

## **Regulamin użytkowania Uczelnianej Sieci Komputerowej w Uniwersytecie Śląskim w Katowicach**

### §1

#### Postanowienia ogólne

1. Uczelniana Sieć Komputerowa Uniwersytetu Śląskiego w Katowicach (USK, zarejestrowana w Internecie jako USNET) przyłączona jest do Śląskiej Akademickiej Sieci Komputerowej (ŚASK) oraz innych sieci komputerowych. W kwestiach nieuregulowanych niniejszym regulaminem użytkowanie USK podlega przepisom zawartym w regulaminach tych sieci.
2. USK stanowi infrastrukturę wspomagającą realizację celów statutowych Uniwersytetu.
3. Zgodę na wykorzystanie sieci USK w zakresie wykraczającym poza cele statutowe Uniwersytetu wydaje Rektor.
4. USK nie może być wykorzystywana w sposób naruszający obowiązujące przepisy prawa.
5. Uniwersytet Śląski w Katowicach nie ponosi odpowiedzialności z tytułu strat wynikających z awarii USK.
6. Prawo do korzystania z USK mają:
  - 1) wszyscy członkowie społeczności akademickiej – pracownicy, doktoranci, studenci, stypendiści, uczestnicy innych form kształcenia, stażyści, goście Uniwersytetu;
  - 2) mieszkańcy domów studenta i domów asystenta;
  - 3) osoby fizyczne lub prawne wynajmujące lub użytkujące na podstawie umowy lub porozumienia pomieszczenia Uniwersytetu. Decyzję o udostępnieniu sieci komputerowej najemcom podejmuje Zastępca Kanclerza ds. Administracyjnych i Zarządzania Mieniem po zasięgnięciu opinii Dyrektora ds. Informatyzacji;
  - 4) inne osoby w zakresie udostępnionych na ich potrzeby przez Uniwersytet Śląski w Katowicach usług sieciowych.

## §2

### Struktura sieci

1. USK jest podzielona na segmenty:
  - 1) sieć szkieletową - obejmującą połączenia pomiędzy budynkami oraz łączy do operatora;
  - 2) sieci lokalne - sieci komputerowe funkcjonujące w obrębie poszczególnych budynków;
  - 3) sieci wykorzystywane i zarządzane przez podmioty wynajmujące pomieszczenia na podstawie umowy.
2. Za utrzymanie okablowania sieci szkieletowej odpowiedzialna jest Sekcja Teletechniczna.
3. Za administrowanie siecią szkieletową odpowiedzialny jest Dział Administracji Sieci i Usług Sieciowych.
4. Za okablowanie oraz administrowanie sieciami lokalnymi dla poszczególnych budynków, z wyłączeniem budynku Rektoratu, CINIBA oraz budynków domów studenta, odpowiedzialny jest Zespół Infrastruktury Informatycznej Kampusu Chorzowskiego, Cieszyńskiego, Katowickiego lub Sosnowieckiego zależnie od tego, który zespół zapewnia obsługę informatyczną w danej lokalizacji.
5. Za okablowanie oraz administrowanie siecią lokalną w budynku Rektoratu odpowiedzialny jest Dział Informatycznych Systemów Zarządzania.
6. Za okablowanie oraz administrowanie siecią lokalną w budynkach domów studenta odpowiedzialne jest Osiedle Akademickie.
7. Za okablowanie oraz administrowanie siecią lokalną w budynku CINIBA odpowiedzialna jest Oddział Obsługi Informatycznej Bibliotek.
8. Jeśli jest to merytorycznie uzasadnione, za zgodą Dyrektora ds. Informatyzacji wydzielone w danym segmencie obszary sieci mogą być administrowane przez inne jednostki niż wskazano w niniejszym Regulaminie.
9. Sieci wykorzystywane przez podmioty wynajmujące pomieszczenia na podstawie umowy traktowane są jako sieci zewnętrzne w stosunku do USK. Sieci takie muszą posiadać własne regulaminy. Podmiot wynajmujący pełni rolę administratora sieci.

## §3

### Sieci bezprzewodowe

1. W Uniwersytecie Śląskim w Katowicach udostępniona jest członkom społeczności akademickiej sieć bezprzewodowa eduroam realizowana zgodnie z regulaminem tej usługi.
2. Za administrację siecią eduroam odpowiedzialny jest Dział Administracji Sieci i Usług Sieciowych.
3. Za instalację punktów dostępowych sieci bezprzewodowej w segmentach sieci odpowiedzialne są jednostki administrujące danym segmentem sieci.

