. UCI prowadzi ewidencję szkoleń informatycznych osób współpracujących.

§ 36.

Szkolenie okresowe

1. Użytkownicy zobowiązani są odbywać szkolenie informatyczne okresowe co najmniej raz na 5 lat.
2. Program szkolenia okresowego powinien obejmować, co najmniej zakres tematyczny szkolenia wstępnego, o którym mowa w § 34 ust. 2.
3. Szkolenia informatyczne okresowe organizuje i przeprowadza UCI. § 34 ust. 3 i 4 oraz § 35 ust. 4 i 5 stosuje się odpowiednio.
4. Odbycie szkolenia okresowego potwierdzone jest wystawionym przez UCI Zaświadczeniem, którego wzór stanowi załącznik nr 5 do Regulaminu. Przepisy § 35 ust. 5-6 stosuje się odpowiednio.

Rozdział IX
Polityka informacyjna

§ 37.

1. UCI jest odpowiedzialne za propagowanie na terenie Uczelni stosowania ustalonych zasad i standardów dotyczących użytkowania sprzętu informatycznego, sieci informatycznej, ochrony danych i praw.
2. UCI prowadzi politykę informacyjną m.in. poprzez:
   1) zamieszczanie zasad, instrukcji, schematów procedur, wzorów formularzy i innych informacji na stronie intranetu pod adresem **https://samszczecin.sharepoint.com/sites/UczelnianeCentrumInformatyczne**,
   2) bieżące informowanie użytkowników, w tym za pomocą poczty elektronicznej o ustaleniu nowych lub zmianie dotychczasowych zasad, instrukcji, procedur itp. oraz sposobie zapoznania się z nimi (strona internetowa, jednostka organizacyjna itp.),
   3) instruktaż bieżący w ramach serwisu informatycznego, również za pomocą „Serwis PM",
   4) szkolenia informatyczne wstępne i okresowe,
   5) szkolenia i spotkania informacyjne organizowane doraźnie, wg potrzeb.

Rozdział X
Inwentaryzacja, przegląd i konserwacja urządzeń i systemów informatycznych

§ 38.

Zasady ogólne

1. UCI zapewnia utrzymywanie aktualności informatycznej inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.
2. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację urządzeń i systemów informatycznych.
3. Przeglądy i konserwację urządzeń i systemów informatycznych, z zastrzeżeniem ust. 4 i 5, zapewnia służba informatyczna.
4. Kierownik UCI może określić szczegółowe wytyczne dotyczące częstotliwości i sposobu dokonywania przeglądów i konserwacji urządzeń i systemów informatycznych, a także wydać dyspozycje dokonania dodatkowego przeglądu lub konserwacji konkretnych urządzeń lub systemów, jeżeli uzna taką potrzebę lub uwzględni zgłoszenie użytkownika lub jego przełożonego w tym zakresie.
5. Bieżący przegląd urządzeń informatycznych i punktów elektryczno-logicznych pod kątem ich sprawności użytkowo-eksploatacyjnej dokonują użytkownicy tych urządzeń.
6. Okresowy przegląd zewnętrznego stanu technicznego punktów elektryczno-logicznych dokonywany jest w ramach przeglądów pomieszczeń.
7. Nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji powinny być niezwłocznie zgłoszone odpowiednim służbom w celu ich usunięcia, a ich przyczyny przeanalizowane.
8. O fakcie ujawnienia istotnych nieprawidłowości zagrażających bezpieczeństwu danych lub systemów służba informatyczna niezwłocznie informuje przełożonego użytkownika lub – w przypadku większej skali nieusuniętego zagrożenia – właściwych kierowników pionów.

§ 39.

Przeglądy i konserwacja urządzeń informatycznych

1. Przeglądy i konserwacja urządzeń informatycznych powinny być wykonywane w terminach określonych przez producenta sprzętu.
2. Jeżeli producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych, lub też nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decydują służby informatyczne, przy czym komputery starsze niż 5 lat powinny podlegać przeglądom nie rzadziej niż raz w roku.
3. Użytkownicy mają obowiązek przeprowadzać bieżący przegląd użytkowanych urządzeń informatycznych pod kątem sprawności użytkowo-eksploatacyjnej oraz zgłaszać potrzeby konserwacyjne lub zakupowe w tym zakresie odpowiednio służbie informatycznej lub przełożonemu. Przełożeni sprawują nadzór nad wykonywaniem bieżącego przeglądu sprawności użytkowo-eksploatacyjnej urządzeń informatycznych użytkowanych w podległej jednostce.

