Zarządzenie Nr 142/2019 Rektora Uniwersytetu Wrocławskiego z dnia 19 listopada 2019 r. w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego z uwzględnieniem zmian wprowadzonych:

1) Zarządzeniem Nr 31/2020 Rektora Uniwersytetu Wrocławskiego z dnia 20 marca 2020 r. w sprawie wprowadzenia Zasad użytkowania systemu TETA EDU w Uniwersytecie Wrocławskim;
2) zarządzeniem Nr 60/2020 Rektora Uniwersytetu Wrocławskiego z dnia 19 maja 2020 r. zmieniającym zarządzenie Nr 142/2019 Rektora Uniwersytetu Wrocławskiego z dnia 19 listopada 2019 r. w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego;
3) zarządzeniem Nr 127/2020 Rektora Uniwersytetu Wrocławskiego z dnia 28 września 2020 r. zmieniającym zarządzenie Nr 142/2019 Rektora Uniwersytetu Wrocławskiego z dnia 19 listopada 2019 r. w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej w Uniwersytecie Wrocławskim;
4) zarządzeniem Nr 48/2021 Rektora Uniwersytetu Wrocławskiego z dnia 13 kwietnia 2021 r. zmieniającym zarządzenie Nr 142/2019 Rektora Uniwersytetu Wrocławskiego z dnia 19 listopada 2019 r. w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego;
5) zarządzeniem Nr 86/2021 Rektora Uniwersytetu Wrocławskiego z dnia 9 czerwca 2021 r. zmieniającym zarządzenie Nr 142/2019 Rektora Uniwersytetu Wrocławskiego z dnia 19 listopada 2019 r. w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego;
6) zarządzeniem Nr 127/2022 Rektora Uniwersytetu Wrocławskiego z dnia 31 maja 2022 r. zmieniającym zarządzenie Nr 142/2019 Rektora Uniwersytetu Wrocławskiego z dnia 19 listopada 2019 r. w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego;
7) zarządzeniem Nr 23/2023 Rektora Uniwersytetu Wrocławskiego z dnia 2 lutego 2023 r. zmieniającym zarządzenie Nr 142/2019 Rektora Uniwersytetu Wrocławskiego z dnia 19 listopada 2019 r. w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego;
8) zarządzeniem Nr 24/2023 Rektora Uniwersytetu Wrocławskiego z dnia 3 lutego 2023 r. zmieniające zarządzenie Nr 142/2019 Rektora Uniwersytetu Wrocławskiego z dnia 19 listopada 2019 r. w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego;
9) zarządzeniem Nr 23/2024 Rektora Uniwersytetu Wrocławskiego z dnia 12 lutego 2024 r. zmieniające zarządzenie Nr 142/2019 Rektora Uniwersytetu Wrocławskiego z dnia 19 listopada 2019 r. w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego.

ZARZĄDZENIE Nr 142/2019
Rektora Uniwersytetu Wrocławskiego
z dnia 19 listopada 2019 r.

w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego

Na podstawie art. 23 ust. 1 i 2 ustawy z dnia 20 lipca 2018 r. - *Prawo o szkolnictwie wyższym i nauce* (Dz. U. z 2018 r., poz. 1668, z późniejszymi zmianami), w związku z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2019 r., poz. 1781) oraz Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 2016. Nr 119.1) oraz rozporządzeniem 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 (tekst jednolity: Dz. U. 2017 r., poz. 2247) zarządza się, co następuje:

§ 1.1. Wprowadza się Regulamin bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasady korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego, zwany dalej Regulaminem, który stanowi Załącznik do niniejszego zarządzenia.

2. Załącznikami do Regulaminu, o którym mowa w ust. 1 są:
   1/ Regulamin serwisów informacyjnych Uniwersytetu Wrocławskiego – Załącznik Nr 1,
   2/ Procedura stosowania oprogramowania antywirusowego oraz zapory sieciowej w Uniwersytecie Wrocławskim - Załącznik Nr 2,
   3/ Regulamin Uczelnianej Sieci Komputerowej Uniwersytetu Wrocławskiego - Załącznik Nr 3,
   4/ Regulamin Lokalnej Sieci Komputerowej Administracji Centralnej Uniwersytetu Wrocławskiego - Załącznik Nr 4,
   5/ Regulamin Korzystania z Usługi MS Office365 w Uniwersytecie Wrocławskim - Załącznik Nr 5,
   6/ Zasady tworzenia adresów poczty elektronicznej w Uniwersytecie Wrocławskim - Załącznik Nr 6,
   7/ Regulamin korzystania z systemu obsługi zgłoszeń informatycznych Logsystem - Załącznik Nr 7,
   8/ Zasady zgłaszania awarii sprzętu komputerowego i oprogramowania oraz przeprowadzania czynności serwisowych w jednostkach organizacyjnych administracji centralnej - Załącznik Nr 8,
   9/ Regulaminu bezpieczeństwa informatycznego dla urządzeń mobilnych w Uniwersytecie Wrocławskim - Załącznik Nr 9,
   10/ Zasady użytkowania systemu TETA EDU w Uniwersytecie Wrocławskim – Załącznik Nr 10,
   11/ Regulamin użytkowania systemu Huesca w Uniwersytecie Wrocławskim – Załącznik Nr 11,
   12/ Regulamin nadawania uprawnień użytkownikom systemu ARIS w Uniwersytecie Wrocławskim – Załącznik Nr 12,
   13/ Regulamin nadawania uprawnień użytkownikom systemu Omega PSIR w Uniwersytecie Wrocławskim – Załącznik Nr 13,
   14/ Regulamin nadawania uprawnień użytkownikom systemu EGERIA w Uniwersytecie Wrocławskim – Załącznik Nr 14,

15/Zasady użytkowania systemu Pulpity dla Kierowników Projektów w Uniwersytecie Wrocławskim – Załącznik Nr 15.

§ 2. Tracą moc:

1/ zarządzenie Nr 142/2017 Rektora Uniwersytetu Wrocławskiego z dnia 14 grudnia 2017 r. w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego;

2/ zarządzenie Nr 110/2018 Rektora Uniwersytetu Wrocławskiego z dnia 23 sierpnia 2018 r. w sprawie wprowadzenia zmiany do zarządzenia Nr 142/2017 Rektora Uniwersytetu Wrocławskiego z dnia 14 grudnia 2017 r. w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego;

3/ zarządzenie Nr 153/2018 Rektora Uniwersytetu Wrocławskiego z dnia 27 grudnia 2018 r. w sprawie wprowadzenia zmian do zarządzenia Nr 142/2017 Rektora Uniwersytetu Wrocławskiego z dnia 14 grudnia 2017 r. w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego.

§ 3. Nadzór nad wykonaniem niniejszego zarządzenia powierza się Dyrektorowi ds. informatycznych.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Adam Jezierski

prof. dr hab. Adam Jezierski
REKTOR

Załącznik
do zarządzenia Nr 142/2019
z dnia 19 listopada 2019 r.

Regulamin bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasady korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego

I. Postanowienia ogólne i definicje

§ 1.1 Celem niniejszego Regulaminu jest określenie zasad oraz działań dotyczących zarządzania bezpieczeństwem informacji przetwarzanych w systemach informatycznych w Uniwersytecie Wrocławskim oraz wskazanie zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego.

2. Stosowanie Regulaminu ma na celu uchronienie Uniwersytetu Wrocławskiego przed nieuprawnionym dostępem do użytkowanych systemów informatycznych oraz informacji udostępnianych z ich wykorzystaniem.

3. Regulamin wyznacza kierunki i zasady dotyczące zarządzania bezpieczeństwem informacji przetwarzanych w systemach informatycznych w Uniwersytecie Wrocławskim oraz ma za zadanie wprowadzenie dobrych praktyk korzystania z infrastruktury informatycznej Uczelni.

§ 2. Ilekroć w Regulaminie jest mowa o:

1) administratorze danych – rozumie się przez to Uniwersytet Wrocławski;
2) administratorze lokalnym – rozumie się przez to osobę zatrudnioną przez Uczelnię, upoważnioną i zobowiązaną do realizacji zadań związanych z zarządzaniem systemami informatycznymi w swojej lokalnej jednostce np. wydziale;
3) administratorze stacji roboczej – rozumie się przez to administratora lokalnego lub Użytkownika, któremu nadano uprawnienia administracyjne do danej stacji roboczej;
4) administratorze systemu informatycznego – rozumie się przez to osobę zatrudnioną przez Uczelnię, upoważnioną i zobowiązaną do realizacji zadań związanych z zarządzaniem systemem informatycznym, w szczególności nadającą uprawnienia do pracy w takim systemie;
5) danych osobowych – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
6) incydencie - rozumie się przez to zdarzenie zagrażające bezpieczeństwu informacji lub nieplanowaną przerwę w działaniu usługi informatycznej bądź znaczące obniżenie jakości usługi informatycznej;
7) kierowniku jednostki - rozumie się przez to Rektora, dziekanów, dyrektorów oraz kierowników jednostek organizacyjnych;
8) nośniku danych – rozumie się przez to przedmiot umożliwiający fizyczne zapisanie informacji w formie elektronicznej, z którego możliwe jest późniejsze odczytanie tej informacji (np. płyta CD, DVD, Blu-ray, pendrive);
9) przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, wykonywane w systemach informatycznych;
10) sieci lokalnej - rozumie się przez to fragment Uczelnianej Sieci Komputerowej UWr administrowanej przez odpowiednią jednostkę organizacyjną Uczelni;
11) sieci szkieletowej – rozumie się część sieci zapewniającą połączenia pomiędzy sieciami lokalnymi oraz sieciami zewnętrznych operatorów; sieć szkieletowa obejmuje serwery oraz infrastrukturę komunikacyjną przeznaczoną do świadczenia usług ogólnouczelnianych;

12) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych;
13) Uczelni – rozumie się przez to Uniwersytet Wrocławski;
14) Uczelnianej Sieci Komputerowej UWr (USK UWr) – rozumie się zbiór wszystkich sieci lokalnych poszczególnych jednostek oraz sieć szkieletową z zasobami;
15) Użytkowniku – rozumie się przez to osobę posiadającą uprawnienia do korzystania z danego systemu informatycznego;
16) Użytkowniku przetwarzającym dane osobowe – rozumie się przez to upoważnionego, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych;
17) wewnętrznych systemach informatycznych – rozumie się przez to: Zintegrowany System Kadrowo Płacowy (ZSKP), Zintegrowany System Informatyczny (ZSI), Uniwersytecki System Obsługi Studiów (USOS), Uniwersytecki System Obsługi Studiów Administracja (USOSadm), ARIS, Kaseya, ERA, Płatnik, do których mają dostęp, tylko dodatkowo uprawnieni pracownicy lub uprawnione podmioty zewnętrzne, z sieci Internet poprzez VPN;
18) VPN (ang. Virtual Private Network) - rozumie się przez to sieć zapewniającą bezpieczne połączenie pomiędzy klientem a serwerem, poprzez sieć publiczną;
19) zabezpieczeniu danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
20) zbiorze danych osobowych – rozumie się przez to każdy, posiadający strukturę, zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
21) zgodzie osoby, której te dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie – zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

§ 3.1. Regulamin określa zasady bezpieczeństwa w zakresie przetwarzania danych przez Użytkowników systemów informatycznych Uniwersytetu Wrocławskiego, a w szczególności przez:

1) wszystkich pracowników Uczelni, w tym kierowników jednostek, administratorów lokalnych, administratorów systemów informatycznych;
2) osoby świadczące usługi na rzecz Uniwersytetu Wrocławskiego na podstawie umów cywilnoprawnych;
3) studentów, doktorantów, słuchaczy oraz stażystów Uniwersytetu Wrocławskiego;
4) przedstawicieli podmiotów zewnętrznych, osoby współpracujące z Uniwersytetem Wrocławskim, którzy realizują pracę lub wykonują zadania na rzecz Uczelni;
5) uczestników konferencji, seminariów, itp.

