

REGULAMIN SIECI KOMPUTEROWEJ UNIwersYTETU JANA KOCHANOWSKIEGO W KIELCACH

§ 1 SŁOWNIK POJĘĆ

Użyte w Regulaminie określenia oznaczają:

- 1) Uniwersytet – Uniwersytet Jana Kochanowskiego w Kielcach;
- 2) Regulamin – niniejszy Regulamin;
- 3) operator – Dział Zabezpieczenia Informatycznego;
- 4) właściwy kierownik operatora – kierownik sekcji w ramach Działu Zabezpieczenia Informatycznego, właściwy do zadania w zakresie odpowiedzialności sekcji;
- 5) SK – Sieć Komputerowa Uniwersytetu – sieć komputerowa służąca do przesyłania danych z i do urządzeń Uniwersytetu, wraz z usługami i zasobami;
- 6) urządzenie – urządzenie podłączone w sposób trwały lub tymczasowy do SK;
- 7) zasób – dane gromadzone/ przetwarzane/ udostępniane za pomocą urządzeń jednostki organizacyjnej/ Uniwersytetu (np. adresy sprzętowe i internetowe, przestrzeń pamięci dyskowej serwerów, aplikacje, bazy danych, strony WWW usługi dostępu do platform pracy i kształcenia zdalnego itp.);
- 8) usługa – udostępnianie i dostęp do zasobów i urządzeń poprzez SK;
- 9) sieć lokalna – wydzielony fragment SK UJK użytkowany w obrębie jednostki organizacyjnej;
- 10) sieć szkieletowa – sieć komputerową łączącą sieci lokalne;
- 11) punkt styku – port (złącze) urządzenia sieci, do której podłączona jest sieć lokalna;
- 12) użytkownik – osoba korzystająca z SK zgodnie z jej przeznaczeniem;
- 13) administrator centralny (AC) – wyznaczona osoba z ramienia Działu Zabezpieczenia Informatycznego, mająca w swoim zakresie odpowiedzialności zarządzanie określonymi urządzeniami, usługami, zasobami SK oraz nadzór nad ich bezpieczeństwem teleinformatycznym;
- 14) administrator lokalny (AL) – osoba delegowana w danej jednostce organizacyjnej do obsługi sieci lokalnej;
- 15) dysponent zasobu (DZ) – osoba kierująca jednostką organizacyjną Uniwersytetu, która posiada/udostępnia zasoby/usługi, ustala zasady wykorzystywania zasobu;
- 16) administrator zasobów (AZ) – osoba oddelegowana w danej jednostce organizacyjnej przez dysponenta zasobu do zarządzania usługami/zasobami;
- 17) elektroniczne urządzenia przenośne – komputer przenośny (laptop), tablet, telefon komórkowy, smartfon, itp. [...] z podstawową funkcją urządzeń mobilnych, tzn. pracą w dowolnym miejscu, z wykorzystaniem technik komunikacyjnych bez konieczności utrzymywania połączenia przewodowego z Internetem.

§ 2 POSTANOWIENIA OGÓLNE

1. Regulamin ustala zasięg, zasady funkcjonowania i korzystania z SK zlokalizowanej w obiektach Uniwersytetu.
2. Regulamin dotyczy wszystkich użytkowników SK.
3. Użytkownicy SK mają obowiązek stosować obowiązujące w Uniwersytecie przepisy dotyczące ochrony informacji, określone w Polityce bezpieczeństwa informacji, Polityce bezpieczeństwa

w zakresie ochrony danych osobowych oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych. Nieprzestrzeganie zasad wynikających z w/w dokumentów może skutkować zablokowaniem dostępu do zasobów i usług w ramach SK.