§ 40.

Przeglądy systemów informatycznych

1. Przegląd systemów informatycznych, przeprowadzany jest w celu sprawdzenia poprawności ich działania i wykonywany jest nie rzadziej niż raz w roku oraz w następujących przypadkach:
   1) zmiany wersji oprogramowania w ramach centralnych systemów informatycznych,
   2) zmiany systemu operacyjnego centralnych urządzeń informatycznych w ramach centralnych systemów informatycznych,
   3) zmiany systemu operacyjnego na komputerze użytkownika,
   4) wykonania zmian w komputerze spowodowanych koniecznością naprawy lub modyfikacji systemu.
2. Przed dokonaniem zmian w centralnym systemie administracyjnym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych, na testowej bazie danych.
3. Przegląd systemów informatycznych może być przeprowadzany zdalnie, jeżeli istnieją do tego możliwości techniczne i gwarancja prawidłowości przeprowadzenia przeglądu. Przegląd zdalny polega m.in. na odczytaniu aktualnej konfiguracji sprzętowo-programowej komputera.
4. Właściwe jednostki realizujące zapewniają zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.
5. UCI przeprowadza okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmuje działania minimalizujące to ryzyko, stosownie do wyników przeprowadzonej analizy.
6. Dział Kontroli Wewnętrznej i Certyfikacji zapewnienia okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Rozdział Xa

Realizacja zadań i obowiązków wynikających z krajowego systemu cyberbezpieczeństwa

§ 40a.

Zakres przedmiotowy rozdziału

1. Uczelnia realizuje obowiązki podmiotów publicznych wynikające z ustawy o krajowym systemie cyberbezpieczeństwa jeżeli realizuje zadanie publiczne zależne od systemu informacyjnego – w zakresie tego systemu.
2. Kierownik UCI w porozumieniu z kierownikami właściwych merytorycznie komórek organizacyjnych i ich kierownikami pionów dokonuje analizy systemów informacyjnych pod kątem uzależnienia od nich wykonania zadań publicznych Uczelni oraz sporządza i aktualizuje listę takich systemów. Listę zatwierdza Prorektor ds. Innowacji i Rozwoju.

3. Jeżeli nie ma systemów do wpisania na listę, o której mowa w ust. 2, Kierownik UCI sporządzą notatkę służbową w tym zakresie, którą zatwierdza Prorektor ds. Innowacji i Rozwoju.
4. Obowiązki Uczelni w zakresie incydentów dotyczą incydentów, które powodują lub mogą spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez Uczelnię.
5. Poniższe przepisy niniejszego rozdziału realizuje się w razie funkcjonowania w uczelni systemu informacyjnego, od którego uzależniona jest realizacja zadań publicznych Uczelni.

§ 40b.

Osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa

1. Wyznacza się każdoczesnego kierownika UCI jako osobę odpowiedzialną za utrzymywanie kontaktów Uczelni z podmiotami krajowego systemu cyberbezpieczeństwa, chyba że Rektor wyznaczy w porozumieniu z kierownikiem UCI na piśmie inną osobę.
2. Kierownik UCI przygotowuje do podpisu Prorektora ds. Innowacji i Rozwoju i przekazuje do CSIRT NASK zgłoszenie danych osoby, o której mowa w ust. 1, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany. Jedną kopię pisma włącza się do akt osobowych osoby wyznaczonej.

§ 40c.

Zakres obowiązków UCI

1. UCI w porozumieniu z Prorektorem ds. Innowacji i Rozwoju:
   1) organizuje zarządzanie incydentem w Uczelni,
   2) zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do CSIRT NASK;
   3) zapewnia obsługę incydentu w Uczelni i incydentu krytycznego we współpracy z CSIRT NASK, przekazując niezbędne dane, w tym dane osobowe;
   4) zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na stronie internetowej Uczelni.
2. Zgłoszenie, o którym mowa w ust. 1 pkt 2, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej - przy użyciu innych dostępnych środków komunikacji.
3. Zgłoszenie, o którym mowa w ust. 1 pkt. 2, zawiera:
   1) dane Uczelni, w tym jej nazwę, siedzibę i adres;
   2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby składającej zgłoszenie;
   3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
   4) opis wpływu incydentu w Uczelni na realizowane zadanie publiczne, w tym:
      a) wskazanie zadania publicznego, na które incydent miał wpływ,
      b) liczbę osób, na które incydent miał wpływ,
      c) moment wystąpienia i wykrycia incydentu oraz czas jego trwania,
      d) zasięg geograficzny obszaru, którego dotyczy incydent,
      e) przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne Uczelni;

5) informacje o przyczynie i źródle incydentu;
6) informacje o podjętych działaniach zapobiegawczych;
7) informacje o podjętych działaniach naprawczych;
8) inne istotne informacje.