2. Zobowiązanie do przestrzegania niniejszego Regulaminu dla osób, o których mowa w ust. 1 pkt 2 i 4 powinno wynikać z treści umów zawieranych z tymi osobami.

3. W przypadku nieprzestrzegania Regulaminu Użytkownik ponosi wszelkie konsekwencje wynikające ze swojego działania.

§ 4. Dane w Uniwersytecie Wrocławskim są chronione zgodnie z polskim prawem oraz wewnętrznymi procedurami dotyczącymi bezpieczeństwa i poufności przetwarzanych danych. Systemy informatyczne, które przetwarzają dane osobowe, są chronione odpowiednimi środkami technicznymi.

§ 5. Z Regulaminem obowiązkowo są zapoznawani wszyscy Użytkownicy systemów informatycznych. Nadzór nad procedurą zapoznania się z Regulaminem sprawują kierownicy jednostek.

§ 6. Regulamin określa odpowiedzialność za bezpieczeństwo informatyczne oraz wskazuje prawa i obowiązki w obszarach:

1) korzystania z systemów Uniwersytetu Wrocławskiego,
2) konfiguracji sprzętu komputerowego,
3) korzystania z Uczelnianej Sieci Komputerowej,
4) rozpoczynania, zawieszania i kończenia pracy Użytkowników w systemach,
5) korzystania z poczty elektronicznej i Internetu,
6) tworzenia i korzystania z kopii zapasowych,
7) korzystania z nośników danych,
8) zgłaszania incydentów, usterek, awarii systemów, uszkodzeń i podatności systemów,
9) przetwarzania danych osobowych w systemach informatycznych, z uwzględnieniem zarządzenia Rektora UWr w sprawie ochrony danych osobowych w Uniwersytecie Wrocławskim.

II. Odpowiedzialność

§ 7.1. Użytkownicy posiadający dostęp do informacji przetwarzanych w systemach informatycznych zobowiązani są do zachowania w tajemnicy danych podlegających ochronie.

2. Dane w systemach informatycznych Użytkownik może przetwarzać wyłącznie w zakresie przyznanych uprawnień.

§ 8.1. Dyrektor ds. informatycznych odpowiada za zarządzanie bezpieczeństwem informacji w Uczelni w zakresie określonym w § 20 rozporządzenia 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.

2. Kierownik Działu Usług Informatycznych odpowiada za bezpieczeństwo informacji przetwarzanych w podległych sieciach lokalnych: administracji centralnej, Biura Dolnośląskiego Festiwalu Nauki oraz jednostek pozawydziałowych UWr niewskazanych w ust. 4, w zakresie:

1) posiadania informacji o sprzęcie komputerowym i oprogramowaniu,
2) aktualizacji oprogramowania, w tym programów zabezpieczających i systemów operacyjnych,
3) kontroli legalności zainstalowanego oprogramowania i plików,
4) stosowania mechanizmów bezpieczeństwa informatycznego, w tym nadawania i odbierania uprawnień, wykrywania nieautoryzowanych działań, wykrywania złośliwych aplikacji, rejestracji incydentów i usuwania ich przyczyn,
5) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności przetwarzanych danych oraz podejmowania działań minimalizujących to ryzyko.

3. Dziekan opowiada za bezpieczeństwo informacji przetwarzanych w podległej sieci lokalnej lub w sieciach lokalnych podległych jednostek organizacyjnych np. instytutów, w zakresie opisanym w ust. 2 pkt 1-5.

4. Za bezpieczeństwo informacji przetwarzanych w sieciach lokalnych:

1) Archiwum Uniwersytetu Wrocławskiego,
2) Biblioteki Uniwersyteckiej,
3) Centrum Edukacji Nauczycielskiej,
4) Centrum Studiów Niemieckich i Europejskich im. Willy Brandta,
5) Instytutu Konfucjusza,

6) Muzeum Uniwersytetu Wrocławskiego,
7) Studium Intensywnej Nauki Języka Angielskiego,
8) Studium Praktycznej Nauki Języków Obcych,
9) Uniwersytetu Trzeciego Wieku,

odpowiada kierownik/dyrektor danej jednostki, w zakresie określonym w ust. 2 pkt 1-5.

5. Administratorzy systemu informatycznego odpowiadają za bezpieczeństwo informacji przetwarzanych w podległych im systemach.

III. Ogólne zasady korzystania z systemów

§ 9.1. Niniejszy Regulamin definiuje sposób postępowania w systemach informatycznych eksploatowanych przez Uczelnię.

2. Użytkownicy, którzy posiadają dostęp do systemów informatycznych Uczelni, są zobowiązani do przestrzegania ich wewnętrznych regulaminów dostępnych na stronie internetowej Uczelni www.uni.wroc.pl/sprawy-komputerowe lub stronach jednostek organizacyjnych.

3. Szczegółowe wytyczne dotyczące wymogów serwisów WWW określa Regulamin serwisów informacyjnych Uniwersytetu Wrocławskiego stanowiący **Załącznik Nr 1** do niniejszego Regulaminu.

§ 10.1. Dostęp do systemów informatycznych użytkowanych w Uczelni zabezpieczony jest poprzez unikatowe dane dostępowe tj. nazwę Użytkownika oraz hasło.

2. Każdy Użytkownik musi zapamiętać swoje dane dostępowe i nie udostępniać ich innym osobom. Użytkownik musi pamiętać o wylogowaniu się po zakończeniu korzystania z systemu informatycznego.

3. W celu zapobieżenia nieautoryzowanemu dostępowi do systemu, Użytkownik:
   1) nie może przechowywać danych dostępowych do systemów w miejscach dostępnych dla innych osób;
   2) nie może ujawniać danych dostępowych innym osobom.

4. Zabrania się:
   1) korzystania z systemu przy wykorzystaniu poświadczeń innego Użytkownika;
   2) zapisywania w używanych przeglądarkach danych dostępowych do systemów informatycznych.

5. Systemy są skonfigurowane zgodnie z następującymi zasadami bezpieczeństwa haseł:
   1) hasło musi składać się z minimum 8 znaków;
   2) hasło musi zawierać wielkie i małe litery oraz cyfry lub znaki specjalne;
   3) hasło można zmieniać nie częściej niż raz na 24 godziny;

6. W systemach, w których polityka opisana w ust. 5 jest niemożliwa do zrealizowania, administrator systemu informatycznego lub administrator lokalny opracowuje osobną politykę haseł.

7. Użytkownik podczas logowania się do systemów (w przypadku systemów korzystających z przeglądarki, jako klienta dostępowego) musi sprawdzić:
   1) czy w pasku adresowym przeglądarki adres zaczyna się od https,
   2) czy w obrębie okna przeglądarki znajduje się symbol kłódki informujący o bezpieczeństwie,
   3) czy po kliknięciu symbolu kłódki pojawia się informacja o tym, że certyfikat jest prawidłowy i ważny.

8. Użytkownicy muszą ustawić ekrany monitorów w taki sposób, aby uniemożliwić osobom nieuprawnionym wgląd lub zapisanie informacji aktualnie wyświetlanej na ekranie monitora.

9. Użytkownikowi nakazuje się przestrzegania tzw. zasady czystego biurka. Przed opuszczeniem swojego stanowiska pracy Użytkownik powinien, w szczególności schować wszelkie dokumenty związane z używanymi systemami informatycznymi oraz nośniki danych.

10. W przypadku nieumyślnego ujawnienia hasła osobie nieuprawnionej lub podejrzenia ujawnienia, należy bezzwłocznie dokonać zmiany hasła na nowe oraz zgłosić to zdarzenie administratorowi lokalnemu.

11. W przypadku braku możliwości dokonania przez Użytkownika zmiany hasła (braku działania funkcjonalności przypominającej/zmieniającej hasło) należy powiadomić o tym fakcie administratora systemu informatycznego lub administratora lokalnego w jednostce.

12. Przekazywanie hasła w większości systemów odbywa się drogą mailową na adres poczty służbowej (lub w szczególnych przypadkach na adres podany w systemie, inny niż służbowy) lub za pomocą sms. Użytkownik musi dokonać niezwłocznej zmiany hasła podanego mu przez administratora lokalnego lub administratora systemu informatycznego.

IV. Konfiguracja sprzętu komputerowego Użytkownika

§ 11.1. Komputer Użytkownika musi posiadać oprogramowanie antywirusowe, którego automatyczna aktualizacja sygnatur wirusów musi być włączona. Oprogramowanie antywirusowe musi być stale aktywne.

2. Użytkownik jest zobowiązany do odczytywania komunikatów pochodzących z oprogramowania antywirusowego zainstalowanego na komputerze Użytkownika i reagowania na wyświetlane komunikaty.

3. Regulamin stosowania oprogramowania antywirusowego oraz zapory sieciowej w UWr stanowi **Załącznik Nr 2** do niniejszego Regulaminu.

§ 12.1 Podczas pracy z systemem na komputerze Użytkownika nie może być uruchomione oprogramowanie umożliwiające udostępnianie informacji poza stanowisko pracy z wyjątkiem oprogramowania służącego do zarządzania stacjami roboczymi, zatwierdzonego przez kierownika danej jednostki.

2. Oprogramowanie komputera musi być regularnie aktualizowane, w szczególności dotyczy to systemu operacyjnego oraz przeglądarki internetowej. Za czynności te odpowiada administrator danej stacji roboczej.

3. Przeglądarka internetowa musi zostać tak skonfigurowana, aby miała włączoną obsługę protokołu OCSP (Online Certificate Status Protocol), umożliwiającego przeprowadzenie weryfikacji ważności certyfikatu systemów oraz stron internetowych.

4. Każde urządzenie użytkowane w systemie informatycznym, musi podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby np. administratora lokalnego.

5. Przed opuszczeniem stanowiska komputerowego, Użytkownik musi zablokować komputer/stację roboczą. Czas trwania nieaktywnej sesji (czas bezczynności), po jakim powinno nastąpić zablokowanie stanowiska Użytkownika wynosi 5 minut. W celu wznowienia pracy na stanowisku, Użytkownik musi wprowadzić swoje dane logowania do komputera. Blokowanie stacji nie powoduje zatrzymania pracy działających w tle aplikacji.

6. Użytkownik nie posiada praw administracyjnych do komputera, z zastrzeżeniem ust. 7, co uniemożliwia wprowadzenie zmian w ustawieniach systemowych oraz ustawieniach aplikacji systemowych. W przypadku konieczności instalacji dodatkowego oprogramowania fakt ten powinien zostać zgłoszony do administratora lokalnego.