4. Dopuszczalne jest tworzenie lokalnych sieci bezprzewodowych przez Dział Administracji Sieci i Usług Sieciowych oraz jednostki odpowiedzialne za administrowanie danym segmentem sieci. Utworzenie lokalnej sieci bezprzewodowej musi być zgłoszone oraz uzgodnione z Działem Administracji Sieci i Usług Sieciowych. Lokalne sieci bezprzewodowe muszą mieć określony regulamin funkcjonowania.
5. Lokalne sieci bezprzewodowe oraz rozgłaszające je urządzenia muszą przez cały okres eksploatacji pozostawać zabezpieczone przed nieuprawnionym dostępem na poziomie określonym w regulaminie usługi odpowiadającym aktualnym standardom bezpieczeństwa.
6. Dział Administracji Sieci i Usług Sieciowych prowadzi rejestr lokalnych sieci bezprzewodowych.
7. Nie jest dopuszczalne uruchamianie w ramach USK innych sieci bezprzewodowych niż wskazane w tym paragrafie.

#### §4

##### Finansowanie

1. Bieżące utrzymanie USK finansowane jest ze środków ogólnouczelnianych znajdujących się w dyspozycji Dyrektora ds. Informatyzacji.
2. Modernizacja sieci może być finansowana z innych środków niż wskazano w ust. 1.
3. W przypadku budowy, remontu, modernizacji budynków należy uwzględniać w budżecie koszty prac związanych z siecią komputerową.
4. Do dnia 30 listopada każdego roku jednostki Pionu IT odpowiedzialne za utrzymanie sieci przygotowują kosztorys utrzymania i modernizacji sieci w roku następnym. Po zatwierdzeniu planu przez Prorektora ds. Nauki i Finansów zostaje on uwzględniony w Planie Zamówień Publicznych oraz Planie Rzeczowo Finansowym.
5. W przypadku zajścia okoliczności mających wpływ na zmianę planu, właściwe jednostki Pionu IT przedstawiają Prorektorowi ds. Nauki i Finansów korektę planu za pośrednictwem Dyrektora ds. Informatyzacji.

#### §5

##### Domena Uniwersytetu

1. Domeną internetową Uniwersytetu Śląskiego w Katowicach jest us.edu.pl.
2. Oficjalne strony internetowe oraz usługi sieciowe są adresowane poprzez tę domenę.
3. Serwery nazw utrzymywane są przez Dział Administracji Sieci i Usług Sieciowych.
4. W uzasadnionych wypadkach Dyktor ds. Informatyzacji może wyrazić zgodę na funkcjonowanie dla poddomeny us.edu.pl dodatkowego serwera nazw

administrowanego przez inną jednostkę niż Dział Administracji Sieci i Usług Sieciowych.

5. Prawo wnioskowania o rejestrację nazwy w domenie internetowej Uniwersytetu Śląskiego w Katowicach mają: rektor, prorektorzy, kanclerz, zastępcy kanclerza, dyrektor ds. Informatyzacji, dziekani, kierownicy jednostek ogólnouczelnianych, oraz pracownicy Pionu Dyrektora ds. Informatyzacji.
6. Za rejestrację domeny odpowiedzialny jest Dział Administracji Sieci i Usług Sieciowych. Każda zarejestrowana domena musi mieć opiekuna. Opiekuna wskazuje wnioskodawca.
7. Domeny inne niż us.edu.pl wykorzystywane przez jednostki Uniwersytetu Śląskiego należy rejestrować za pośrednictwem Działu Administracji Sieci i Usług Sieciowych. Prawo do rejestrowania takiej domeny mają: rektor, prorektorzy, kanclerz, zastępcy kanclerza, dziekani i kierownicy jednostek ogólnouczelnianych. Wniosek o rejestrację należy kierować do Działu Administracji Sieci i Usług Sieciowych. We wniosku należy wskazać opiekuna domeny oraz źródło finansowania domeny.