4. W zgłoszeniu przekazuje się informacje znane w chwili dokonywania zgłoszenia, które uzupełnia się w trakcie obsługi incydentu w Uczelni.
5. W zgłoszeniu przekazuje się, w niezbędnym zakresie, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań CSIRT NASK.
6. W zgłoszeniu oznacza się informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Rozdział XI
Postanowienia końcowe

§ 41.

Odpowiedzialność za naruszenie Regulaminu

1. Uczelnia nie ponosi jakiejkolwiek odpowiedzialności za naruszenie przez użytkowników lub inne osoby zasad Regulaminu i obowiązujących przepisów prawnych, w szczególności dotyczących naruszenia praw autorskich, rozpowszechniania w sieci treści naruszających istniejące normy prawne, obyczajowe oraz prawa i dobre imię innych użytkowników lub osób trzecich.
2. Za uszkodzenia, zniszczenie sprzętu oraz utratę danych, wynikłe z zaniedbania, nieprzestrzegania zapisów niniejszego Regulaminu lub nieprawidłowej obsługi komputera odpowiadają osoby winne tym zaniedbaniom.
3. Użytkownik sieci PM w ramach korzystania z tej sieci odpowiada za naruszenie zasad współżycia społecznego, działania niezgodne z obowiązującym porządkiem prawnym, działania, które naruszałyby dobra osobiste innych osób lub narażały te osoby na straty moralne lub materialne.
4. Użytkownik sieci PM umożliwiający pracę na swoich danych dostępowych innej osobie bierze na siebie pełną odpowiedzialność za poczynania tej osoby w ramach korzystania z sieci PM.
5. Odpowiedzialność, o której mowa w ust. 1-4, obejmuje odpowiedzialność karną, odpowiedzialność odszkodowawczą cywilną oraz odpowiedzialność służbową, dyscyplinarną i materialną.
6. Rażące naruszenie Regulaminu może spowodować zablokowanie dostępu do systemu informatycznego oraz konsekwencje służbowe i dyscyplinarne przewidziane w treści niniejszego Regulaminu oraz w Regulaminie pracy Politechniki Morskiej w Szczecinie.
7. Nieznajomość Regulaminu nie zwalnia z obowiązku jego przestrzegania i ponoszenia odpowiedzialności za jego naruszenie.

§ 42.

Rozstrzyganie sporów

1. Sprawy sporne pomiędzy użytkownikami a służbą informatyczną rozstrzyga kierownik UCI.
2. Odwołania od decyzji kierownika UCI rozpatruje Prorektor ds. Innowacji i Rozwoju.

§ 43.

W sprawach nieujętych w niniejszym Regulaminie zastosowanie mają przepisy kodeksu cywilnego, kodeksu karnego i inne przepisy prawa, a także wewnętrzne przepisy Uczelni.

Załącznik nr 1 do „Regulaminu informatycznego Akademii Morskiej w Szczecinie”
(Zarządzenie nr 4/2016 Rektora AM w Szczecinie z dnia 17.02.2016 r., z późn. zm.)

POROZUMIENIE

z pracownikiem

Niniejsze porozumienie (zwane dalej „Porozumieniem”) zostało zawarte w dniu ___ _____ 20___ r. w Szczecinie pomiędzy: Politechniką Morską w Szczecinie, ul. Wały Chrobrego 1-2, 71-500 Szczecin, zwaną dalej „Pracodawcą”, reprezentowaną przez: _____,

a

Panią/Panem _____, zwaną/ym dalej „Użytkownikiem”.

§ 1.