7. Wyróżnia się Użytkowników zaawansowanych, którym ze względu na specyfikę pracy na danym stanowisku nadaje się prawa administracyjne do tej stacji roboczej. Status Użytkownika zaawansowanego nadaje osoba odpowiedzialna za bezpieczeństwo przetwarzania danych w systemach informatycznych, zgodnie z § 8 niniejszego Regulaminu.

V. Zasady korzystania z Uczelnianej Sieci Komputerowej

§ 13.1. Uczelniana Sieć Komputerowa UWr, jest przyłączona do Wrocławskiej Akademickiej Sieci Komputerowej (WASK), a poprzez nią do Naukowej Akademickiej Sieci Komputerowej (NASK) i podlega przepisom zawartym w regulaminach NASK, Wrocławskiego Centrum Sieciowo-Superkomputerowego (WCSS) i WASK dostępnych na stronie WCSS, które mają zastosowanie w kwestiach nieobjętych niniejszym Regulaminem.

2. Uczelniana Sieć Komputerowa UWr ma na celu zagwarantowanie uprawnionym Użytkownikom dostępu do informacji niezbędnych do realizacji celów dydaktyczno-naukowych, ponadto wspiera realizację zadań związanych z zarządzaniem Uczelnią.

3. USK UWr tworzą:
   1/ sieć szkieletowa Uczelni,
   2/ sieci lokalne poszczególnych jednostek organizacyjnych UWr,
   3/ lokalna sieć administracji centralnej, zwana dalej „LAN-AC”,
   4/ sieć Domów Studenckich.

4. Szczegółowy Regulamin Uczelnianej Sieci Komputerowej Uniwersytetu Wrocławskiego stanowi **Załącznik Nr 3** do niniejszego Regulaminu.

5. Szczegółowy Regulamin Lokalnej Sieci Komputerowej Administracji Centralnej Uniwersytetu Wrocławskiego stanowi **Załącznik Nr 4** do niniejszego Regulaminu.

§ 14.1. Uczelnia udostępnia Użytkownikom bezprzewodową sieć o nazwie Eduroam. Jest to sieć ogólnodostępna wymagająca uwierzytelnienia Użytkownika.

2. Użytkownik sieci Eduroam jest odpowiedzialny za wszelkie działania sieciowe dokonane po uwierzytelnieniu przy pomocy jego poświadczeń. W przypadku podejrzenia, że poświadczenia mogły się dostać w ręce osób trzecich, Użytkownik jest zobowiązany do niezwłocznego zawiadomienia o tym fakcie administratora lokalnego w swojej jednostce macierzystej. W przypadku niewykonania powyższego obowiązku Użytkownik ponosi pełną odpowiedzialność za szkody wywołane działaniem lub zaniechaniem osób trzecich korzystających z jego danych uwierzytelniających.

3. Dane kontaktowe administratora lokalnego są dostępne na stronie internetowej Uczelni dotyczącej sieci Eduroam.

4. Użytkownik sieci Eduroam musi dołożyć starań, aby przed wysłaniem danych uwierzytelniających upewnić się, że korzysta z autentycznego zasobu Eduroam.

5. Użytkownik powinien być świadomy, że fakt korzystania z sieci Eduroam jest odnotowywany w logach systemowych zarówno instytucji udostępniającej zasoby, jak i jego macierzystej instytucji uwierzytelniającej.

6. Użytkownik musi działać zgodnie z regulaminem sieci komputerowej, z której korzysta.

7. Użytkownik sieci Eduroam może korzystać z gościnnego dostępu wyłącznie na swój własny użytek.

8. Zabrania się udostępniania na terenie Uczelni prywatnych sieci bezprzewodowych.

9. Pracownicy Działu Usług Informatycznych (DUI) informują z wyprzedzeniem administratorów lokalnych o planowanych aktualizacjach i innych czynnościach mających wpływ na wewnętrzne systemy informatyczne.

10. Pracownicy DUI informują administratorów lokalnych o usunięciu usterek i przywróceniu pełnej funkcjonalności ogólnouczelnianych systemów.

VI. Rozpoczynanie, zawieszanie i kończenie pracy Użytkowników w systemach

§ 15.1. Rozpoczęcie pracy Użytkownika w systemach następuje po uruchomieniu przeglądarki lub aplikacji zainstalowanej na stanowisku.

2. Użytkownik musi zwracać uwagę na wszelkie anomalie związane z rozpoczęciem lub zakończeniem pracy w systemach oraz zgłaszać je do administratora lokalnego lub administratora systemu informatycznego.

3. Dostęp do wewnętrznych systemów informatycznych może nastąpić jedynie poprzez sprzęt służbowy, który uzyskuje dostęp do sieci poprzez sieć uczelnianą lub poprzez usługę VPN.

4. W celu uwierzytelnienia się w systemach należy wykorzystać swoje dane dostępowe do danego systemu. Należy dochować wszelkich starań, aby zachować poufność danych dostępowych.

5. Nie należy rozpoczynać pracy w systemach, jeśli istnieje groźba utraty poufności danych dostępowych osobie trzeciej, przebywającej w pobliżu stanowiska.

6. Zabrania się rozpoczynania pracy w systemach na stanowiskach do tego nieprzeznaczonych, np. na komputerach bez aktualnego oprogramowania antywirusowego.

7. W celu chwilowego zawieszenia pracy w systemie, należy zablokować ekran (zablokować pulpit lub włączyć wygaszacz ekranu zabezpieczony hasłem). Jeśli komputer Użytkownika nie pozwala na zabezpieczenie ekranu hasłem, należy wylogować się z systemu.

8. Zakończenie pracy Użytkownika w systemie następuje po wykonaniu procedury wylogowaniu się z systemu.

9. Niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury wylogowania np. poprzez wyłączenie napięcia zasilającego stanowisko lub poprzez zamknięcie przeglądarki.

10. W przypadku rozwiązania umowy z Użytkownikiem, z dniem zakończenia umowy lub stosunku pracy wygasają uprawnienia do posiadanych kont i wykonywane są następujące czynności administracyjne:

1) zablokowana zostaje możliwość dostępu do wszystkich systemów informatycznych, w tym poczty elektronicznej,
2) blokowana jest indywidualna strona WWW Użytkownika,
3) blokowane są wszystkie uprawnienia wynikające z posiadanego konta,
4) identyfikator konta nie zostaje ponownie przydzielony innej osobie.

11. Użytkownik jest zobowiązany przed zakończeniem stosunku pracy lub rozwiązaniem umowy cywilnoprawnej do przekazania danych istotnych dla działania Uczelni uprawnionej osobie.

12. Przepisy ust. 10 stosuje się odpowiednio do podmiotów zewnętrznych.

13. W przypadku studentów, doktorantów i słuchaczy przepisy ust. 10. stosuje się odpowiednio, po upływie dwóch lat od zakończenia studiów lub skreślenia z listy studentów, doktorantów, słuchaczy.

14. Pracownik przed dniem zakończenia umowy lub stosunku pracy, w celu otrzymywania wiadomości przychodzących w domenie uwr.edu.pl powinien ustawić przekierowanie wiadomości na inny wybrany przez siebie e-mail. Przekierowanie będzie aktywne przez 24 miesiące od dnia zakończenia umowy lub stosunku pracy. Przekierowanie pracownik ustawia sam w ustawieniach skrzynki pocztowej.

VII. Korzystanie z poczty elektronicznej i Internetu

§ 16.1. Obowiązek posiadania (służbowego) konta poczty elektronicznej w domenie uwr.edu.pl mają:

1/ wydziały oraz jednostki pozawydziałowe;
2/ pracownicy Uniwersytetu Wrocławskiego;
3/ osoby funkcyjne;
4/ studenci, doktoranci i słuchacze Uniwersytetu Wrocławskiego.

2. Szczegółowy regulamin korzystania z usługi MS Office365 stanowi **Załącznik Nr 5** do niniejszego Regulaminu.

3. Zasady tworzenia adresów poczty elektronicznej stanowi **Załącznik Nr 6** do niniejszego Regulaminu.

VIII. Kopie zapasowe

§ 17.1. Użytkownicy zaawansowani, określeni w § 12 ust. 7, zobowiązani są do tworzenia kopii zapasowych zbiorów danych na nośnikach informacji (backup), według zasad określonych w danej jednostce.

2. W przypadku standardowych stanowisk komputerowych, do których Użytkownik nie posiada praw administracyjnych, za tworzenie kopii awaryjnych systemu i danych służbowych odpowiada administrator lokalny.

3. Kopie zapasowe powinny być kontrolowane przez administratora lokalnego, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.

4. Kopia zapasowa oprogramowania oraz danych Użytkownika wykonywana na komputerze lokalnym musi zawierać wszystkie dane służbowe.

5. Kopie zapasowe muszą być wykonywane w odstępach czasu nie dłuższych niż 14 dni roboczych.

IX. Nośniki danych

§ 18.1. Nośniki danych, na których zapisane są dane podlegające ochronie, muszą być zabezpieczone przed nieuprawnionym dostępem, np. poprzez ich zaszyfrowanie.

2. Nośniki danych, na których zapisane są dane podlegające ochronie, są przechowywane w sposób uniemożliwiający dostęp do nich osób nieuprawnionych, jak również zabezpieczający je przez zagrożeniami środowiskowymi, np. przed wpływem pól elektromagnetycznych.

3. Nośniki danych, na których przetrzymywano dane podlegające ochronie lub dla których istnieje uzasadnione podejrzenie, że takie dane mogły się na nich znajdować, a których czas eksploatacji dobiegł końca, muszą zostać zutylizowane w sposób właściwy i bezpieczny.

4. Każdy nośnik danych spełniający kryteria opisane w ust. 2 powinien zostać przekazany do administratora lokalnego po wcześniejszym usunięciu z niego wszystkich danych w sposób dostępny Użytkownikowi np. poprzez formatowanie nośnika typu pendrive czy dysku twardego.

5. Administrator lokalny jest odpowiedzialny za utylizację nośników danych przekazanych przez Użytkownika po zakończeniu eksploatacji nośników danych, zgodnie z zasadami określonymi w UWr.

6. Nośnik musi zostać pozbawiony zawartości w sposób uniemożliwiający odczyt danych według zasad właściwych dla danego nośnika np. poprzez wpięcie pendriva do portu USB lub podłączenie dysku twardego do stacji roboczej poprzez odpowiednie kable sygnałowe i zasilające.

X. Zgłaszania incydentów, usterek, awarii systemów oraz zagrożeń dla bezpieczeństwa danych

§ 19.1. Uczelnia posiada ogólnouczelniany system obsługi zgłoszeń informatycznych – Logsystem.

2. System Logsystem zarządza zgłoszeniami Użytkowników, dotyczącymi problemów powstałych podczas pracy z systemami informatycznymi oraz problemów związanych z eksploatacją sprzętu komputerowego administrowanego przez Dział Usług Informatycznych.