4. Sieć Komputerowa służy do wspomagania realizacji zadań statutowych Uniwersytetu – kształcenia i prowadzenia badań naukowych oraz koniecznych działań administracyjnych.
5. Sieć Komputerowa zapewnia możliwość komunikacji urządzeń w obrębie Uniwersytetu oraz dostęp do Sieci MAN, PIONIER (w tym również usług teleinformatycznych realizowanych w sieci PIONIER, takich jak Federacyjne Zarządzanie Tożsamością PIONIER.Id, sieć bezprzewodowa eduroam), a następnie do innych akademickich i naukowych sieci komputerowych w kraju i zagranicą oraz do Internetu.
6. Urządzeniami komunikującymi się z wykorzystaniem infrastruktury teleinformatycznej Uniwersytetu mogą być wyłącznie urządzenia użytkowane zgodnie z przeznaczeniem SK UJK, a więc do celów wynikających z zadań statutowych, organizacyjnych oraz administracyjnych Uniwersytetu lub jednostki organizacyjnej.
7. Usługi i zasoby Sieci Komputerowej muszą być zgodne z jej przeznaczeniem, a więc służyć do celów wynikających z zadań statutowych, organizacyjnych oraz administracyjnych Uniwersytetu.
8. Użytkownikami są pracownicy, wykonawcy umów cywilno-prawnych, doktoranci i studenci wszystkich form studiów Uniwersytetu, słuchacze studiów podyplomowych, uczestnicy kursów i szkoleń. Studenci innych uczelni oraz goście Uniwersytetu, a także podmioty zewnętrzne niebędące osobami fizycznymi, mogą stać się czasowymi użytkownikami sieci po uzyskaniu zgody kierownika właściwej jednostki organizacyjnej, a w przypadku konieczności dodatkowej konfiguracji urządzeń/ zasobów/ usług Uniwersytetu – właściwego kierownika operatora. Wszyscy użytkownicy oraz administratorzy Sieci Komputerowej zobowiązani są do przestrzegania prawa, zasad współżycia społecznego oraz zasad etyki, w szczególności poprzez powstrzymywanie się od podejmowania działań, które naruszałby dobra osobiste innych osób lub narażałyby te osoby na straty materialne, a także takie, które mogą zakłócać pracę Sieci Komputerowej oraz narażać na niebezpieczeństwo urządzenia i zasoby Uniwersytetu.

§ 3

STRUKTURA SIECI KOMPUTEROWEJ UNIWERSYTETU JANA KOCHANOWSKIEGO W KIELCACH

1. SK składa się z:
 - 1) sieci szkieletowej – zarządzanej przez AC;
 - 2) sieci bezprzewodowej – zarządzanej przez AC,
 - 3) sieci lokalnych – zarządzanych przez AL;
 - 4) zasobów i usług Uniwersytetu – zarządzanych przez AC;
 - 5) zasobów i usług jednostek organizacyjnych – zarządzanych przez AZ;– przy czym sieci komputerowe znajdujące się w budynkach Miasteczek Akademickich Uniwersytetu w Kielcach i Filii w Piotrkowie Trybunalskim traktowane są jako wyodrębnione sieci lokalne.
2. Podstawą do powołania AC, AL, oraz AZ jest wniosek stanowiący załącznik nr 1 do Regulaminu.
3. Podstawą do uruchomienia zasobu/usługi jest właściwy wniosek stanowiący jeden z załączników od 2a do 2h – w zależności od szczegółowego przedmiotu tego wniosku.
4. Siecią szkieletową, siecią bezprzewodową oraz ogólnouczelnianymi usługami i zasobami Uniwersytetu zarządzają administratorzy powołani przez kierownika właściwej sekcji w ramach Działu Zabezpieczenia Informatycznego.
5. Sieciami lokalnymi zarządzają lokalni administratorzy powołani przez osobę zarządzającą jednostką organizacyjną.

6. Sieć lokalna, przyłączona do sieci szkieletowej, może zawierać sieci lokalne składowych jednostek organizacyjnych.
7. Punkt styku z siecią szkieletową stanowi część sieci szkieletowej. Punkt styku z siecią lokalną stanowi część nadrzędnej sieci lokalnej.
8. Zasobami i usługami jednostek organizacyjnych administrują, powołani przez DZ, administratorzy zasobów.
9. Każda sieć lokalna, usługa i zasób jednostki organizacyjnej musi posiadać swojego administratora lokalnego lub administratora zasobów, będącego pracownikiem jednostki.
10. Aktualizacja dokumentacji dotyczącej uruchomienia usług i zasobów jednostki organizacyjnej leży po stronie dysponenta zasobów.
11. Zasoby Uniwersytetu są rejestrowane, a rozwiązania techniczne konieczne do ich uruchomienia są zatwierdzane przez kierownika właściwej sekcji, w ramach Działu Zabezpieczenia Informatycznego w zakresie usług/ zasobów/ infrastruktury teleinformatycznej Uniwersytetu.
12. Kierownik Działu Zabezpieczenia Informatycznego, na wniosek kierownika właściwej sekcji, występuje do kierownika jednostki organizacyjnej/dysponenta zasobu o wyznaczenie innego administratora lokalnego lub administratora zasobu w przypadku, gdy aktualny administrator nie wykonuje swoich obowiązków lub wykonuje je niewłaściwie.