1. Porozumienie niniejsze zostaje zawarte w związku z pozostawaniem przez Użytkownika w stosunku pracy z Pracodawcą oraz korzystaniem przez Użytkownika z oprogramowania komputerowego przy wykonywaniu obowiązków służbowych.
2. Pracodawca wyposaża stanowisko pracy Użytkownika w legalne oprogramowanie komputerowe, zwane dalej „Oprogramowaniem”.
3. Wykaz standardowego legalnego oprogramowania znajduje się na stronie intranetu pod adresem **https://samszczecin.sharepoint.com/sites/UczelnianeCentrumInformatyczne**

§ 2.

1. Do podstawowych obowiązków Użytkownika należy:
   1) korzystanie z Oprogramowania w związku z wykonywaniem obowiązków służbowych, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania tych obowiązków lub realizacji tej umowy,
   2) niekorzystanie z jakiegokolwiek oprogramowania komputerowego, do używania którego Pracodawca nie jest uprawniony, w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Pracodawcy,
   3) zaniechanie instalowania na komputerach Pracodawcy jakiegokolwiek oprogramowania komputerowego, do używania którego Pracodawca nie jest uprawniony.
2. Użytkownik oświadcza, iż jest świadomy odpowiedzialności karnej, o której mowa w artykułach: 278 § 2, 293 w związku z artykułami 291 oraz 292 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997, Nr 88, poz. 553, z późn. zm.), oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach 116 i nast. ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r., Nr 90, poz. 631, z późn. zm.) za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie oprogramowania.
3. Użytkownik oświadcza, że znane są mu zasady używania Oprogramowania obowiązujące u Pracodawcy i zobowiązuje się do ich przestrzegania.
4. Użytkownik zobowiązuje się nie korzystać z Oprogramowania i sprzętu Pracodawcy w celu przechowywania, utrwalania, uzyskiwania lub zwielokrotniania wszelkich treści, mających postać zapisu elektronicznego, co do których Pracodawca nie nabył licencji lub które stanowią treści powszechnie uważane za obraźliwe, niemoralne czy też niezgodne z prawem, w tym naruszające prawa ich twórców.
5. Naruszenie przez Użytkownika podstawowych obowiązków, o których mowa w ust. 1, 3 i 4, może stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, w tym może stanowić podstawę wypowiedzenia przez Pracodawcę stosunku pracy łączącego Pracodawcę z Użytkownikiem, rozwiązania tego stosunku pracy bez wypowiedzenia z winy Użytkownika (zgodnie z przepisami ustawy z dnia 26 czerwca 1974 roku Kodeks pracy, Dz. U. z 2014 r. poz. 1502, z późn. zm., oraz ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce, Dz.U. z 2020 r., poz. 85, z późn. zm.) lub rozwiązania w trybie natychmiastowym wiążącej strony umowy cywilnoprawnej.
6. Użytkownik oświadcza, iż jest świadom tego, że naruszenie przez niego obowiązków w zakresie wskazanym powyżej, może skutkować powstaniem odpowiedzialności odszkodowawczej Użytkownika wobec Pracodawcy.

§ 3.

1. Porozumienie obowiązuje od chwili jego podpisania do końca trwania wiążącego strony stosunku pracy, nie krócej jednak niż przez okres użytkowania sprzętu komputerowego Pracodawcy.
2. Zmiana, uzupełnienie oraz rozwiązanie niniejszego Porozumienia za zgodą obu stron wymaga formy pisemnej pod rygorem nieważności.
3. Niniejsze Porozumienie zostało sporządzone w dwóch egzemplarzach, po jednym dla każdej ze stron i z chwilą podpisania stanowi załącznik do umowy regulującej stosunek pracy.

_____ _____

podpis Użytkownika *podpis osoby upoważnionej do reprezentowania Pracodawcy*

Załącznik nr 2 do „Regulaminu informatycznego Akademii Morskiej w Szczecinie”
(Zarządzenie nr 4/2016 Rektora AM w Szczecinie z dnia 17.02.2016. r., z późn. zm.)

POROZUMIENIE

z osobą współpracującą

Niniejsze porozumienie (zwane dalej „Porozumieniem”) zostało zawarte w dniu ___ _____ 20___ r. w Szczecinie pomiędzy: Politechniką Morską w Szczecinie, ul. Wały Chrobrego 1-2, 71-500 Szczecin, zwaną dalej „Politechniką” reprezentowaną przez: _____,

a

Panią/Panem _____ , zwaną/ym dalej „Użytkownikiem”.

§ 1.