3. Szczegółowy Regulamin korzystania z systemu Logsystem stanowi **Załącznik Nr 7** do niniejszego Regulaminu.

§ 20.1. W przypadku awarii lub konieczności konserwacji lub napraw sprzętu komputerowego należy ten fakt zgłosić bezpośrednio do administratora lokalnego.

2. Naprawy sprzętu objętego umowami serwisowymi odbywają się zgodnie z zasadami ustalonymi w umowie serwisowej.

3. Naprawa sprzętu, która odbywa się w miejscu użytkowania sprzętu wymaga nadzoru osób użytkujących sprzęt lub osób za niego odpowiedzialnych.

4. Sprzęt przed oddaniem do naprawy/serwisu poza miejsce jego użytkowania powinien zostać odpowiednio przygotowany, w szczególności należy skutecznie usunąć z niego zbiory danych, zwłaszcza zbiory zawierające dane osobowe, za co odpowiedzialny jest Użytkownik. W przypadku braku odpowiedniej wiedzy do wykonania ww. zadania możliwe jest przekazanie przez Użytkownika wniosku do administratora lokalnego o wykonanie tych czynności przed naprawą sprzętu.

5. Szczegółowe zasady zgłaszania awarii sprzętu komputerowego i oprogramowania oraz przeprowadzania czynności serwisowych w jednostkach organizacyjnych administracji centralnej określa **Załącznik Nr 8** do niniejszego Regulaminu.

§ 21.1. Każdy Użytkownik, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych jest zobowiązany niezwłocznie zgłosić to administratorowi danych osobowych, administratorowi systemu informatycznego lub administratorowi lokalnemu.

2. Każdy pracownik Uczelni, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia.

3. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia odpowiedniego administratora.

XI. Ogólne zasady przetwarzania danych osobowych w systemach

§ 22.1. W przypadku przetwarzania danych osobowych w systemach informatycznych w Uniwersytecie Wrocławskim, należy postępować zgodnie z zarządzeniem Rektora Uniwersytetu Wrocławskiego w sprawie ochrony danych osobowych w Uniwersytecie Wrocławskim oraz zgodnie z innymi obowiązującymi przepisami, a w szczególności zgodnie z:

1) art. 25 RODO - konieczne jest uwzględnianie ochrony danych już w fazie projektowania nowych rozwiązań informatycznych dla Uniwersytetu Wrocławskiego; ponadto w systemach informatycznych w Uniwersytecie Wrocławskim wdraża się takie środki, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia celów przetwarzania;

2) art. 32 RODO – przed doborem środków mających zapewnić bezpieczeństwo przetwarzania danych osobowych w systemach należy przeprowadzić udokumentowana ocenę ryzyka naruszenia prawa lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, tak by dobrać środki zapewniające odpowiedni stopień bezpieczeństwa;

3) art. 35 RODO – przed rozpoczęciem przetwarzania dokonuje się oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

2. Informacje o: służbowym adresie e-mail pracownika, sprawowanej funkcji oraz jednostce organizacyjnej, w której jest zatrudniony, są jawne i dostępne powszechnie, w tym na stronie internetowej Uczelni.

3. Zakres danych osobowych przetwarzanych przez Użytkownika w systemie określa upoważnienie do przetwarzania danych osobowych nadane przez Uczelnię.

4. Użytkownik odpowiada za zgodność danych osobowych, wprowadzonych przez siebie do systemów, z dokumentami źródłowymi.

5. Fakt przekazania na zewnątrz Uniwersytetu Wrocławskiego danych osobowych w postaci cyfrowej, zawartych w bazach wewnętrznych systemów informatycznych: ZSKP, ZSI, USOS, odnotowywany jest w rejestrach prowadzonych przez administratora danego systemu informatycznego.

6. Rejestracja przekazywania danych osobowych na zewnątrz Uniwersytetu Wrocławskiego z wewnętrznego systemu informatycznego Płatnik prowadzona jest w logach elektronicznych tego oprogramowania.

7. Każda osoba, której dane dotyczą ma prawo dostępu do treści swoich danych oraz prawo żądania ich uzupełnienia, uaktualnienia lub sprostowania.

Załącznik Nr 1
do Regulaminu

Regulamin serwisów informacyjnych w Uniwersytecie Wrocławskim

Postanowienia ogólne i definicje

§ 1

1. Regulamin dotyczy wszystkich serwisów informacyjnych posiadających adres w domenie uni.wroc.pl lub w jej poddomenach oraz tych serwisów, które są publikowane w zewnętrznych domenach na podstawie zawartej przez jednostkę organizacyjną UWr umowy na usługę hostingową.
2. Ilekroć w Regulaminie jest mowa o:
   a) serwisie informacyjnym — rozumie się przez to usługę informacyjną udostępnioną on-line np. stronę WWW, forum dyskusyjne, pocztę elektroniczną, itp.;
   b) właścicielu serwisu informacyjnego — rozumie się przez to kierownika jednostki organizacyjnej, w której domenie serwis jest publikowany, z zastrzeżeniem ust. 3;
   c) administratorze merytorycznym — rozumie się przez to pracownika UWr (zespół pracowników) odpowiedzialnego za materiał udostępniony w serwisie, który został wyznaczony przez właściciela serwisu informacyjnego;
   d) administratorze technicznym — rozumie się przez to pracownika UWr lub firmę zewnętrzną (z którą jest podpisana stosowna umowa) odpowiedzialnego za poprawne funkcjonowanie serwisu, który został wyznaczony przez właściciela serwisu informacyjnego;
   e) usłudze hostingowej — rozumie się przez to udostępnienie zasobów serwerowych w celu przechowywania plików serwisu oraz zagwarantowanie możliwości przesyłania danych poprzez sieć internetową.
3. Właścicielem następujących serwisów jest:
   a) BIP, strona główna i rekrutacyjna — kierownik Biura ds. Promocji;
   b) strona Ogrodu Botanicznego — Dyrektor Ogrodu Botanicznego;
   c) strona USOS Web i serwis IRKa — kierownik Działu Informatycznych Systemów Obsługi Studiów;
   d) strony jednostek organizacyjnych administracji centralnej — Dyrektor Generalny;
   e) serwisy kół studenckich — Prorektor ds. studenckich;
   f) strona usługi Office 365 — kierownik Działu Usług Informatycznych (DUI);
   g) strona International Application — kierownik Biura Współpracy Międzynarodowej.

Zakładanie i likwidacja serwisu informacyjnego

§ 2

1. Jednostki organizacyjne UWr zobowiązane są do posługiwania się adresami serwisów w domenie uni.wroc.pl.
2. Serwisy stowarzyszeń, kół naukowych i innych organizacji działających na terenie UWr publikowane są w domenie wydziału, na którym działa dana organizacja lub na stronie głównej UWr.
3. Z wnioskiem o założenie poddomeny w domenie uni.wroc.pl może wystąpić właściciel serwisu. Wniosek składa się do kierownika DUI. Wzór wniosku stanowi Załącznik Nr 1 do niniejszego Regulaminu.
4. DUI zapewnia usługę hostingową dla serwisów wszystkich jednostek organizacyjnych, organizacji działających w Uczelni oraz pracowników UWr.

5. Jeżeli jednostka organizacyjna posiada odpowiednie zasoby sprzętowe i kadrowe, może publikować serwisy informacyjne na własnym serwerze hostingowym.
6. W uzasadnionych przypadkach możliwe jest skorzystanie z zewnętrznej usługi hostingowej. Uruchomienie takiej usługi wymaga zgody Rektora.
7. Serwis może zostać zamknięty na wniosek właściciela serwisu informacyjnego lub zablokowany w trybie § 5 ust. 4 lit. b.

Zawartość serwisu WWW

§ 3

1. Każdy serwis WWW powinien zawierać:
   a) nazwę i adres jednostki;
   b) strukturę jednostki;
   c) informacje o kierownictwie jednostki;
   d) informacje o jednostce organizacyjnej administracji obsługującej kierownictwo jednostki;
   e) link do strony głównej UWr bez konieczności przewijania strony;
   f) politykę prywatności w brzmieniu Załącznika Nr 2 do niniejszego Regulaminu.
2. Serwis jednostki prowadzącej działalność dydaktyczną lub dydaktyczno-naukową powinien dodatkowo zawierać:
   a) informację o studiach i prowadzonych zajęciach;
   b) spis pracowników wraz z adresem poczty elektronicznej, telefonem i numerem pokoju;
   c) zasady rekrutacji na studia i zapisów na zajęcia;
   d) informacje o badaniach naukowych, organizowanych konferencjach itp.
3. Zabrania się umieszczania w serwisach WWW:
   a) reklam, z zastrzeżeniem ust. 4;
   b) treści niezgodnych z misją Uczelni np. pornografii;
   c) treści naruszających obowiązujące prawo, w tym związanych z ochroną wizerunku;
   d) materiałów stanowiących przedmiot prawa autorskiego bez posiadania stosownej zgody;
   e) nielegalnego oprogramowania;
   f) oprogramowania służącego do naruszenia bezpieczeństwa informacji;
   g) linków do stron z powyższymi treściami.
4. Zamieszczanie reklam komercyjnych, w szczególności loga lub logotypu, tekstu reklamowego, bannera, artykułu sponsorowanego, jest dopuszczalne, jeżeli:
   a) materiał jest wyraźnie oznaczony jako reklama oraz
   b) została zawarta umowa sponsorska lub została wyrażona pisemna zgoda kierownika Biura ds. Promocji co do formy i czasu publikacji reklamy.

Obowiązki

§ 4

1. Właściciel serwisu zobowiązany jest do:
   a) nadzoru nad serwisem w zakresie bezpieczeństwa przetwarzania informacji w systemach informatycznych oraz przepisów dotyczących ochrony danych osobowych;
   b) dostosowania istniejących serwisów do standardów WCAG 2.0 na poziomie A i AA oraz wymogów systemu identyfikacji wizualnej w ciągu jednego roku od daty wejścia w życie niniejszego Regulaminu;
   c) Wykonywania zaleceń Biura ds. Promocji w zakresie, o którym mowa w § 5 ust. 2.
2. Administrator merytoryczny zobowiązany jest do:
   a) dbania o zgodność treści serwisu z zapisami § 3;
   b) używania w polskich tekstach polskich znaków diakrytycznych zgodnie ze standardem kodowania UTF-8;
   c) zamieszczania w serwisie dokumentów w plikach możliwych do odczytania przez programy czytające dla osób niewidomych i niedowidzących;

   d) bieżącej aktualizacji zamieszczonych w serwisie informacji.
3. Administrator techniczny zobowiązany jest do:
   a) okresowego tworzenia kopii zapasowych plików serwisu;
   b) przywrócenia prawidłowego funkcjonowania serwisu po ewentualnej awarii lub incydencie;
   c) corocznej kontroli mechanizmów bezpieczeństwa;
   d) prowadzenia rejestru incydentów.
   e) przeniesienia serwisu w przypadku zmiany dostawcy usługi hostingowej.

