Załącznik
do Zarządzenia nr 64/2025 Rektora ANS w Lesznie z dnia 26 listopada 2025 r.

Regulamin korzystania z infrastruktury informatycznej Akademii Nauk Stosowanych im. Jana Amosa Komeńskiego w Lesznie

Spis treści

1. Postanowienia ogólne

1.1 Cel i zakres

Niniejszy regulamin określa zasady korzystania z infrastruktury informatycznej Akademii Nauk Stosowanych im. Jana Amosa Komeńskiego w Lesznie (dalej zwanej “Uczelnią” lub „ANS”) oraz udostępnianych systemów i usług IT w szczególności:

- Systemu zarządzania tokiem studiów oraz obsługi procesów administracyjnych i dydaktycznych (USOS)

- Usług Microsoft Office 365 (dalej zwanych “usługami chmurowymi”)
- Sieci komputerowej ANS
- Stanowisk pracy i urządzeń dostarczonych przez Uczelnię
- Pozostałych zasobów informatycznych Uczelni

1.2 Zastosowanie

Regulamin stosuje się do wszystkich użytkowników infrastruktury informatycznej Uczelni, w tym:

- Pracowników Uczelni
- Studentów
- Gości i pracowników tymczasowych
- Użytkowników zdalnych

1.3 Zgodność z przepisami prawa

Korzystanie z infrastruktury informatycznej Uczelni podlega:

- Ustawie o ochronie danych osobowych (UODO)
- Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO)
- Ustawie o krajowych ramach interoperacyjności (KRI)
- Przepisom prawa karnego dotyczącym mienia i tajemnicy
- Wytycznym bezpieczeństwa Ministerstwa Cyfryzacji
- Polityce bezpieczeństwa informacji Uczelni
- Polityce bezpieczeństwa danych osobowych Uczelni

2. Definicje

2.1 Pojęcia podstawowe

Infrastruktura informatyczna Uczelni - zespół systemów, urządzeń, oprogramowania, zasobów sieciowych i danych należących do Uczelni lub przez nią administrowanych.

Konto użytkownika - unikalna tożsamość przydzielona pracownikowi lub studentowi, umożliwiająca dostęp do systemów informatycznych Uczelni.

System USOS - Uniwersytecki System Obsługi Studiów, centralny system informatyczny Uczelni służący do zarządzania procesami dydaktycznymi, zarządzania personelem i obsługą finansową.

Microsoft Office 365 - zestaw usług chmurowych firmy Microsoft, obejmujący Exchange Online (poczta elektroniczna), SharePoint Online (dokumentacja i kolaboracja), Teams (komunikacja), OneDrive (magazyn danych) oraz pozostałe aplikacje.

Dane osobowe - wszelkie informacje dotyczące ustalonej lub możliwej do ustalenia osoby fizycznej.

Dane uczelni - wszelkie informacje i dokumenty będące własnością Uczelni lub przetwarzane w imieniu Uczelni.

Stanowisko pracy - komputer lub terminal z dostępem do infrastruktury Uczelni.

Dostęp zdalny - możliwość połączenia się z zasobami informatycznymi Uczelni spoza sieci lokalnej.

3. Zakresy odpowiedzialności

3.1 Odpowiedzialność Uczelni

Uczelnia zobowiązana jest do:

- Zapewnienia bezpiecznego i niezawodnego działania infrastruktury informatycznej
- Implementacji odpowiednich mechanizmów bezpieczeństwa
- Ochrony danych osobowych użytkowników
- Regularnego przeprowadzania audytów bezpieczeństwa
- Szkolenia użytkowników w zakresie bezpiecznego korzystania z systemów
- Posiadania planu ciągłości działania i odtwarzania danych
- Utrzymywania dokumentacji systemowej i logów dostępu
- Informowania użytkowników o incydentach bezpieczeństwa

3.2 Odpowiedzialność użytkownika

Każdy użytkownik infrastruktury informatycznej zobowiązany jest do:

- Ochrony danych dostępu do swojego konta
- Natychmiastowego zgłaszania podejrzeń naruszenia bezpieczeństwa
- Przestrzegania wszystkich zasad zawartych w niniejszym regulaminie
- Korzystania z zasobów zgodnie z celem ich przeznaczenia
- Przechowywania poufnych informacji zgodnie z obowiązującymi wytycznymi
- Niezwłocznej zmiany hasła w przypadku jego ujawnienia
- Wylogowania się z systemu po zakończeniu sesji

4. Konta użytkowników

4.1 Przydzielanie kont

Konta zostają przydzielone automatycznie dla studentów w momencie immatrykulacji. Konta dla pracowników przydzielane są przez Dział IT w dniu rozpoczęcia pracy.