§ 4

ADMINISTROWANIE SIECIĄ KOMPUTEROWĄ UNIwersYTETU JANA KOCHANOWSKIEGO W KIELCACH

1. Operator, poprzez właściwych administratorów centralnych (AC), w szczególności:
 - 1) dba o prawidłową eksploatację SK;
 - 2) projektuje wykorzystanie i wdraża konfigurację urządzeń, usług i zasobów Uniwersytetu;
 - 3) odpowiada za połączenie urządzeń/ usług/ zasobów SK z Internetem;
 - 4) opracowuje i aktualizuje zasady korzystania z infrastruktury teleinformatycznej oraz określa procedury w zakresie bezpieczeństwa sieci, urządzeń sieciowych oraz aplikacji i danych, w tym udostępnia zasoby na podstawie właściwych wniosków – załączniki nr 2a-2h do Regulaminu;
 - 5) może zrealizować zdalny dostęp do wskazanych zasobów Uniwersytetu przez bezpieczny tunel szyfrowany; podstawą do uzyskania zdalnego dostępu jest wypełniony wniosek – załącznik nr 2h do Regulaminu – oraz zapis w umowie w przypadku podmiotów zewnętrznych; przyznane dostępy zdalne do zasobów SK są rejestrowane;
 - 6) dba o aktualizację oprogramowania centralnych urządzeń sieci szkieletowej, serwerów, usług i zasobów Uniwersytetu;
 - 7) odpowiada za bezpieczeństwo centralnych urządzeń sieci szkieletowej, usług i zasobów Uniwersytetu;
 - 8) monitoruje stan centralnych urządzeń, systemów i usług;
 - 9) zarządza systemem kopii zapasowych aplikacji ogólnouczelnianych;
 - 10) zapewnia stały monitoring parametrów środowiskowych (takich jak temperatura, wilgotność) oraz ciągłość zasilania poprzez stosowanie zasilaczy awaryjnych, agregatów prądotwórczych lub niezależnych linii energetycznych w głównych węzłach sieciowych i centrach przetwarzania danych;
 - 11) prowadzi rejestr zdarzeń związanych z eksploatacją SK, zasobów i usług (w wersji elektronicznej w oparciu o funkcje udostępniane przez poszczególne urządzenia/systemy);
 - 12) prowadzi niezbędną dokumentację, w tym Ewidencję Sieci (załącznik nr 3 do Regulaminu) i ewidencję zasobów i usług;
 - 13) przygotowuje adresację IP i konfiguruje uprawnienia dostępowe dla sieci lokalnych;