Nadzór i sankcje

§ 5

1. Nadzór nad przestrzeganiem niniejszego Regulaminu sprawuje Dyrektor ds. informatycznych.
2. Kierownik Biura ds. Promocji przeprowadza rokrocznie weryfikację wybranych serwisów pod kątem spełnienia wymogów prawa w zakresie świadczenia usług drogą elektroniczną oraz wymogów systemu identyfikacji wizualnej, z zastrzeżeniem ust. 3.
3. Weryfikację strony głównej i rekrutacyjnej oraz strony BIP pod kątem spełnienia wymogów prawa w zakresie świadczenia usług drogą elektroniczną oraz wymogów systemu identyfikacji wizualnej przeprowadza Dyrektor ds. informatycznych.
4. Dyrektor ds. informatycznych ma prawo stosować wobec właściciela serwisu, który naruszył przepisy niniejszego Regulaminu:
   a) pisemne upomnienie;
   b) zablokowanie działania serwisu;
   c) zablokowanie nazwy domeny w DNSie;
   d) likwidację wpisu w DNSie, po co najmniej miesięcznym okresie zablokowania domeny.
5. Od decyzji o zablokowaniu serwisu lub domeny właścicielowi przysługuje prawo wniesienia odwołania do Rektora. Decyzja Rektora jest ostateczna.
6. Zastosowanie sankcji, o których mowa w ust. 4 nie zwalnia właściciela serwisu z odpowiedzialności wynikającej z odrębnych przepisów.

Załącznik Nr 1
do Regulaminu serwisów
informacyjnych UWr

……
znak sprawy

……
nazwa jednostki

Wrocław, ……

Kierownik Działu Usług Informatycznych

WNIOSEK O ZAŁOŻENIE PODDOMENY

Zwracam się z prośbą o założenie poddomeny w domenie uni.wroc.pl dla usług:

- WWW*
- Poczta elektroniczna*
- Forum dyskusyjne*
- Inne……..

……
(*proponowana nazwa poddomeny*)

dla
……
(*nazwa jednostki organizacyjnej ubiegającej się o poddomenę*)

Administrator techniczny. Domeną będzie administrował**:

……..……

Administrator merytoryczny. Nadzór merytoryczny nad domeną będzie sprawował**:

……..……

……..

pieczęć, data i podpis kierownika jednostki organizacyjnej

(właściciela serwisu informacyjnego)

Wyjaśnienia:

* niepotrzebne skreślić
** podać imię, nazwisko, jednostkę, telefon, adres e-mail.

Załącznik Nr 2
do Regulaminu serwisów
informacyjnych UWr

Polityka prywatności Uniwersytetu Wrocławskiego

I. Informacje o przetwarzaniu danych osobowych w serwisach Uniwersytetu Wrocławskiego

1. Uniwersytet Wrocławski przywiązuje szczególną wagę do poszanowania prywatności, w tym prywatności użytkowników odwiedzających serwisy internetowe Uczelni.

2. Uniwersytet Wrocławski ma siedzibę przy pl. Uniwersyteckim 1, 50-137 Wrocław i jest administratorem danych, w rozumieniu RODO (*Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE*), zobowiązanym do zapewnienia, aby przetwarzanie danych osobowych użytkownika serwisu internetowego UWr odbywało się zgodnie z przepisami.

3. W Uczelni powołany został inspektor ochrony danych, z którym można się skontaktować poprzez adres e-mail: IOD@uwr.edu.pl.

4. Jeśli podczas korzystania z serwisów internetowych UWr gromadzone są jakiekolwiek dane, które uznać można za dane osobowe, wówczas Uczelnia przestrzega zasad wskazanych przez RODO oraz inne przepisy dotyczące ochrony danych, a w szczególności dba o to, aby:
1) przetwarzane odbywało zgodnie z prawem, rzetelnie i w sposób przejrzysty, a w pozyskiwaniu danych przyświecały konkretne, uzasadnione cele;
2) gromadzić jedynie niezbędne i prawidłowe dane i tylko na taki czas, jaki jest konieczny;
3) przetwarzanie danych osobowych odbywało się w sposób bezpieczny, oparty na ocenie ryzyka.

5. Dane użytkownika serwisu internetowego UWr mogą być przekazywane jedynie osobom upoważnionym, sprawdzonym podmiotom, z którymi zostały zawarte stosowne umowy oraz podmiotom uprawnionym do ich uzyskania na podstawie obowiązującego prawa.

6. Uniwersytet Wrocławski dba o to, aby każda osoba działająca z upoważnienia Uczelni i mająca dostęp do danych osobowych przetwarzała je wyłącznie na polecenie Uczelni.

7. Uniwersytet Wrocławski podejmuje niezbędne działania aby prawa użytkownika serwisu internetowego UWr, odnoszące się do przetwarzania danych osobowych, były właściwie spełniane, a w szczególności aby:
1) komunikacja odbywała się w sposób przejrzysty;
2) udzielane były właściwe informacje i dostęp do danych osobowych;
3) wypełniane były żądania do których użytkownik serwisu internetowego UWr ma prawo, w tym sprostowania i usuwania danych oraz prawo sprzeciwu wobec przetwarzania danych.

8. Uczelnia stara się wykonać dobrze obowiązki przewidziane w RODO i innych przepisach dotyczących ochrony danych, nie mniej użytkownik serwisu internetowego UWr ma prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;

II. Informacje o plikach cookie w serwisach Uniwersytetu Wrocławskiego.

1. Dane prywatne na temat użytkowników nie są rozpowszechniane i przekazywane innym podmiotom.

2. Podczas odwiedzin naszej witryny mogą być zapisywane pliki cookie, które zawierają między innymi: numer IP użytkownika, dostawcę Internetu użytkownika, sposób poruszania się użytkownika po naszej witrynie (np. jakie zakładki otwiera), nazwę przeglądarki z której korzysta.

3. Pliki cookie użytkownik może zdezaktywować lub całkowicie wyłączyć w opcjach swojej przeglądarki, uniemożliwi to zalogowanie się do strony, gdyż funkcjonalność ta wymaga działających ciasteczek.

4. Liczba odwiedzin na naszej stronie internetowej jest monitorowana przez Google Analytics, w celu gromadzenia danych o popularności naszej witryny i sposobie korzystania z niej. Akceptując naszą politykę plików cookie, użytkownik zgadza się na analizę swoich danych przez Google Analytics.

Załącznik Nr 2
do Regulaminu

Procedura stosowania oprogramowania antywirusowego oraz zapory sieciowej w Uniwersytecie Wrocławskim

§ 1
Wymagania stawiane oprogramowaniu antywirusowemu oraz zaporze sieciowej

1. Każda stacja robocza i serwer podłączony do Uczelnianej Sieci Komputerowej musi posiadać aktualne oprogramowanie antywirusowe oraz zaporę sieciową.
2. Oprogramowanie antywirusowe oraz zapora sieciowa muszą posiadać automatyczną aktualizację z sieci Internet lub z lokalnego repozytorium.
3. Oprogramowanie antywirusowe powinno wykrywać poza wirusami jak największą liczbę złośliwych programów innego rodzaju (np. konie trojańskie, backdoory, exploity, niebezpieczne aplety Javy i ActiveX, spam, itp.). Ponadto powinno się charakteryzować dobrymi narzędziami do analizy heurystycznej, skanowaniem na żądanie całości systemu, bądź jego elementów, skanowaniem w czasie rzeczywistym i niskim obciążeniem systemu.
4. Oprogramowanie antywirusowe powinno posiadać funkcję automatycznego powiadamiania administratora o wystąpieniu incydentu (np. pojawieniu się wirusa w poczcie, próby włamania do systemu, itp.), a także powinno monitorować system on-line i reagować na bieżąco na wszelkie incydenty wg ustawionych przez administratora reguł.
5. Oprogramowanie antywirusowe powinno automatycznie sprawdzać wszelkie podłączane do systemu urządzenia.
6. Oprogramowanie antywirusowe oraz zapora sieciowa (firewall) powinny być w języku polskim.
7. Szkolenie pracowników UWr w zakresie korzystania z systemu antywirusowego jest prowadzone przez administratorów lokalnych, z wykorzystaniem platformy e-learningowej przygotowanej i udostępnianej przez pracowników DUI.

§ 2
Zadania kierownika jednostki organizacyjnej

1. Kierownik jednostki organizacyjnej wyznacza administratora sieci lokalnej, który jest odpowiedzialny za wdrożenie i przestrzeganie niniejszej procedury.
2. Kierownik jednostki organizacyjnej ma obowiązek przeznaczyć odpowiednie środki finansowe na zakup ww. oprogramowania.
3. Kierownik jednostki, po otrzymaniu zgłoszenia o wystąpieniu incydentu od administratora sieci lokalnej i po zapoznaniu się ze sprawą, w wyniku której doszło do utraty (kradzieży) danych lub innego rodzaju przestępstwa, zobowiązany jest podjąć właściwe działania dla danej sytuacji, w szczególności zawiadomić właściwe organy Państwa.

§ 3
Zadania administratorów sieci lokalnej

1. Administrator sieci lokalnej odpowiada za:
   1/ aktualizację oprogramowania i jego baz;
   2/ właściwą konfigurację oprogramowania antywirusowego oraz zapory sieciowej. Podczas konfiguracji zapory sieciowej administrator zobowiązany jest zablokować wszystkie porty w zaporze sieciowej zezwalając tylko na komunikację aplikacji niezbędnych do pracy na danej stacji roboczej.
2. Administrator sieci lokalnej ma obowiązek:
   1/ przeglądania i zabezpieczenia elektronicznie logów oprogramowania antywirusowego oraz zapory sieciowej;
   2/ niezwłocznego reagowania na wszelkie powiadomienia o wystąpieniu incydentu, związanego z zainstalowanym oprogramowaniem antywirusowym i zaporą sieciową;

3/ odnotowywania w elektronicznym dzienniku wszelkich incydentów, w wyniku których doszło do utraty/kradzieży danych lub innego przestępstwa, a także niezwłocznego zgłaszania tego faktu kierownikowi jednostki organizacyjnej. Ponadto administrator ma obowiązek zabezpieczyć logi dla celów dowodowych.

3. Administrator sieci lokalnej ma prawo wyłączyć Użytkownikom mechanizm przeglądania i wysyłania treści wiadomości w formacie HTML w przeglądarce poczty. W przeglądarkach internetowych ma prawo ograniczyć możliwości otwierania się różnego rodzaju skryptów.
4. Administrator sieci lokalnej jest zobowiązany do sporządzania zestawu programów freeware akceptowalnych w sieci przez niego zarządzanej.