4.2 Struktura identyfikatora użytkownika

Identyfikatory użytkowników mają postać:

- Dla pracowników: imie.nazwisko@ansleszno.pl lub unikalny identyfikator
- Dla studentów: nr-indeksu@student.ansleszno.pl

4.3 Prawo dostępu

Dostęp do określonych systemów i zasobów przydzielany jest na podstawie:

- Stanowiska pracy
- Roli pełnionej w Uczelni
- Funkcji dydaktycznych i naukowych
- Wymagań procesów biznesowych
- Zasady najmniejszych uprawnień

Każdy użytkownik ma dostęp jedynie do zasobów niezbędnych do realizacji swoich obowiązków.

4.4 Dezaktywacja i usuwanie kont

Konto użytkownika zostaje dezaktywowane w następujących przypadkach:

- Rezygnacji z pracy lub ukończenia studiów
- Bezpłatnego urlopu lub zawieszenia prawa do nauki
- Naruszenia warunków niniejszego regulaminu
- Nieaktywności przez okres 12 miesięcy (dla kont studenckich)
- Decyzji administracyjnej Rektora

5. System USOS

5.1 Przeznaczenie systemu

System USOS jest dedykowanym narzędziem do:

- Obsługi toku studiów wszystkich stopni i rodzajów (zajęcia, oceny, protokoły, wznowienia)

- Zarządzania programami studiów i zapisami na zajęcia
- Składania podań i wniosków (np. o pomoc socjalną)
- Elektronicznej archiwizacji prac dyplomowych i obsługi egzaminów
- Obsługi stypendiów i akademików
- Zarządzania płatnościami za usługi edukacyjne
- Organizacji praktyk zawodowych studentów
- Przeprowadzania ankiet i sprawozdawczość
- Obsługi spraw pracowniczych (zatrudnienia, pensum itp.)
- Komunikacji studentów i wykładowców w grupach zajęciowych
- Dostępu do mLegitymacji i integracja z systemem mObywatel
- Zdalnego dostępu do usług dla kandydatów, studentów i wykładowców
- Wymiany danych z uczelniami partnerskimi w systemie Erasmus

5.2 Dostęp do systemu USOS

Dla studentów:

- Dostęp osobisty do swoich danych (oceny, plan zajęć, rejestracja)
- Przeglądanie ogólnodostępnych informacji o ofercie edukacyjnej
- Dostęp do funkcji samoobsługowych określonych w systemie

Dla pracowników dydaktycznych:

- Dostęp do list studentów na przedmiotach
- Wpisywanie ocen i obecności
- Dostęp do materiałów do prowadzenia zajęć
- Dostęp do informacji o kierunkach i specjalizacjach
- Możliwość kontaktu z władzami Uczelni

Dla pracowników administracyjnych:

- Dostęp ograniczony do funkcji niezbędnych do pełnienia obowiązków
- Dostęp do danych do rozrachunków finansowych (dla pracowników finansów)
- Dostęp do danych osobowych pracowników (dla kadr)
- Rozbudowanie raportowanie

Dla kierownictwa:

- Dostęp do raportów i analiz
- Dostęp do agregowanych danych
- Dostęp do procedur zatwierdzania

5.3 Ochrona danych w systemie USOS

System USOS zabezpiecza dane i funkcjonowanie poprzez następujące środki techniczne:

- Ograniczenie dostępności danych i szyfrowanie połączeń sieciowych, co zapewnia ochronę przesyłanych informacji przed nieuprawnionym dostępem
- System ról i uprawnień użytkowników, które precyzyjnie kontrolują kto i w jakim zakresie może korzystać z danych i funkcji systemu
- Tworzenie regularnych kopii bezpieczeństwa (backupów) bazy danych, co umożliwia odtworzenie informacji po awariach lub incydentach bezpieczeństwa
- Dziennik zmian w systemie (logowanie operacji), co pozwala na audyt i monitorowanie działań podejmowanych przez użytkowników systemu
- Uwierzytelnianie i autoryzacja użytkowników przy pomocy usług stowarzyszonych (CAS), podnosząc poziom kontroli dostępu
- Wykorzystanie podpisów elektronicznych i kart kryptograficznych do zabezpieczenia dokumentów i potwierdzenia tożsamości
- System modularny z jasno określonymi uprawnieniami poszczególnych modułów oraz centralną bazą danych, co zwiększa kontrolę i bezpieczeństwo

6. Microsoft Office 365

6.1 Usługi wchodzące w skład pakietu

Microsoft Office 365 dostępny dla użytkowników Uczelni obejmuje:

Exchange Online - system poczty elektronicznej:

- Konto e-mail w domenie uczelni
- Skrzynka pocztowa o pojemności 50 GB
- Możliwość założenia list dystrybucyjnych dla zespołów

SharePoint Online - platforma do wspólnej pracy nad dokumentami:

- Biblioteki dokumentów dla zespołów
- Witryny zespołowe
- Zarządzanie wersjonowaniem dokumentów
- Funkcjonalność wyszukiwania
- Możliwości współpracy w czasie rzeczywistym

Microsoft Teams - narzędzie komunikacji:

- Czaty zespołowe
- Wideokonferencje

- Udostępnianie ekranu
- Integracja z aplikacjami Office

OneDrive - magazyn danych w chmurze:

- 1 TB przestrzeni dla każdego użytkownika
- Synchronizacja plików na urządzeniach
- Udostępnianie dokumentów

Aplikacje Office Online - wersje internetowe oraz desktopowe:

- Word, Excel, PowerPoint, OneNote

Dodatkowe usługi:

- Stream (udostępnianie filmów wideo)
- Forms (tworzenie ankiet i formularzy)
- Planner (zarządzanie projektami)
- Power Automate (automatyzacja procesów)

6.2 Zasady korzystania z poczty elektronicznej

Akceptowalny użytek:

- Korespondencja służbowa
- Wymiana informacji dotyczącej działalności Uczelni
- Komunikacja z pracownikami, studentami i partnerami zewnętrznymi
- Przesyłanie materiałów edukacyjnych

Niedopuszczalny użytek:

- Wysyłanie spamu lub wiadomości zbiorowych bez uzasadnienia
- Rozpowszechnianie pornografii, materiałów zawierających nienawiść lub przemoc
- Nękanie, dokuczanie, molestowanie, mobbing lub inne formy zastraszania
- Rozpowszechnianie złośliwego oprogramowania (malware, wirus, ransomware)
- Udzielanie dostępu do konta osobom trzecim
- Automatyczne przeniesienie korespondencji na konto zewnętrzne

6.3 Zarządzanie wiadomościami

- Konto jest własnością Uczelni, a pracownicy Działu IT mogą przeglądać wiadomości w celach dostępu awaryjnego lub śledztwa

- Użytkownik nie może usunąć wiadomości trwale - mogą być odzyskane z archiwum
- Wiadomości zawierające dane osobowe muszą być szyfrowane

6.4 SharePoint i wspólna praca nad dokumentami

Przeznaczenie:

- Współpraca nad dokumentami z innymi użytkownikami
- Przechowywanie dokumentów zespołowych
- Dokumentowanie procesów i procedur
- Udostępnianie materiałów dydaktycznych

Zasady bezpieczeństwa:

- Dokumenty zawierające dane osobowe muszą być przechowywane w zabezpieczonych lokalizacjach
- Udostępnianie dokumentów osobom spoza Uczelni wymaga zgody kierownika/przełożonego
- Nazwa dokumentu powinna jasno wskazywać na jego zawartość i poziom poufności

6.5 Microsoft Teams

Akceptowalny użytek:

- Komunikacja zespołowa
- Spotkania i zajęcia online
- Wymiana dokumentów
- Planowanie projektów

Zasady kanałów Teams:

- Kanały powinny być tworzone dla konkretnych projektów lub zespołów
- Każdy kanał powinien mieć właściciela z wyznaczoną odpowiedzialnością
- Zabrania się tworzenia kanałów publicznych zawierających dane osobowe
- Nagrania spotkań przechowywane są domyślnie przez 120 dni po czym automatycznie wygasają i są usuwane.
- Członkowie zespołu powinni być dodawani tylko jeśli mają dostęp do zasobów zespołu

6.6 OneDrive

- OneDrive przeznaczony jest do przechowywania dokumentów osobistych użytkownika
- Dokumenty mogą być synchronizowane z urządzeniami lokalnymi
- Udostępnianie plików wymaga jawnej zgody poprzez ustawienia dostępu
- Zabrania się przechowywania w OneDrive danych szczególnie chronionych bez szyfrowania
- Aby uniknąć utraty dostępu - zawsze należy posiadać lokalną kopię ważnych dokumentów

7. Bezpieczeństwo infrastruktury

7.1 Wymagania dotyczące haseł

Polityka haseł:

- Hasła muszą mieć minimum 14 znaków
- Hasła muszą zawierać: wielkie litery, małe litery, cyfry i znaki specjalne
- Hasła nie mogą zawierać imienia lub nazwiska użytkownika
- Hasła nie mogą być słowami dostępnymi w słowniku
- Hasła muszą być zmieniane natychmiast po jego ujawnieniu
- Historia haseł musi obejmować ostatnich 5 haseł
- Błędna próba zalogowania przez 7 razy skutkuje blokowaniem konta - na 10 minut lub do czasu odblokowania przez administratora - w przypadku systemów które mają taką funkcjonalność.
- Zabrania się zapisywania haseł w widocznym miejscu

Polityka haseł nie dotyczy komputerów dostępnych na salach wykładowych i laboratoriach ANS, służących do prezentowania materiałów dydaktycznych.

Ochrona haseł:

- Każdy użytkownik jest odpowiedzialny za ochronę swojego hasła
- Hasło nigdy nie powinno być dzielone z inną osobą, również z pracownikami Działu IT
- Zabrania się wysyłania hasła drogą elektroniczną w postaci niezaszyfrowanej

7.2 Uwierzytelnianie wieloskładnikowe (MFA)

- Usługi Microsoft Office 365 obowiązkowo wymagają stosowania uwierzytelniania wieloskładnikowego (MFA)
- MFA wymaga posiadania drugiego czynnika (np. aplikacja Authenticator, SMS, token, klucz sprzętowy)
- Użytkownik jest odpowiedzialny za przechowywanie kodów zapasowych
- Kody zapasowe muszą być przechowywane w bezpiecznym miejscu

7.3 Urządzenia końcowe

Wymagania dla urządzeń Uczelni:

- Wszystkie urządzenia muszą posiadać zainstalowany system operacyjny wspierany przez producenta
- Obowiązkowa jest instalacja i regularna aktualizacja oprogramowania antywirusowego
- Zabrania się dezaktywacji zapory sieciowej lub innych mechanizmów bezpieczeństwa
- Wszystkie urządzenia przenośne muszą być szyfrowane (BitLocker dla Windows, FileVault dla macOS)
- Automatyczne aktualizacje systemu operacyjnego muszą być włączone
- Zabrania się instalacji oprogramowania innego niż zatwierdzone przez Dział IT

Dla urządzeń prywatnych (BYOD - Bring Your Own Device):

- Urządzenie może być podłączone tylko do sieci dla gości lub ANS-FREE-WIFI
- Urządzenie musi spełniać minimalne wymagania bezpieczeństwa
- Ruch z i do takich urządzeń jest monitorowany i logowany a logi przechowywane przez okres 12 m-cy
- W razie naruszenia warunków - dostęp będzie wstrzymany
- Uczelnia nie odpowiada za kradzież lub uszkodzenie urządzenia prywatnego

7.4 Sieć bezprzewodowa

- Sieć WiFi Uczelni wymagają logowania za pomocą konta użytkownika lub certyfikatu
- Zabrania się tworzenia własnych punktów dostępowych WiFi o nazwach z których korzysta Uczelnia