## §6

### Systemy informatyczne

1. Uniwersytet utrzymuje systemy informatyczne w USK lub w domenie Uniwersytetu.
2. Systemem informatycznym nazywamy dowolne oprogramowanie uruchomione w USK na urządzeniach komputerowych służące przetwarzaniu danych z wykorzystaniem sieci komputerowej, udostępniające użytkownikom USK usługi informatyczne. Systemem informatycznym będą zarówno systemy dziedziczne takie jak USOS lub SAP, jak również serwisy WWW.
3. Dla każdego systemu informatycznego:
  - 1) musi być określona jednostka odpowiedzialna merytorycznie za cele funkcjonowania oraz za zapewnienie finansowania funkcjonowania systemu informatycznego w całym okresie jego funkcjonowania;
  - 2) musi być wskazana co najmniej jedna osoba pełniąca rolę administratora systemu informatycznego;
  - 3) musi być wskazana co najmniej jedna osoba odpowiedzialna za nadawanie uprawnień w danym systemie informatycznym;
  - 4) musi być wskazane źródło finansowania utrzymania danego systemu informatycznego;
  - 5) muszą być wskazane zasoby fizyczne, w oparciu o które będzie utrzymywany dany system informatyczny;
  - 6) musi być określony regulamin funkcjonowania systemu informatycznego określający co najmniej: cel funkcjonowania systemu, jednostkę odpowiedzialną merytorycznie za system informatyczny, zasady

tworzenia, usuwania i modyfikowania kont oraz uprawnień użytkowników, sposób zarządzania danymi.

4. Rolę administratora systemu informatycznego może pełnić podmiot zewnętrzny w stosunku do Uniwersytetu, z którym Uniwersytet zawrze umowę na świadczenie tego typu usług.
5. Jeżeli w systemie administrowanym przez podmiot zewnętrzny, będą przetwarzane dane osobowe dla których administratorem jest Uniwersytet, należy zawrzeć z podmiotem świadczącym usługę stosowną umowę powierzenia przetwarzania danych osobowych.
6. Do zadań administratora systemu informatycznego należy bieżąca obsługa systemu, wykonywanie kopii bezpieczeństwa, aktualizacji oprogramowania systemu informatycznego, zmiana konfiguracji w zależności od potrzeb, zabezpieczenie systemu informatycznego, analiza incydentów bezpieczeństwa.
7. Prawo do wnioskowanie o uruchomienie systemu informatycznego mają: rektor, prorektorzy, kanclerz, zastępcy kanclerza, Dyrektor ds. Informatyzacji, dziekani i kierownicy jednostek ogólnouczelnianych.
8. Planując uruchomienie systemu informatycznego jednostka merytorycznie odpowiedzialna za funkcjonowanie systemu zobowiązana jest do dokonania udokumentowanej analizy obejmującej cały przewidywany okres funkcjonowania systemu informatycznego, która uwzględni:
  - 1) koszty pozyskania i wdrożenia systemu informatycznego;
  - 2) koszty aktualizacji i modernizacji;
  - 3) koszty administracji systemem;
  - 4) koszty infrastruktury informatycznej niezbędnej do funkcjonowania systemu informatycznego;
  - 5) zakres przetwarzanych danych, w tym danych osobowych;
  - 6) źródła finansowania systemu informatycznego w całym przewidywanym okresie funkcjonowania;
  - 7) ryzyka związane z funkcjonowaniem systemu informatycznego;
  - 8) ocenę ryzyka i stopnia bezpieczeństwa danych osobowych w przypadku ich przetwarzania w systemie.
9. Wprowadza się rejestr systemów informatycznych. Rejestr utrzymywany jest przez Dział Administracji Sieci i Usług Sieciowych.
10. Do rejestru nie wprowadza się telefonów komórkowych oraz komputerów osobistych, o ile nie są w nich uruchomione usługi sieciowe inne niż standardowo udostępnione z systemem operacyjnym w ramach standardowej konfiguracji.
11. Rejestr systemów informatycznych zawiera co najmniej następujące informacje:
  - 1) nazwę systemu;
  - 2) datę uruchomienia systemu;
  - 3) datę wyłączenia systemu (zaprzestania funkcjonowania) - dotyczy systemów wyłączonych z eksploatacji;
  - 4) jednostkę merytorycznie odpowiedzialną za cele funkcjonowania oraz finansowanie systemu informatycznego;