§ 4
Zadania Użytkowników

1. Użytkownicy odpowiadają za poufność swoich danych dostępowych (login i hasło) oraz za dane wytwarzane przez siebie w ramach obowiązków pracy.
2. Użytkownicy nie mogą instalować żadnego oprogramowania bez wiedzy i pisemnej zgody administratora ich lokalnej sieci komputerowej. Przez pisemną zgodę uważa się akceptację przez administratora pisma z wymienionym oprogramowaniem.
3. Użytkownicy nie mają prawa podłączać do sieci lokalnej Uczelni żadnych urządzeń typu: routery, access pointy, switche, za wyjątkiem urządzeń służbowych, bez wiedzy i pisemnej zgody administratora ich sieci lokalnej. Przez pisemną zgodę uważa się akceptację przez administratora pisma z wymienionym sprzętem.
4. Zabrania się Użytkownikom otwierania załączników poczty oraz plików nieznanego pochodzenia. Dotyczy to również plików pobranych ze stron WWW (np. aplikacji flash, muzyki, krótkiego filmiku, itp.).
5. Użytkownik ma obowiązek pracować na koncie z uprawnieniami Użytkownika lub Użytkownika zaawansowanego. W wyjątkowych sytuacjach, za wiedzą i pisemną zgodą administratora sieci, może korzystać z konta administratora systemu.
6. Każdy Użytkownik powinien zostać przeszkolony w zakresie obsługi oprogramowania antywirusowego oraz zapory sieciowej, a także sposobów powiadamiania administratora sieci lokalnej o wystąpieniu incydentów (np. wirusów) wykrytych przez oprogramowanie antywirusowe. Użytkownicy nieprzeszkoleni mogą żądać przeprowadzenia stosownego szkolenia w ustalonym z administratorem terminie.
7. Po włożeniu zewnętrznego nośnika danych, jeśli nie zostanie on sprawdzony automatycznie przez oprogramowanie antywirusowe lub inne oprogramowanie chroniące, Użytkownik ma obowiązek sprawdzenia go ręcznie przy pomocy ww. oprogramowania.
8. W przypadku, gdy oprogramowanie powiadomi Użytkownika o wystąpieniu incydentu (np. pojawieniu się wirusa, próbie włamania do systemu, itp.), Użytkownik ma obowiązek postępować zgodnie z ustaleniami jakie uzyskał od administratora sieci lokalnej podczas szkolenia.

Załącznik Nr 3
do Regulaminu

Regulamin Uczelnianej Sieci Komputerowej Uniwersytetu Wrocławskiego

I. Postanowienia ogólne

§ 1

1. Uczelniana Sieć Komputerowa Uniwersytetu Wrocławskiego (USK UWr) ma na celu umożliwienie jej uprawnionym Użytkownikom dostępu do informacji niezbędnych do realizacji celów dydaktyczno-naukowych, ponadto wspiera realizację zadań związanych z zarządzaniem Uczelnią.
2. W przypadku przetwarzania danych osobowych w sieci USK UWr, należy postępować zgodnie z zarządzeniem Rektora Uniwersytetu Wrocławskiego w sprawie ochrony danych osobowych w Uniwersytecie Wrocławskim.

II. Definicje

§ 2

1. Jako Uczelnianą Sieć Komputerową Uniwersytetu Wrocławskiego rozumie się zbiór wszystkich sieci lokalnych poszczególnych jednostek oraz sieć szkieletową wraz z zasobami.
2. Jako sieć szkieletową definiuje się część sieci zapewniającą połączenia pomiędzy sieciami lokalnymi oraz sieciami zewnętrznych operatorów. Sieć szkieletowa służy wszystkim jednostkom UWr i ma za zadanie zapewnić możliwość wymiany danych zarówno pomiędzy sieciami lokalnymi, jak i pozwolić na dostęp do zewnętrznych źródeł informacji np. do ogólnoświatowej sieci Internet, zasobów danych zgromadzonych na innych uczelniach itp.
3. Zasoby są integralną częścią sieci szkieletowej. Jako zasoby definiuje się serwery wraz z udostępnianymi na nich usługami takimi jak: poczta elektroniczna, publikacje elektroniczne, konta Użytkowników, usługi ftp, news, obsługa nazw itp.
4. Jako elementy sieci definiuje się sprzęt aktywny (routery, switche, huby itp.) oraz okablowanie sieci.
5. Jako sieci lokalne definiuje się fragmenty sieci wybudowane i administrowane poprzez jednostki UWr. Sieci lokalne zapewniają wymianę danych komputerowych na terenie jednostki/komórki (wydział, instytut, dział itp.) i mogą zostać przyłączone do sieci szkieletowej w miejscu wyznaczonym przez administratora USK UWr.
6. Administratorem USK UWr jest kierownik DUI lub osoba przez niego wyznaczona.
7. Użytkownikiem USK UWr jest każda osoba, której Dział Usług Informatycznych udostępnił możliwość korzystania z sieci USK UWr.
8. Przez sieć chronioną rozumie się sieć komputerową odseparowaną od Internetu zaporą sieciową (firewall).
9. Jako adres IP (Internet Protocol address) rozumie się unikatowy numer przyporządkowany urządzeniom sieci komputerowej.

III. Uczelniana Sieć Komputerowa Uniwersytetu Wrocławskiego

§ 3

1. USK UWr tworzą:
   1/ sieć szkieletowa Uczelni,
   2/ sieci lokalne poszczególnych jednostek organizacyjnych UWr,
   3/ lokalna sieć administracji centralnej, zwana dalej „LAN-AC”,
   4/ sieć Domów Studenckich UWr, zwana dalej „siecią DS”.
2. Nadzór nad USK UWr sprawuje Dział Usług Informatycznych (DUI).

3. Sieć szkieletowa obejmuje serwery oraz infrastrukturę komunikacyjną przeznaczoną do świadczenia usług ogólnouczelnianych.
4. Sieć lokalna jednostki organizacyjnej UWr obejmuje komputery, serwery i infrastrukturę komunikacyjną danej jednostki i podlega jej kierownikowi.
5. Sieć LAN-AC obejmuje komputery, serwery i wydzieloną infrastrukturę komunikacyjną przeznaczone do obsługi administracji centralnej i podlega kierownikowi DUI.
6. Sieć DS obejmuje infrastrukturę komunikacyjną oraz serwery domów studenckich i podlega Prorektorowi ds. studenckich.
7. Kierownik DUI rozstrzyga wszelkie spory dotyczące niniejszego Regulaminu, których rozpatrzenie nie podlega właściwości władz Uczelni, bądź właściwości sądów powszechnych.
8. Kierownik DUI może, za zgodą Dyrektora ds. informatycznych, przekazać w formie pisemnej wybranym podmiotom – pracownikom lub jednostkom organizacyjnym UWr - część swoich uprawnień dotyczących zarządzania siecią.
9. Na podstawie pisemnego wniosku złożonego we właściwym trybie przez uprawnione organy państwowe, kierownik DUI jest uprawniony za wiedzą i zgodą Rektora do udostępniania uprawnionym organom danych umożliwiających identyfikację sprawców czynów zabronionych.

§ 4

1. Podłączenie lokalnej sieci komputerowej danej jednostki do sieci szkieletowej Uniwersytetu Wrocławskiego jest realizowane na wniosek jej kierownika złożony w Dziale Usług Informatycznych.
2. Kierownik jednostki organizacyjnej jest zobowiązany ustanowić wewnętrzny regulamin użytkowania sieci lokalnej, który podlega zatwierdzeniu przez kierownika DUI. Postanowienia regulaminu sieci lokalnej nie mogą być sprzeczne z ustaleniami niniejszego Regulaminu.
3. Prorektor ds. studenckich, w porozumieniu z kierownikiem DUI, ustanawia regulamin sieci DS.
4. Każda sieć lokalna podłączana do sieci szkieletowej UWr musi posiadać lokalnego administratora oraz regulamin korzystania z tej sieci.
5. Administratora sieci lokalnej powołuje kierownik jednostki organizacyjnej, której ona podlega. Dane administratora sieci lokalnej (imię, nazwisko, nr telefonu służbowego oraz adres e-mail) jednostka organizacyjna ma obowiązek przekazać do DUI w ciągu 5 dni roboczych od jego powołania. W sprawach dotyczących zachowania ciągłości, spójności i bezpieczeństwa sieci oraz współpracy na styku sieci lokalnej z siecią szkieletową administrator sieci lokalnej podlega administratorowi USK UWr.
6. Administrator sieci lokalnej ma obowiązek prowadzenia i aktualizowania na bieżąco wszelkich zmian w elektronicznej ewidencji oprogramowania swojej jednostki.
   Ewidencja oprogramowania powinna zawierać:
   1/ typ i numer ewidencyjny komputera, na którym zainstalowany jest program,
   2/ nazwę oprogramowania,
   3/ informację o posiadanej licencji (tak, nie),
   4/ fakturę zakupu (data zakupu, nr faktury).
   Administrator sieci lokalnej ma obowiązek przedstawiać ewidencję na żądanie Administratora sieci USK UWr lub organu kontrolującego legalność oprogramowania.
7. Administrator sieci lokalnej jest odpowiedzialny za eksploatację sieci lokalnej oraz przestrzeganie przez Użytkowników postanowień zawartych w § 13 niniejszego Regulaminu.
8. Administrator sieci lokalnej prowadzi konta na komputerach w swojej sieci oraz jest zobowiązany zagwarantować ochronę dostępu do USK UWr przed osobami nieuprawnionymi.
9. Administrator USK UWr ma prawo odmówić podłączenia sieci lokalnej do szkieletu sieci w przypadku, gdy nie został wyznaczony administrator sieci lokalnej do czasu jego powołania.

10. Administrator USK UWr ma prawo odłączyć sieć lokalną od sieci szkieletowej, gdy jednostka nie posiada administratora, do czasu jego powołania. O zamiarze odłączenia sieci lokalnej od sieci szkieletowej administrator USK UWr ma obowiązek pisemnie poinformować kierownika jednostki organizacyjnej, na 5 dni roboczych przed planowanym terminem odłączenia.

§ 5

1. Uczelnia nie ponosi odpowiedzialności z tytułu strat poniesionych wskutek awarii USK UWr.
2. Uczelniana Sieć Komputerowa Uniwersytetu Wrocławskiego może być użytkowana wyłącznie w zgodzie z obowiązującym prawem.
3. Za pośrednictwem USK UWr nie wolno rozpowszechniać bez zgody Rektora treści lub obrazów o charakterze komercyjnym, reklamowym, politycznym.
4. W przypadku stwierdzenia, że w sieci lokalnej USK UWr pracuje komputer w sposób niezgodny z ust. 2 lub 3, administrator sieci ma obowiązek powiadomić o tym fakcie zwierzchnika Użytkownika komputera. Administrator ma również prawo do natychmiastowego wyłączenia dostępu komputera do sieci, jeżeli w jego ocenie jest to niezbędne.
5. Jeżeli w sieci DS pracuje komputer w sposób niezgodny z ust. 2 lub 3, administrator sieci DS wyłącza dostęp do sieci i powiadamia o tym fakcie kierownika DS i kierownika DUI.