- 14) nadzoruje pracę sieci lokalnych;
 - 15) monitoruje usługi/zasoby jednostek organizacyjnych pod kontem bezpieczeństwa SK;
 - 16) po uzyskaniu zgody kierownika operatora może zablokować działanie sieci lokalnych, usług i zasobów jednostek organizacyjnych oraz urządzeń końcowych i użytkowników w przypadku naruszenia Regulaminu lub stwierdzenia nieprawidłowości w działaniu/zarządzaniu.
2. Administrator lokalny (w szczególności):
- 1) dba o bezpieczeństwo i prawidłową eksploatację sieci lokalnej;
 - 2) odpowiada za sieć lokalną i wykonuje zadania powierzone przez operatora;
 - 3) wspiera jednostkę organizacyjną i użytkowników w działaniach związanych z siecią lokalną;
 - 4) monitoruje stan podległych urządzeń aktywnych i odpowiada za ich konfigurację;
 - 5) prowadzi niezbędną dokumentację, w tym Ewidencję Sieci (załącznik nr 3 do Regulaminu) i zasobów;
 - 6) prowadzi rejestr zdarzeń związanych z eksploatacją SK (w wersji elektronicznej w oparciu o funkcje udostępniane przez poszczególne urządzenia/systemy);
 - 7) dokumentuje zmiany mające wpływ na punkty styku z siecią szkieletową w Karcie zmian w sieci lokalnej, stanowiącej załącznik nr 4 do Regulaminu, w wersji elektronicznej, i na bieżąco przesyła ją do odpowiedniego AC;
 - 8) przyjmuje zgłoszenia dotyczące problemów w sieci lokalnej od użytkowników i po przeprowadzeniu testów, w razie potrzeby, zgłasza problem operatorowi;
 - 9) w przypadku stwierdzenia naruszenia Regulaminu, na wniosek kierownika Działu Zabezpieczenia Informatycznego lub kierownika właściwej sekcji (lub z własnej inicjatywy – po uzyskaniu zgody osoby powołującej) odłącza urządzenia w sieci lokalnej.
3. Administrator zasobów, odpowiadając za powierzone mu usługi i zasoby (w szczególności):
- 1) dba o prawidłową eksploatację;
 - 2) odpowiada za bezpieczeństwo;
 - 3) monitoruje ich stan;
 - 4) dba o bieżącą aktualizację oprogramowania związanego z usługami i zasobami jednostki organizacyjnej;
 - 5) prowadzi rejestr zdarzeń związanych z eksploatacją usług i zasobów (w wersji elektronicznej w oparciu o funkcje udostępniane przez poszczególne urządzenia/systemy);
 - 6) udziela dostępu użytkownikom, wspiera jednostkę organizacyjną i użytkowników w działaniach związanych z zasobami i usługami;
 - 7) dba, aby strony WWW spełniały warunki określone w załączniku nr 5 do Regulaminu;
 - 8) w przypadku stwierdzenia naruszenia Regulaminu, na wniosek kierownika Działu Zabezpieczenia Informatycznego lub kierownika właściwej sekcji (lub z własnej inicjatywy – po uzyskaniu zgody dysponenta zasobów) blokuje dostęp użytkowników do usług/zasobów.

§ 5

OBOWIĄZKI UŻYTKOWNIKÓW

1. Użytkownik SK zobowiązany jest w szczególności do:
 - 1) zapoznania się z niniejszym Regulaminem i przestrzegania jego zapisów;
 - 2) korzystania z SK zgodnie z zadaniami, do których sieć została stworzona;
 - 3) przestrzegania przepisów dotyczących ochrony informacji, w szczególności danych osobowych, w tym Polityki bezpieczeństwa informacji, Polityki bezpieczeństwa w zakresie ochrony danych osobowych oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych;