- 5) informację o projektach mających wpływ na finansowanie lub funkcjonowanie systemu informatycznego;
  - 6) administratorów systemu informatycznego;
  - 7) osoby odpowiedzialne za nadawanie uprawnień w systemie;
  - 8) adresy sieciowe oraz nazwy domenowe wykorzystywane przez system informatyczny;
  - 9) opis uprawnień w systemie informatycznym;
  - 10) wskazanie miejsca przechowywania dokumentacji konfiguracji oraz procedur związanych z funkcjonowaniem systemu informatycznego.
12. Dyrektor ds. Informatyzacji ma prawo rozszerzać zakres danych przetwarzanych w rejestrze.
  13. Kierownik jednostki merytorycznie odpowiedzialnej za cele funkcjonowania systemu informatycznego ma obowiązek niezwłocznie informować Dział Administracji Sieci i Usług sieciowych o wszelkich zmianach mających wpływ na rejestr systemów informatycznych.
  14. System Informatyczny nie może zostać publicznie udostępniony przed rejestracją w rejestrze systemów informatycznych.

## §7

### Tożsamość elektroniczna

1. Tożsamością elektroniczną nazywamy konto użytkownika wraz z zakresem uprawnień w systemie informatycznym utrzymywanym przez Uniwersytet Śląski w Katowicach.
2. Tożsamość może być przypisana do określonej osoby lub dotyczyć konta technicznego wykorzystywanego przez system informatyczny.
3. Tworzenie tożsamości elektronicznej dla poszczególnych systemów informatycznych określone jest w regulaminie funkcjonowania tych systemów.
4. Tożsamości elektroniczne mogą być tworzone:
  - 1) automatycznie na podstawie innych tożsamości elektronicznych lub roli osoby w organizacji;
  - 2) na wniosek.
5. Tworzenie tożsamości na wniosek należy udokumentować w rejestrze systemów informatycznych lub w inny sposób opisany w regulaminie funkcjonowania systemu informatycznego.
6. Tożsamości elektroniczne muszą być blokowane lub usuwane zgodnie z regulaminem funkcjonowania systemu informatycznego, tak aby minimalizować ryzyko dostępu do systemu informatycznego przez podmiot niemający do tego prawa.
7. Wnioskowanie o utworzenie tożsamości elektronicznej odbywa się zgodnie z zasadami wskazanymi w regulaminie systemu Informatycznego.

## Administratorzy sieci

1. Administratorem USK jest kierownik Działu Administracji Sieci i Usług Sieciowych.
2. Administrator USK odpowiedzialny jest za:
  - 1) podział adresacji sieci;
  - 2) ustalenie routingu pomiędzy segmentami sieci;
  - 3) zabezpieczenie USK na styku z operatorem,
  - 4) nadzór nad funkcjonowaniem sieci;
  - 5) określanie standardów sieci. Standardy określają wymagania:
    - a) w stosunku do urządzeń sieciowych oraz ich konfiguracji,
    - b) w stosunku do okablowania strukturalnego,
    - c) w stosunku do projektowania sieci oraz prowadzenia prac modernizacyjnych w zakresie sieci komputerowych,
  - 6) reprezentowanie Uniwersytetu wobec dostawców Internetu.
3. Administrator USK dokonuje do dnia 31 października każdego roku przeglądu standardów sieci za pomocą zespołu pracowników Pionu IT wskazanych na wniosek Administratora USK przez Dyrektora ds. Informatyzacji. Administrator USK publikuje do dnia 31 października standardy sieci.
4. Standardy sieci publikowane są na stronie internetowej <https://us.edu.pl/it/standardy-sieci>
5. Rolę administratorów sieci dla poszczególnych segmentów sieci pełnią kierownicy jednostek odpowiedzialnych za funkcjonowanie danego segmentu sieci oraz wskazani przez nich pracownicy.
6. Aktualną listę administratorów poszczególnych segmentów sieci przechowuje Dział Administracji Sieci i Usług Sieciowych. Kierownicy jednostek odpowiedzialnych za funkcjonowanie danych segmentów sieci zobowiązani są niezwłocznie informować Dział Administracji Sieci i Usług Sieciowych o wszelkich zmianach mających wpływ na listę administratorów sieci.
7. Tylko administratorzy sieci mają prawo konfiguracji urządzeń sieciowych.
8. Administratorzy mają obowiązek zarządzać podległym sobie segmentem sieci zgodnie z wytycznymi administratora USK.
9. Administratorzy sieci mają prawo odłączyć urządzenie komputerowe od sieci, gdy:
  - 1) konfiguracja urządzenia destabilizuje pracę sieci;
  - 2) konfiguracja powoduje ryzyko dla bezpieczeństwa sieci;
  - 3) doszło do incydentu bezpieczeństwa teleinformatycznego;
  - 4) działania użytkownika sieci są niezgodne z prawem lub wykraczają poza dopuszczalny zakres wykorzystania sieci;
  - 5) na wniosek administratora systemu informatycznego, w sytuacji, gdy użytkownik wykonał działania niezgodne z zasadami funkcjonowania systemu informatycznego.