IV. Użytkownicy Uczelnianej Sieci Komputerowej Uniwersytetu Wrocławskiego

§ 6

1. Prawo do bezpłatnego konta WWW na serwerach w domenie uni.wroc.pl, konta domowego w domenie uni.wroc.pl mają:
   1/ jednostki organizacyjne,
   2/ nauczyciele akademiccy UWr,
   3/ organizacje studenckie.
2. Konto jest zakładane na pisemny wniosek uprawnionego podmiotu skierowany do kierownika DUI.
3. W przypadku ubiegania się o uzyskanie własnej nazwy (poddomeny) w domenie uni.wroc.pl Użytkownik zobowiązany jest do złożenia pisemnego wniosku do kierownika DUI.
4. Na serwerach ogólnouniwersyteckich jedna osoba może posiadać tylko jedno konto.
5. Konto Użytkownika nie może być używane do rozpowszechniania treści lub obrazów godzących w dobre imię Uniwersytetu, ani do rozpowszechniania treści lub obrazów o charakterze komercyjnym, reklamowym, politycznym.
6. Administrator danej domeny decyduje o założeniu i likwidacji kont oraz o przyznaniu i odebraniu praw Użytkownikowi w zakresie korzystania z zasobów systemu. Użytkownicy zobowiązani są do przestrzegania zaleceń administratora podczas pracy w systemie.
7. Konto Użytkownika musi być zabezpieczone hasłem lub kluczem, gwarantującym poufność danych Użytkownika oraz uniemożliwiającym korzystanie z systemu przez osoby nieuprawnione. Prawo wykorzystywania konta należy wyłącznie do jego uprawnionego Użytkownika.
8. Udostępnianie konta osobom trzecim traktowane jest jako poważne naruszenie zasad pracy w sieci. Fakt nieuprawnionego korzystania z konta przez osoby trzecie powinien być natychmiast zgłoszony administratorowi.
9. Administrator systemu dokonuje weryfikacji kont Użytkowników 2 razy w ciągu roku. Konta osób, które utraciły status pracownika oraz konta jednostek organizacyjnych (komórek administracyjnych), które utraciły swoją podmiotowość są blokowane nie później niż w dniu ustania stosunku pracy lub nie później niż w dniu utraty przez jednostkę podmiotowości.
10. W przypadku wygaśnięcia uprawnień do posiadania konta uruchamiana jest poniższa procedura likwidacji:

1/ blokowana jest możliwość wysyłania poczty elektronicznej,
2/ blokowana jest indywidualna strona WWW Użytkownika,
3/ blokowane są wszystkie uprawnienia wynikające z posiadanego konta,
4/ identyfikator konta nie zostaje ponownie przydzielony innej osobie.

11. Użytkownik konta odpowiada za wszelkie szkody wynikające z tytułu wykorzystywania kont niezgodnie z przeznaczeniem na zasadach ogólnych oraz na zasadach przewidzianych w niniejszym Regulaminie.
12. Użytkownik konta zobowiązany jest przestrzegać Regulaminu Uczelnianej Sieci Komputerowej Uniwersytetu Wrocławskiego.

§ 7

Dodatkowe zasady prowadzenia kont Użytkowników w sieciach lokalnych USK UWr mogą zostać określone w regulaminach tych sieci.

§ 8

Administratorzy mają prawo limitowania wielkości udostępnianych zasobów, z których może korzystać Użytkownik, a także w uzasadnionych przypadkach, mogą ograniczyć dostęp do usług sieciowych, operacji typu uruchomienia programu, odczytu/zapisu plików lub połączenia z innym systemem.

V. Usługi sieciowe Uczelnianej Sieci Komputerowej UWr

§ 9

1. Jednostką odpowiedzialną za funkcjonowanie podstawowych usług sieciowych i koordynującą działania dotyczące udostępniania usług sieciowych w USK UWr jest DUI.
2. Dział Usług Informatycznych utrzymuje uniwersytecki serwer nazw (DNS) dla potrzeb USK UWr. Delegacja poddomen i rejestracja nowych nazw lokalnej sieci odbywa się w porozumieniu z administratorem USK UWr.
3. W razie stwierdzenia nieprawidłowości administrator USK UWr ma prawo odmówić dołączenia serwera nazw, jak również w uzasadnionych przypadkach wyłączyć usługę.
4. Dział Usług Informatycznych utrzymuje ogólnouniwersytecki serwer poczty elektronicznej, odpowiada za jego prawidłową konfigurację i ciągłą dostępność.
5. Sieci lokalne USK UWr mogą dysponować własnymi serwerami poczty elektronicznej bądź korzystać z serwera ogólnouniwersyteckiego. Administrator USK UWr ma prawo podjąć decyzję o wyłączeniu serwisu poczty elektronicznej w sieci lokalnej po stwierdzeniu niepoprawnego funkcjonowania tej usługi.
6. Usługi typu ogólnodostępny serwer FTP, serwer WWW oraz inne serwisy oferowane w sieci USK UWr podlegają kontroli administratora USK UWr, który w szczególności może domagać się:
   1/ zagwarantowania ciągłej dostępności serwisu,
   2/ podporządkowania się obowiązującym w USK UWr zasadom bezpieczeństwa.

§ 10

1. Za stronę główną UWr odpowiada Biuro ds. Promocji.
2. Wszystkie strony WWW udostępniane przez serwery USK UWr muszą być u dołu strony oznaczone informacją o osobie/jednostce odpowiedzialnej za zawartość danej strony, w sposób pozwalający na przekazanie uwag dotyczących zawartości strony.
3. Administrator serwera głównego WWW określa warunki techniczne utrzymywania stron WWW Użytkowników.
4. Strony WWW Użytkowników służą do celów edukacyjnych i naukowych, a w przypadku jednostek organizacyjnych, jednostek organizacyjnych administracji i organizacji – do celów zgodnych z ich działalnością statutową.
5. Użytkownik jest odpowiedzialny za treści umieszczane na jego stronie WWW.

§ 11

1. W celu uruchomienia usługi forum lub listy dyskusyjnej konieczne jest określenie administratora usługi, który będzie odpowiedzialny za przestrzeganie zasad prawa oraz niniejszego Regulaminu.
2. Administrator forum lub listy dyskusyjnej ma obowiązek usuwania ze zbioru znajdujących się tam wypowiedzi treści niezgodnych z prawem, dobrymi obyczajami lub zasadami niniejszego Regulaminu.

VI. Prawa i obowiązki administratora i Użytkownika

§ 12

1. Administrator USK UWr zapewnia ochronę USK UWr oraz określa zasady zewnętrznego dostępu do usług.
2. W zakresie ochrony danych osobowych administrator USK UWr i administratorzy sieci lokalnych są zobowiązani do przestrzegania postanowień zarządzenia Rektora w sprawie ochrony danych osobowych w Uniwersytecie Wrocławskim, w szczególności do przestrzegania zaleceń Inspektora Ochrony Danych UWr.
3. Administrator USK UWr ma prawo wystąpić do administratora sieci lokalnej z zaleceniem instalacji w jego systemie wskazanych mechanizmów ochrony.
4. Administratorzy sieci lokalnych USK UWr są zobowiązani utrzymywać zapis podstawowych zdarzeń w systemie przez okres dwóch tygodni i w razie potrzeby analizować zapisy systemowe i przekazywać wyniki administratorowi USK UWr.
5. Administrator sieci lokalnej zapewnia ochronę zasobów Użytkowników za pomocą dostępnych narzędzi systemowych oraz zgodnie z procedurą antywirusową.
6. Administrator sieci lokalnej posiadającej serwer poczty elektronicznej podporządkowuje się zaleceniom administratora USK UWr w celu ochrony przed atakowaniem sieci za pośrednictwem programów obsługi poczty elektronicznej.
7. Personel obsługujący sieć ma obowiązek zachowywania tajemnicy służbowej.
8. Administrator ma prawo czasowo zablokować konto, gdy jest ono niewłaściwie chronione lub zachodzi uzasadnione podejrzenie, że jest używane przez osoby nieupoważnione.
9. Uczelniana Sieć Komputerowa Uniwersytetu Wrocławskiego nie zapewnia szyfrowania transmisji na poziomie łącza, ale administratorzy sieci lokalnych powinni udostępniać techniki umożliwiające szyfrowanie danych.
10. W przypadku stwierdzenia generowania przez komputer dołączony do USK UWr strumienia danych zakłócającego prace sieci, administrator USK UWr lub administrator sieci lokalnej ma prawo zablokować dostęp do tego komputera do czasu wyjaśnienia sprawy. O powtarzających się problemach tego typu administratorzy powiadamiają kierownika jednostki, w której znajduje się ten komputer.
11. Urządzenia dostępowe łączności bezprzewodowej mogą być podłączane do USK UWr wyłącznie w porozumieniu z administratorem USK UWr lub osobą upoważnioną przez administratora USK UWr do podejmowania takich decyzji na określonym terenie. Podłączanie urządzeń bez porozumienia będzie traktowane jako poważne naruszenie zasad bezpieczeństwa USK UWr.
12. Strony WWW zawierające formularz logowania Użytkownika nie mogą narażać danych Użytkownika na przechwycenie, a w szczególności:
    1/ cała strona musi korzystać z protokołu HTTPS,
    2/ skrypt formularza danych musi korzystać z protokołu HTTPS,
    3/ serwer obsługujący stronę musi korzystać z certyfikatu,
    4/ jeżeli serwer obsługuje wyłącznie logowanie do sieci lokalnej, to musi to być wyraźnie zaznaczone,

5/ obsługa logowania w zakresie szerszym niż do sieci lokalnej może być uruchomiona wyłącznie za zgodą administratora USK UWr, wydaną na piśmie.

§ 13

1. Użytkownicy są zobowiązani do:
   1/ przestrzegania Regulaminu USK UWr,
   2/ przestrzegania zaleceń, uwag oraz wytycznych pochodzących od administratorów sieci lokalnych oraz administratora USK UWr.
2. Użytkownikom sieci zabrania się działań sprzecznych z regulaminem oraz obowiązującym w Rzeczypospolitej Polskiej porządkiem prawnym, przyjętymi zasadami współżycia społecznego, dobrymi obyczajami oraz normami etycznymi.
3. W celu ochrony sieci Użytkownik USK UWr powinien dbać o bezpieczeństwo swojego konta, w szczególności chronić swoje hasło i inne dane służące do uwierzytelnienia.
4. Użytkownik nie może żądać zmiany hasła czy otwarcia zablokowanego dostępu drogą telefoniczną, jeżeli nie ma możliwości identyfikacji dzwoniącego.
5. Zabrania się Użytkownikowi USK UWr:
   1) odstępowania uprawnień dotyczących posiadanego konta innym osobom,
   2) podejmowania prób wykorzystania obcego konta i uruchamiania aplikacji deszyfrujących hasła,
   3) prowadzenia działań mających na celu podsłuchiwanie lub przechwytywanie informacji przepływającej w sieci,
   4) zmiany adresu sprzętowego karty sieciowej lub przydzielonego adresu IP (z wyjątkiem sytuacji uzgodnionych z administratorem odpowiedniej sieci),
   5) uruchamiania aplikacji, które mogą zakłócać lub destabilizować pracę systemu lub sieci komputerowej, bądź naruszyć prywatność zasobów systemowych,
   6) nieuprawnionej rozbudowy sieci m.in. niedozwolone jest uruchamianie urządzeń i programów świadczących usługę DHCP (np. router bezprzewodowy, router przewodowy),
   7) ręcznej konfiguracji adresu IP w urządzeniu sieciowym lub końcowym bez pisemnej zgody administratora,
   8) zmian w lokalizacji urządzeń będących w jego użytkowaniu bez pisemnego poinformowania administratora,
   9) dezorganizowania pracy innych Użytkowników sieci,
   10) wykorzystywania służbowych kont w celach zarobkowych,
   11) gromadzenia, rozpowszechniania i udostępniania materiałów sprzecznych z prawem, dobrymi obyczajami oraz etyką,
   12) instalowania i uruchamiania oprogramowania: utrudniającego wykorzystywanie sprzętu, oprogramowania i zasobów sieci innym Użytkownikom; uszkadzającego lub narażającego na uszkodzenia sprzęt komputerowy; bez ważnej licencji,
   13) podejmowania działań mających na celu niezgodne z obowiązującym prawem udostępnianie, kopiowanie, rozpowszechnianie wytworów objętych prawem autorskim,
   14) przetwarzania danych osobowych, niezgodnie z ustawą o ochronie danych osobowych oraz z zarządzeniem Rektora Uniwersytetu Wrocławskiego w sprawie ochrony danych osobowych w Uniwersytecie Wrocławskim,
   15) podejmowania działań mogących narazić na uszczerbek dobre imię Uczelni,
   16) wysyłania masowej poczty kierowanej do losowych odbiorców (spam).
6. W przypadku nieprzestrzegania powyższych zasad przez Użytkownika, administrator sieci lokalnej lub administrator USK UWr może czasowo ograniczyć lub zablokować dostęp do sieci.
7. O naruszeniu obowiązujących zasad użytkowania USK UWr powiadamiany jest przełożony Użytkownika, a w przypadku studentów i doktorantów - dziekan.