- 4) zapobiegania kradzieży i nieupoważnionemu użytkowaniu stacji roboczej, przekazanej do użytkowania (w tym elektronicznego urządzenia przenośnego), dbania o bezpieczeństwo powierzonego sprzętu oraz ochronę swoich zasobów w szczególności poprzez szyfrowanie nośników/danych oraz dostępu do konta, a także natychmiastowego zgłaszania do administratora informacji o lukach stwierdzonych w systemie praw dostępu lub wskazujących na uzyskanie dostępu do zasobów przez osoby do tego nieuprawnione;
 - 5) dbania o bezpieczeństwo nośników danych, w tym sprzętu komputerowego, objętego procedurą likwidacji – (nośniki danych przy likwidacji sprzętu komputerowego podlegają zdemagnetyzowaniu i fizycznemu zniszczeniu zgodnie z procedurą, opisaną w załączniku nr 6 do Regulaminu);
 - 6) stosowania wygaszaczy ekranu z ustawionym hasłem i hasła dostępowego do komputera;
 - 7) zmian swojego hasła co najmniej raz na kwartał z zastrzeżeniem wymogów Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych;
 - 8) nieujawniania swoich haseł;
 - 9) nieodpowiadania na oferty przesyłane jako reklamy lub spam, sprawdzanie podejrzanych załączników programem antywirusowym;
 - 10) przestrzegania poufności zasobów w systemie i nieingerowania w ich zawartość, nawet jeśli nie byłyby one stosownie chronione;
 - 11) umożliwiania dostępu do powierzonych zasobów tylko osobom uprawnionym;
 - 12) przekazywania informacji o nieprawidłowości w działaniu sieci usług i zasobów do administratora lokalnego lub administratora zasobów;
 - 13) natychmiastowego zgłoszenia utraty danych do logowania (login/hasło) do administratora zasobu;
 - 14) aktualizowania i przechowywania wymaganej dokumentacji, dotyczącej powierzonego zasobu/urządzeń Uniwersytetu;
 - 15) niepodjmowania działań niezgodnych z przepisami prawa, Regulaminem, normami społecznymi oraz netykietą sieciową;
 - 16) posiadania konta na serwerze UJK, które jest zakładane na podstawie wniosku o założenie konta pocztowego, stanowiącego załącznik nr 2c do Regulaminu;
 - 17) przestrzegania zasad bezpiecznego odbierania i wysłania informacji, w tym danych osobowych, za pomocą służbowej poczty elektronicznej, w spakowanych plikach, zabezpieczonych silnym, niesłownikowym hasłem, składającym się z minimum 8 znaków, które zawiera małe i duże litery oraz znaki specjalne; hasło nie może być przekazywane razem z zabezpieczonym plikiem;
 - 18) przestrzegania zasad bezpiecznego wysyłania wiadomości e-mail do więcej niż jednego adresata;
 - 19) podporządkowania się zaleceniom administratorów dotyczącym eksploatacji zasobów sieci, a także stosowania haseł zgodnych z zaleceniami administratorów;
 - 20) przestrzegania zasad bezpiecznego korzystania z usług systemu eduroam dostępnych pod adresem <https://www.eduroam.pl/regulamin/>;
 - 21) przestrzegania zasad bezpiecznego dostępu do zewnętrznych usług sieciowych w ramach Polskiej Federacji Zarządzania Tożsamością PIONIER.Id, opisanych w załączniku nr 7 do Regulaminu;
 - 22) przestrzegania zasad bezpiecznego korzystania z usług platform do pracy i kształcenia zdalnego, opisanych w załączniku nr 8 do Regulaminu
2. Użytkownikowi SK zabrania się:
- 1) udostępniania zasobów innym użytkownikom i osobom nieuprawnionym;
 - 2) podszywania się pod innych użytkowników, nielegalnego pozyskiwania informacji z SK, wykonywania czynności mogących zakłócać funkcjonowanie sieci i jej zasobów poprzez naruszanie bezpieczeństwa lub stabilności, w szczególności atakowania sieci lub jej zasobów, deszyfrowania haseł, podsłuchiwanie lub przechwytywanie informacji przepływającej w sieci, skanowania portów, celowego przeciążania łącz, uniemożliwiania działania usług sieciowych,

- wysyłania spamu (niechcianej korespondencji), świadomego rozsyłania szkodliwego oprogramowania;
- 3) włączania do gniazd elektrycznych sieci komputerowej urządzeń elektrycznych do tego nieprzeznaczonych;
 - 4) podłączania do sieci i odłączania od niej jakichkolwiek urządzeń bez zgody administratora, w szczególności dołączania urządzeń technicznych umożliwiających dostęp do SK przez osoby nieuprawnione;
 - 5) zmieniania ustawień konfiguracji sieciowej urządzenia sieciowego lub końcowego (komputer, drukarka) bez zgody administratora, w szczególności zmieniania adresu sprzętowego lub przyznanego adresu internetowego;
 - 6) nieuprawnionej rozbudowy sieci, między innymi poprzez niedozwolone uruchamianie urządzeń i programów, mogących zakłócać pracę innych urządzeń w sieci, np. świadczących usługę DHCP, jak router bezprzewodowy lub przewodowy;
 - 7) składowania, instalowania i uruchamiania oprogramowania bez licencjonowanego prawa do jego posiadania i wykorzystywania,
 - 8) podejmowania działań mających na celu niezgodne z prawem gromadzenie, udostępnianie, kopiowanie i rozpowszechnianie zasobów prawnie chronionych, w tym utworów objętych prawem autorskim.