7.5 VPN i dostęp zdalny

- Dostęp zdalny do zasobów Uczelni wymaga korzystania z autoryzowanego serwera VPN
- VPN jest dostępne dla pracowników oraz studentów Uczelni
- Zabrania się dzielenia się dostępem VPN
- Sesja VPN będzie rozłączona po 4 godzinach bezczynności

8. Zasady prywatności i ochrony danych

8.1 Przetwarzanie danych osobowych

Uczelnia przetwarza dane osobowe pracowników i studentów zgodnie z:

- RODO
- UODO
- Polityką bezpieczeństwa danych osobowych
- Polityką bezpieczeństwa informacji

Dane osobowe przetwarzane są wyłącznie w celach:

- Administracyjno-edukacyjnych
- Kadrowo-płacowych
- Bezpieczeństwa infrastruktury
- Zgodności z obowiązującymi przepisami
- Komunikacji

8.2 Prawa użytkownika w zakresie ochrony danych

Każdy użytkownik ma prawo do:

- Wglądu do swoich danych
- Sprostowania danych nieprawidłowych
- Usunięcia danych (prawo do bycia zapomnianym) w wypadkach określonych w RODO
- Ograniczenia przetwarzania
- Przenoszenia danych

Wnioski w tych sprawach należy kierować do Inspektora Ochrony Danych Uczelni.

8.3 Bezpieczeństwo danych

- Wszystkie dane w systemach Uczelni są przechowywane w centrach danych z zabezpieczeniami fizycznymi
- Dane są szyfrowane zarówno w trakcie transmisji jak i na serwerach
- Dostęp do danych jest rejestrowany w logach
- Regularne kopie zapasowe są wykonywane zgodnie z procedurą wykonywania kopii zapasowych
- Dane osobowe są przechowywane w zabezpieczonych lokalizacjach z ograniczonym dostępem

9. Dopuszczalne i niedopuszczalne zastosowania

9.1 Dopuszczalne zastosowanie

Infrastruktura informatyczna Uczelni może być używana do:

- Nauki i badań naukowych
- Dydaktyki
- Zarządzania administracyjnego Uczelni
- Komunikacji służbowej
- Realizacji projektów naukowych
- Działalności wspierającej misję Uczelni
- Zatwierdzonych inicjatyw edukacyjnych

9.2 Niedopuszczalne zastosowanie

Zabrania się używania infrastruktury informatycznej Uczelni do:

- Kopiowania, rozpowszechniania lub przechowywania materiałów naruszających prawa autorskie
- Rozpowszechniania pornografii, materiałów zawierających nienawiść, rasizm lub przemoc
- Zastraszania, nękania, mobbingu, cyberbullingu
- Działalności o charakterze seksualnym lub zastraszającym
- Rozpowszechniania wirusa, malware czy ransomware
- Obchodzenia systemów bezpieczeństwa i kontroli dostępu
- Nieuprawnionego dostępu do cudzych kont lub danych

- Kradzieży intelektualnej
- Działalności niezgodnej z prawem
- Ujawniania poufnych informacji Uczelni
- Konkurencyjnej działalności biznesowej
- Obchodzenia filtrów treści
- Handlowania lub szerzenia narkotyków
- Prowadzenia hazardu

9.3 Monitorowanie prawidłowości

- Uczelnia zastrzega sobie prawo do monitorowania użycia infrastruktury w celu:
    - Egzekwowania niniejszego regulaminu
    - Ochrony zasobów Uczelni
    - Identyfikacji zagrożeń bezpieczeństwa
    - Spełnienia wymogów prawnych
- Monitorowanie może obejmować:
    - Logi dostępu do systemów
    - Analiza ruchu sieciowego
    - Przegląd wiadomości e-mail
    - Sprawdzenie zawartości dysków
- Monitorowanie nie obejmuje:
    - Poczty elektronicznej w systemach prywatnych
    - Danych w służbowych aplikacjach wymogiem szyfrowania end-to-end
    - Treści przesyłanej poprzez autoryzowane kanały prywatne

10. Monitorowanie i dostęp do zasobów

10.1 Logi dostępu

- Wszystkie logowania do systemów są rejestrowane
- Logi zawierają: datę, godzinę, identyfikator użytkownika, szczegóły połączenia
- Logi przechowywane są przez okres co najmniej 90 dni
- Dostęp do logów ma wyłącznie Dział IT i kierownictwo Uczelni