1. Porozumienie niniejsze zostaje zawarte w związku z zawarciem pomiędzy Politechniką i Użytkownikiem umowy z dnia …… (zwanej dalej Umową) oraz korzystaniem przez Użytkownika z oprogramowania komputerowego przy wykonywaniu Umowy.
2. Politechnika wyposażyła stanowisko pracy Użytkownika w oprogramowanie komputerowe, zwane dalej „Oprogramowaniem”.
3. Wykaz standardowego legalnego oprogramowania znajduje się na stronie intranetu pod adresem **https://samszczecin.sharepoint.com/sites/UczelnianeCentrumInformatyczne**

§ 2.

1. Do podstawowych obowiązków Użytkownika należy:
   1) korzystanie z Oprogramowania w związku z realizacją Umowy, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków wynikających z Umowy,
   2) niekorzystanie z jakiegokolwiek oprogramowania komputerowego, do używania którego Politechnika nie jest uprawniona, w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Politechniki,
   3) zaniechanie instalowania na komputerach Politechniki jakiegokolwiek oprogramowania komputerowego, do używania którego Politechnika nie jest uprawniona.
2. Użytkownik oświadcza, iż jest świadomy odpowiedzialności karnej, o której mowa w artykułach: 278 § 2, 293 w związku z artykułami 291 oraz 292 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997, Nr 88, poz. 553, z późn.zm.), oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach 116 i nast. ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r., Nr 90, poz. 631, z późn. zm.) za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie oprogramowania.
3. Użytkownik oświadcza, że znane są mu zasady używania Oprogramowania obowiązujące w Politechnice i zobowiązuje się do ich przestrzegania.
4. Użytkownik zobowiązuje się nie korzystać z Oprogramowania i sprzętu Politechniki w celu przechowywania, utrwalania, uzyskiwania lub zwielokrotniania wszelkich treści, mających postać zapisu elektronicznego, co do których Politechnika nie nabyła licencji lub które stanowią treści powszechnie uważane za obraźliwe, niemoralne czy też niezgodne z prawem, w tym naruszające prawa ich twórców.
5. Naruszenie przez Użytkownika podstawowych obowiązków, o których mowa w ust. 1, 3 i 4, może stanowić podstawę do podjęcia przez Politechnikę przysługujących jej środków prawnych, w tym może stanowić podstawę wypowiedzenia przez Politechnikę Umowy łączącej Politechnikę z Użytkownikiem.
6. Użytkownik oświadcza, iż jest świadom tego, że naruszenie przez niego obowiązków w zakresie wskazanym powyżej, może skutkować powstaniem odpowiedzialności odszkodowawczej Użytkownika wobec Politechniki.

§ 3.

1. Porozumienie obowiązuje od chwili jego podpisania do końca trwania wiążącej strony Umowy, nie krócej jednak niż przez okres użytkowania sprzętu komputerowego Politechniki.
2. Zmiana, uzupełnienie oraz rozwiązanie niniejszego Porozumienia za zgodą obu stron wymaga formy pisemnej pod rygorem nieważności.
4. Niniejsze Porozumienie zostało sporządzone w dwóch egzemplarzach, po jednym dla każdej ze stron i z chwilą podpisania stanowi załącznik do zawartej Umowy.

_____ _____

podpis Użytkownika *podpis osoby upoważnionej do reprezentowania Politechniki*

……..
(imię i nazwisko)

……
(stanowisko)

……...
(jednostka organizacyjna)

\

Administrator Legalności
Uczelniane Centrum Informatyczne
Politechnika Morska
w Szczecinie

1. **Zgłoszenie opracowanego programu informatycznego dla potrzeb użytkowych Uczelni**
   Zgodnie z § 31 ust. 2 Regulaminu informatycznego PM zgłaszam, iż w wyniku wykonywania przeze mnie obowiązków ze stosunku pracy z Politechniką Morską w Szczecinie opracowałem/am program komputerowy :

   ……..……..……,
   który może być wykorzystywany do potrzeb Uczelni do celów/w obszarze organizacyjnym

   ……..……..…… .

2. **Oświadczenie dot. praw autorskich do programu informatycznego**
   Oświadczam, iż prawa majątkowe do wyżej wymienionego programu komputerowego przysługują Politechnice Morskiej w Szczecinie. Opracowany/współopracowany* przeze mnie program komputerowy nie narusza praw autorskich osób trzecich.
   Program został/nie został* opracowany w ramach projektu europejskiego/krajowego*.