§ 6

PRZERWY W DZIAŁANIU SIECI I ZGŁASZANIE AWARII

1. Zaplanowane przerwy w działaniu sieci oraz usług i zasobów operator zobowiązany jest ogłosić zainteresowanym drogą mailową z wyprzedzeniem 3 dni.
2. Wszelkie inne przerwy w działaniu SK będą uznane za awarie.
3. W razie wystąpienia awarii (przeciążenia lub niezaplanowanej przerwy w działaniu sieci oraz usług i zasobów SK) obowiązkiem Działu Zabezpieczenia Informatycznego jest niezwłoczne usunięcie awarii oraz powiadomienie osób zainteresowanych o jej przyczynach i podjętych działaniach naprawczych zgodnie z Instrukcją zapewnienia ciągłości działania opracowaną na podstawie Polityki Bezpieczeństwa Informacji.
4. Zgłaszanie awarii SK:
 - 1) użytkownicy zgłaszają problemy z funkcjonowaniem SK do swoich lokalnych administratorów lub administratorów zasobów;
 - 2) właściwy lokalny administrator przystępuje do czynności diagnostycznych; po usunięciu nieprawidłowości informuje zgłaszającego;
 - 3) w przypadku braku możliwości usunięcia awarii (wykraczającej poza zakres odpowiedzialności administratora) właściwy administrator przekazuje sprawę operatorowi;
 - 4) administrator lokalny lub administrator zasobów zobowiązany jest do współpracy z AC w trakcie usuwania awarii w zakresie podległej mu sieci/ usługi/ zasobu.

§ 7

POSTANOWIENIA KOŃCOWE

1. O naruszeniu Regulaminu powiadamiany jest przełożony użytkownika, w przypadku studentów, doktorantów, słuchaczy studiów podyplomowych i uczestników kursów i szkoleń – właściwy dziekan, a w przypadkach dotyczących działania sieci lokalnych Miasteczek Akademickich Prorektor ds. Kształcenia.
2. Uniwersytet nie ponosi odpowiedzialności z tytułu szkód poniesionych na skutek awarii SK.

3. Całkowitą odpowiedzialność prawną za treść udostępnianą, przechowywaną lub sprowadzaną, ponosi użytkownik urządzenia, które zostało wykorzystane do zapisu lub przechowywania treści.
4. Za zgodą Rektora, na wniosek upoważnionych organów, operator ma obowiązek udostępnić wszystkie posiadane dane użytkowników, urządzeń, usług i wydarzeń w podległej sieci.

§ 8

W Uniwersytecie, do przeprowadzenia spraw uregulowanych Regulaminem, stosuje się następujące instrukcje i wzory, stanowiące załączniki do niniejszego zarządzenia:

- 1) załącznik nr 1 – wniosek o rejestrację administratora/administradora zasobów/ lokalnego administratora z oświadczeniem o zachowaniu poufności;
- 2) załącznik nr 2a – wniosek o założenie telefonu;
- 3) załącznik nr 2b.1. – uprawnienia do zasobów Zintegrowanego Systemu Informatycznego Uniwersytetu Jana Kochanowskiego w Kielcach (moduły w części obsługi toku studiów);
- 4) załącznik nr 2b.2. – uprawnienia do zasobów Zintegrowanego Systemu Informatycznego Uniwersytetu Jana Kochanowskiego w Kielcach (Simple ERP),
- 5) załącznik nr 2c – wniosek o założenie konta pocztowego;
- 6) załącznik nr 2d – wniosek o założenie serwisu WWW;
- 7) załącznik nr 2e – wniosek o uruchomienie tymczasowej sieci wi-fi;
- 8) załącznik nr 2f – wniosek o dostęp do sieci wi-fi w Miasteczku Akademickim dla osób spoza UJK;
- 9) załącznik nr 2g – wniosek o udostępnienie innego zasobu/ usługi;
- 10) załącznik nr 2h – wniosek o usługę zdalnego udostępnienia zasobu;
- 11) załącznik nr 3 – Ewidencja Sieci;
- 12) załącznik nr 4 – Karta zmian w sieci lokalnej (dokument elektroniczny);
- 13) załącznik nr 5 – Zasady tworzenia serwisów WWW;
- 14) załącznik nr 6 – Procedura postępowania w zakresie niszczenia elektronicznych nośników informacji;
- 15) załącznik nr 7 – Regulamin korzystania z zewnętrznych usług sieciowych dostępnych przez Centralny Punkt Logowania;
- 16) załącznik nr 8 – Zasady korzystania z platform do pracy i nauki na odległość.