10.2 Audyt bezpieczeństwa

- Regularne audyty bezpieczeństwa przeprowadzane są co najmniej raz w roku
- Audyty mogą być przeprowadzane przez zewnętrznych audytorów
- Wyniki audytów są przedmiotem działań naprawczych

10.3 Testowanie penetracyjne

- Testy bezpieczeństwa mogą być przeprowadzane na zasobach Uczelni
- Testy penetracyjne są planowane i koordynowane z Działem IT oraz Pełnomocnikiem Rektora ds. Cyberbezpieczeństwa
- Bez specjalnego zezwolenia zabrania się testowania na systemach produkcyjnych

11. Polityka haseł i uwierzytelniania

11.1 Resetowanie hasła

- Użytkownik może zmienić hasło samodzielnie poprzez portal samoobsługowy
- W przypadku utraty dostępu – należy skontaktować się z Działem IT
- Pracownicy Działu IT nigdy nie będą prosić użytkownika o podanie hasła
- Zabrania się uzewnętrzniania haseł drogą SMS czy telefonicznie (poza hasłami startowymi)

12. Procedury awaryjne i bezpieczeństwa

12.1 Raportowanie incydentów bezpieczeństwa

W przypadku podejrzenia incydentu bezpieczeństwa (np. kradzież konta, złośliwy dostęp, utrata danych):

- Natychmiast powiadom Dział IT
- E-mail: it@ansleszno.pl
- Telefon: +48 65 528 78 79
- Nie próbuj samodzielnie naprawiać incydentu
- Zbierz wszelkie dostępne informacje o incydencie
- Nie usuwaj dowodów/logów

12.2 Procedura odtwarzania danych

- Kopie zapasowe są wykonywane codziennie

- Dane mogą być odtworzone z kopii w ciągu 24 godzin
- Prace odtwarzania są wykonywane przez Dział IT
- Wniosek o odtworzenie danych musi być przedłożony kierownikowi Działu IT

12.3 Plan ciągłości działalności

- Uczelnia posiada plan ciągłości działalności
- Wszystkie systemy krytyczne posiadają redundancję
- Czas przywrócenia (RTO) wynosi max 1 dzień
- Cel punktu przywracania (RPO) wynosi max 24 godziny

12.4 Powiadomienie o naruszeniu

W przypadku naruszenia bezpieczeństwa danych:

- Użytkownik będzie niezwłocznie powiadomiony
- Powiadomienie będzie zawierać szczegóły incydentu
- Powiadomienie będzie zawierać zalecenia dla użytkownika
- Incydent będzie raportowany do Inspektora Ochrony Danych, jeśli wymaga tego prawo

13. Konsekwencje naruszenia regulaminu

13.1 Odpowiedzialność administratora

W przypadku naruszenia niniejszego regulaminu przez użytkownika:

- Pierwsze naruszenie: ostrzeżenie pisemne od kierownika Działu IT
- Drugie naruszenie: czasowe ograniczenie dostępu (do 7 dni)
- Trzecie naruszenie: czasowe wstrzymanie dostępu (do 30 dni)
- Poważne naruszenie: trwałe usunięcie dostępu

Poważne naruszenia obejmują:

- Dostęp do cudzych kont
- Rozpowszechnianie złośliwego oprogramowania
- Ujawnianie danych osobowych
- Działalność niezgodna z prawem
- Narażanie Uczelni na znaczne straty

13.2 Odpowiedzialność dyscyplinarna

Naruszenie niniejszego regulaminu może powodować:

- **Dla pracowników**: rozpatrzenie przez komisję dyscyplinarną Uczelni
- **Dla studentów**: rozpatrzenie przez komisję dyscyplinarną Uczelni, zawiadomienie Rektora, wszczęcie postępowania o skreślenie z listy studentów
- **Dla gości**: natychmiastowe wstrzymanie dostępu

13.3 Odpowiedzialność karna

Użytkownik może ponieść odpowiedzialność karną za:

- Kradzież wizerunku
- Nieautoryzowany dostęp do systemów komputerowych
- Rozpowszechnianie złośliwego oprogramowania
- Naruszenie prawa do prywatności
- Kradzież intelektualną
- Działalność niezgodną z prawem

14. Postanowienia przejściowe

14.1 Wejście w życie

Niniejszy regulamin wchodzi w życie z dniem podpisania przez Rektora. Wszyscy użytkownicy mają obowiązek zapoznać się z regulaminem w ciągu 14 dni od jego ogłoszenia.