   ……..… ……..…….
   (data) *(podpis zgłaszającego – autora programu)*

3. ****Opinia opiekuna projektu/kierownika jednostki wsparcia:**

   ……

   ……..… …….
   (data) *(podpis)*

4. **Kierownik pionu, w którym ma być użytkowany program:**
   Potwierdzam przydatność programu komputerowego dla potrzeb Politechniki Morskiej w Szczecinie.

   ……..… …….
   (data) *(podpis)*

5. **Adnotacje Administratora Legalności:**
   Program komputerowy wprowadzono do centralnego rejestru legalnego oprogramowania Uczelni pod nazwą ……..…… .

   ……..… …….
   (data) *(podpis)*

*niepotrzebne skreślić
**wypełnić tyko w przypadku programu opracowanego w ramach projektu

Załącznik nr 4 do „Regulaminu informatycznego Akademii Morskiej w Szczecinie”
(Zarządzenie nr 4/2016 Rektora AM w Szczecinie z dnia 17.02.2016 r.), z późn. zm.)

KARTA SZKOLENIA INFORMATYCZNEGO WSTĘPNEGO

I. DANE OSOBOWE

Imię i nazwisko……..,

Jednostka organizacyjna /Projekt: ……, Stanowisko ……..……,

Umowa cywilna nr…….…….. zawarta na okres od …… do ……

II. INSTRUKTAŻ PODSTAWOWY

Oświadczam, że zapoznałem się z „Regulaminem informatycznym Politechniki Morskiej w Szczecinie” i zasadami bezpieczeństwa kont dostępowych oraz zobowiązuję się do ich przestrzegania.

.....

(data i podpis użytkownika)

III. DANE DOSTĘPOWE

Założono następujące konta użytkownika umożliwiające pracownikowi pracę w sieci PM:

- usługa katalogowa (użytkownik w domenie ADM): .....
- skrzynka pocztowa (e-mail w domenie @pm.szczecin.pl): .....

.....

(data i podpis pracownika UCI)

IV. PRZEPROWADZONE SZKOLENIE WSTĘPNE

Program szkolenia

1. Obsługa stanowiska komputerowego
2. Logowanie do sieci
3. Obsługa poczty
4. Dyski sieciowe
5. Serwer www i ftp
6. Praca zdalna (VPN)
7. Legalność oprogramowania
8. Ochrona danych osobowych
9. Zagrożenia bezpieczeństwa informacji w tym zgłaszanie incydentów
10. Skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna
11. Stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizujących ryzyko błędów ludzkich
12. Zadania UCI
13. ……..
14. ……

Informacje dodatkowe ……..

Szkolenie odbyło się w dniu …… , w formie e-learningu: Tak/Nie

Zakres szkolenia wykonano zgodnie z w.w. programem.

.....

(podpis pracownika UCI)

.....

(podpis użytkownika
- nie wymagany przy formie e-learningu)

Załącznik nr 5 do „Regulaminu informatycznego Akademii Morskiej w Szczecinie”
(Zarządzenie nr 4/2016 Rektora AM w Szczecinie z dnia 17.02.2016 r., z późn. zm.)

KARTA SZKOLENIA INFORMATYCZNEGO OKRESOWEGO

I. DANE OSOBOWE

Imię i nazwisko……..,

Jednostka organizacyjna/Projekt: ……, Stanowisko ……..…….

II. PRZEPROWADZONE SZKOLENIE OKRESOWE

Program szkolenia

1. Obsługa stanowiska komputerowego
2. Logowanie do sieci
3. Obsługa poczty
4. Dyski sieciowe
5. Serwer www i ftp
6. Praca zdalna (VPN)
7. Legalność oprogramowania
8. Ochrona danych osobowych
9. Zagrożenia bezpieczeństwa informacji w tym zgłaszanie incydentów
10. Skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna
11. Stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizujących ryzyko błędów ludzkich
12. Zadania UCI
13. ……..
14. ……

Informacje dodatkowe ……..

Szkolenie odbyło się w dniu …… , w formie e-learningu: Tak/Nie

Zakres szkolenia wykonano zgodnie z w.w. programem.

....

(podpis pracownika UCI) *(podpis użytkownika - nie wymagany przy formie e-learningu)*