10. Administratorzy sieci mają prawo i obowiązek dokonywać w obrębie zarządzanego przez nich segmentu sieci analizy sieci oraz poszukiwać luk bezpieczeństwa sieci. Administratorzy sieci mają prawo w podległym im segmencie sieci wykonywać testy penetracyjne po wcześniejszym uzgodnieniu z jednostkami odpowiedzialnymi merytorycznie za funkcjonujące w danym segmencie sieci systemy informatyczne.

## §9

### Użytkownicy

1. Użytkownikiem USK jest każda osoba korzystająca z urządzenia podłączonego do USK, niezależnie od jego lokalizacji.
2. Użytkownikiem USK jest również każda osoba korzystająca z USK za pośrednictwem systemów informatycznych funkcjonujących w USK.
3. Użytkownicy mają obowiązek stosowania się do regulaminu sieci oraz zasad funkcjonowania systemów informatycznych z których korzystają, a które funkcjonują w USK.
4. Administratorzy sieci oraz administratorzy systemów informatycznych nie ponoszą odpowiedzialności za działania użytkowników sieci i systemów informatycznych niezgodne z prawem, niezgodne z regulaminem sieci lub z zasadami funkcjonowania systemów informatycznych.
5. Użytkownicy USK nie mają prawa wykonywać działań mających na celu przełamanie zabezpieczeń udostępnionego im połączenia sieciowego lub systemu informatycznego.
6. Użytkownicy mają obowiązek wykorzystywać połączenie sieciowe oraz udostępnione im systemu informatyczne w sposób zgodny z ich przeznaczeniem.
7. Użytkownicy USK nie mają prawa udostępnić danych służących autoryzacji innym osobom.
8. Zasady funkcjonowania systemów informatycznych przez użytkowników są określone niezależnie dla każdego systemu informatycznego.
9. Możliwość podłączenia się użytkowników do USK jest określona niezależnie dla poszczególnych segmentów sieci.
10. Konta w systemach informatycznych tworzy się zgodnie z przyjętymi zasadami funkcjonowania danego systemu informatycznego.

## §10

### Bezpieczeństwo sieci komputerowej i usług sieciowych

1. Standardy zarządzania systemami informatycznymi, standardy bezpieczeństwa systemów informatycznych oraz standardy bezpieczeństwa sieci komputerowych określone są przez zespół powołany przez Dyrektora ds. Informatyzacji.
2. Przegląd standardów następuje każdego roku do dnia 30 listopada.



3. Standardy publikowane są na stronie internetowej o adresie <https://us.edu.pl/it/standardy-bezpieczenstwa-sieci>

## §11

### Incydenty bezpieczeństwa

1. Użytkownicy USK mają obowiązek zgłaszać wszelkie nieprawidłowości w funkcjonowaniu USK, w tym również incydenty bezpieczeństwa.
2. Zgłoszenia należy dokonywać u właściwych administratorów sieci lub w Dziale Administracji Sieci i Usług Sieciowych za pomocą kanałów komunikacji wskazanych na stronie internetowej <https://us.edu.pl/it/incydenty-bezpieczenstwa>
3. Zgłaszając incydent należy podać swoje dane, system informatyczny lub segment sieci którego dotyczy zgłoszenie oraz dokładnie opisać zaistniałą sytuację.
4. Administrator sieci oraz Dział Administracji Sieci i Usług Sieciowych przekazują informacje o zgłoszeniu do właściwego administratora sieci lub administratora systemu informatycznego, jeśli nie stanowią właściwych adresatów danego zgłoszenia. O ile zachodzi ryzyko związane z naruszeniem praw i wolności w zakresie danych osobowych, to informacja o incydencie przekazywana jest do Inspektora Ochrony Danych oraz Dyrektora ds. Informatyzacji.

## §12

### Elektroniczne rozpatrywanie wniosków

Ustala się, iż wszelkie wnioski, o których mowa w niniejszym regulaminie są rozpatrywane drogą elektroniczną. Format wniosku oraz sposób komunikacji określają jednostki odpowiedzialne za realizację wniosków.