14.2 Rozwiązywanie sporów

Spory wynikające z interpretacji regulaminu będą rozstrzygane przez kierownika Działu IT, Pełnomocnika Rektora ds. Cyberbezpieczeństwa oraz Inspektora Ochrony Danych

14.3 Modyfikacje regulaminu

Regulamin podlega przeglądu raz w roku lub w miarę zmian w infrastrukturze lub przepisach prawa. Zmiany regulaminu będą ogłaszane z wyprzedzeniem co najmniej 30 dni.

Dodatek A. Kontakty i zasoby

Dział IT:

- E-mail: it@ansleszno.pl
- Telefon: +48 65 525 01 02
- Godziny: pn-pt 7:00-15:00

Inspektor Ochrony Danych:

- E-mail: iodo@ansleszno.pl
- Telefon: +48 529 60 55

Przydatne zasoby:

- Dział IT: https://it.ansleszno.pl
- Strona główna Uczelni: https://ansleszno.pl
- System USOS – https://ususweb.ansleszno.pl
- System poczty elektronicznej – https://outlook.microsoft.com
- Microsoft Teams – https://teams.microsoft.com
- Microsoft Office 365 – https://office.com

Dodatek B. Lista regulaminów powiązanych

- Regulamin usługi dostępu do sieci Internet (ZR 49/2024)
- Regulamin korzystania z uczelnianej poczty elektronicznej oraz usługi OneDrive (ZR 38/2024)
- Regulamin pracowni informatycznej

Dodatek C. Checklist bezpieczeństwa dla nowych użytkowników

Po przydzieleniu konta:

- ☐ Zmień hasło na bezpieczne
- ☐ Włącz uwierzytelnianie wieloskładnikowe (MFA)
- ☐ Przejrzyj politykę ochrony danych
- ☐ Skonfiguruj podpis e-mail
- ☐ Zapoznaj się z aplikacjami Microsoft Office 365
- ☐ Przejdź szkolenie z bezpieczeństwa IT
- ☐ Upewnij się, że wiesz, jak raportować incydenty

Dodatek D. Najczęściej zadawane pytania (FAQ)

P: Czy mogę korzystać z Uczelnianych zasobów do celów prywatnych?

O: Nie. Infrastruktura Uczelni jest wyłącznie dla celów związanych z pracą i nauką.

P: Co zrobić, jeśli zapomnę hasła lub utracę dostęp do metody MFA?

O: Jeśli nie ustawiłeś dodatkowego zabezpieczenia konta, podejdź z dokumentem tożsamości do Działu IT.

P: Czy mogę przesłać poufne dokumenty e-mailem?

O: Lepiej przechowuj dokumenty w OneDrive i udostępnij je przez link na określony czas. Po tym czasie usuń poufne informacje z OneDrive. Jeśli musisz wysłać e-mailem - zaszyfruj wiadomość.

P: Czy moje e-maile są monitorowane?

O: Tak, ale wyłącznie w celu zapewnienia bezpieczeństwa i zgodności z przepisami.

P: Czy mogę zainstalować własne oprogramowanie?

O: Nie, chyba że uzyskasz uprawnienia od Działu IT.

P: Co jeśli na moim koncie zostaną złamane zabezpieczenia?

O: Natychmiast powiadom Dział IT. Zmień hasło i włącz MFA jeśli nie jest włączone.

P: Jak długo są przechowywane moje e-maile?

O: Minimum 2 lata po wyłączeniu konta.

P: Czy mogę wziąć z sobą pliki z systemu po odejściu?

O: Tylko osobiste dokumenty - pliki stanowiące własność Uczelni muszą pozostać w systemach.

Data dokumentu: 16.11.2025

Wersja dokumentu: 1.0