8. Złamanie regulaminu pociąga za sobą odpowiedzialność Użytkowników z tego tytułu, według postanowień regulaminu.
9. Złamanie regulaminu, stanowiące naruszenie prawa będzie zgłaszane przez administratorów właściwym organom.
10. Użytkownicy sieci mają prawo do:
    1) zgłaszania administratorom uwag i wniosków dotyczących działania sieci,
    2) składania wyjaśnień dotyczących złamania regulaminu,
    3) korzystania z USK UWr w zakresie przewidzianym przez regulamin oraz przyjęte wewnętrzne akty prawne UWr.

VII. Sankcje związane z naruszeniem regulaminu

§ 14

1. Wobec Użytkownika, który dopuścił się naruszenia regulaminu, DUI może zastosować, w zależności od wagi naruszenia, następujące sankcje:
    1/ pisemne ostrzeżenie od kierownika Zespołu Infrastruktury Teleinformatycznej,
    2/ pisemne ostrzeżenie od Kierownika DUI,
    3/ czasową utratę uprawnień Użytkownika USK UWr na okres 1 miesiąca,
    4/ czasową utratę uprawnień Użytkownika USK UWr na okres 3 miesięcy,
    5/ czasową utratę uprawnień Użytkownika USK UWr na okres jednego semestru,
    6/ czasową utratę uprawnień Użytkownika USK UWr na okres roku akademickiego,
    7/ bezterminową utratę uprawnień Użytkownika USK UWr.
2. Użytkownik, który dopuścił się naruszenia regulaminu lub innych powszechnie obowiązujących przepisów prawa, zobowiązany jest do złożenia Kierownikowi DUI pisemnych wyjaśnień, w terminie 7 dni od dnia otrzymania wezwania. Nie złożenie wyjaśnień w terminie powoduje zablokowanie praw Użytkownika do czasu ich złożenia.
3. Od decyzji o zablokowaniu praw Użytkownikowi przysługuje prawo wniesienia odwołania. Odwołanie wnoszone jest do Dyrektora ds. informatycznych i powinno zawierać w szczególności wyjaśnienie okoliczności naruszenia regulaminu lub innych powszechnie obowiązujących przepisów prawa.
4. Dyrektor ds. informatycznych rozpatruje odwołanie w terminie 14 dni kalendarzowych od daty jego wpływu. Brak odpowiedzi w ww. terminie oznacza, iż sankcja została utrzymana.
5. Zastosowanie sankcji, o których mowa w ust. 2 nie zwalnia Użytkownika z odpowiedzialności wynikającej z odrębnych przepisów, w szczególności z kodeksu karnego.

Załącznik Nr 4
do Regulaminu

Regulamin Lokalnej Sieci Komputerowej Administracji Centralnej Uniwersytetu Wrocławskiego

Postanowienia Ogólne

§ 1

1. Jako sieć LAN-AC rozumie się lokalną sieć komputerową administracji centralnej, zwaną dalej „LAN-AC".
2. Sieć LAN-AC oraz serwery tej sieci znajdują się pod zarządem Zespołu Infrastruktury Teleinformatycznej DUI.
3. Siecią LAN-AC administruje wyznaczony przez Kierownika DUI pracownik lub pracownicy Zespołu Infrastruktury Teleinformatycznej DUI, zwany administratorem LAN-AC.
4. Konto Użytkownika LAN-AC zakłada, modyfikuje, likwiduje oraz nadaje i zmienia prawa dostępu administrator LAN-AC, na pisemny wniosek kierownika jednostki organizacyjnej administracji centralnej. We wniosku kierownik powinien określić zakres uprawnień dla Użytkownika.
5. Nadanie uprawnień dostępu do danych osobowych musi być uzgodnione z lokalnym administratorem danych osobowych odpowiedzialnym za tę bazę danych.
6. W przypadku przetwarzania danych osobowych w sieci LAN-AC, należy postępować zgodnie z zarządzeniem Rektora Uniwersytetu Wrocławskiego w sprawie ochrony danych osobowych w Uniwersytecie Wrocławskim.
7. Administrator LAN-AC ma prawo zablokować konto osoby łamiącej regulamin do czasu rozpatrzenia sprawy przez kierownika jednostki organizacyjnej administracji centralnej.
8. Użytkownik lokalnej sieci komputerowej Administracji Centralnej, która jest częścią Uczelnianej Sieci Komputerowej, zwanej dalej „USK" jest także jednocześnie indywidualnym Użytkownikiem USK. Indywidualny Użytkownik USK zobowiązany jest do przestrzegania postanowień Regulaminu USK.
9. Użytkownicy nieprzestrzegający regulaminu i innych zarządzeń Rektora mogą zostać pozbawieni prawa dostępu do sieci LAN-AC.

§ 2

Użytkownicy LAN-AC zobowiązani są do przestrzegania i krzewienia dobrych obyczajów, a w szczególności do:

1/ zgłaszania administratorom LAN-AC nieprawidłowości w działaniu komputerów lub programów;
2/ nieobciążania bez istotnej potrzeby komputerów;
3/ oszczędnego używania urządzeń, których eksploatacja jest kosztowna (np. drukarek).

Obowiązki Użytkownika Sieci Komputerowej

§ 3

Użytkownik LAN-AC zobowiązany jest do:

1/ zapoznania się z regulaminem korzystania z LAN-AC;
2/ przestrzegania postanowień regulaminu LAN-AC i innych zarządzeń Rektora;
3/ podporządkowywania się zaleceniom administratorów LAN-AC;
4/ dbania o ochronę dostępu do własnego konta;
5/ natychmiastowego zgłaszania luk w systemie praw dostępu. Zgłoszenie luk nie pociąga negatywnych następstw dla Użytkownika;
6/ zgłaszania drogą elektroniczną (pocztą e-mail lub poprzez stronę WWW) wszelkich awarii komputerów, sieci lub oprogramowania, o ile jest to technicznie możliwe;
7/ uzgadniania z administratorem LAN-AC możliwości i zasad pracy w LAN-AC po godzinach pracy i w dni wolne od pracy;

8/ zgłaszania administratorowi LAN-AC spraw wyjątkowych (np. gdy konieczne jest naruszenie któregoś z postanowień regulaminu LAN-AC lub zarządzenia Rektora);
9/ zapisywania wszelkich wytworzonych w ramach swojego zakresu obowiązków danych w specjalnie dla tego utworzonym katalogu na serwerze.

Prawa Użytkownika Lokalnej Sieci Komputerowej

§ 4

Użytkownik LAN-AC ma prawo do:
1/ korzystania z zasobów LAN-AC w granicach określonych przez administratorów LAN-AC. Administratorzy ustalając zakres uprawnień Użytkownika kierują się zasadami określonymi przez kierowników jednostek organizacyjnych administracji centralnej oraz lokalnych administratorów danych osobowych;
2/ ochrony prywatności danych przechowywanych w systemach komputerowych włączonych do LAN-AC;
3/ zmiany uprawnień w sieci, jeśli zaistnieje uzasadniona potrzeba. Zmiany dokonuje administrator LAN-AC na wniosek kierownika jednostki organizacyjnej administracji centralnej;
4/ zapoznawania się z programami i sprzętem na zasadach określonych przez kierownictwo Uczelni;
5/ odwoływania się do administratora LAN-AC, w przypadku otrzymywania poleceń łamiących regulamin LAN-AC;
6/ zapisywania na dyskach lokalnych, za zgodą kierownika jednostki organizacyjnej administracji centralnej, danych które nie łamią przepisów prawa autorskiego oraz innych regulacji prawnych, nie związanych z zakresem obowiązków danego Użytkownika. Zabezpieczenie tych danych w przypadku konieczności reinstalacji komputera należy do Użytkownika;
7/ korzystania z udostępnionych zasobów sieciowych, plików oraz drukarek lokalnym Użytkownikom (w obrębie działu) po uzgodnieniu tego faktu z administratorem LAN-AC.

Czynności zabronione

§ 5

Użytkownikowi LAN-AC zabrania się:
1/ utrudniania pracy administratorom i innym Użytkownikom;
2/ dezinformowania administratorów i innych Użytkowników;
3/ używania identyfikatorów i haseł innych Użytkowników;
4/ korzystania z komputerów, zasobów i informacji, do których administrator LAN – AC nie przydzielił Użytkownikowi prawa dostępu;
5/ dokonywania zmian w konfiguracji sprzętu oraz w oprogramowaniu bez uzgodnienia z administratorem;
6/ instalowania i uruchamiania oprogramowania:
   a/ utrudniającego wykorzystywanie sprzętu (np. programy wirusowe),
   b/ uszkadzającego lub narażającego na uszkodzenia sprzęt komputerowy,
   c/ na które brak licencji;
   Uruchomienia usług sieciowych (np. serwis WWW, ftp, poczta) dokonuje administrator LAN-AC na serwerach centralnych. Nieuzgodnienie z administratorem uruchomienia usług powoduje wyłączenie komputera z sieci do czasu usunięcia usług;
7/ wykorzystywania sprzętu, sieci lub oprogramowania LAN-AC do celów komercyjnych, bez zgody władz Uczelni;
8/ wykorzystywania sprzętu, oprogramowania i zasobów LAN-AC do zadań, które nie są związane ze statutowym zakresem jednostki (np. uruchamiania gier sieciowych);
9/ udostępniania komputera, na którym jest w danym momencie dostęp do zasobów LAN-AC, osobom nieposiadającym uprawnień do korzystania z tych zasobów;

10/pracowania równocześnie w sieci Internet oraz z programami korzystającymi z baz danych umieszczonych w sieci LAN-AC;
11/przetwarzania danych osobowych niezgodnie z przepisami prawnymi o ochronie danych osobowych, w tym zarządzeniem Rektora Uniwersytetu Wrocławskiego w sprawie ochrony danych osobowych w Uniwersytecie Wrocławskim.

Załącznik Nr 5
do Regulaminu

Regulamin Korzystania z Usługi MS Office365 W Uniwersytecie Wrocławskim

Postanowienia ogólne

§ 1

Ilekroć w niniejszym Regulaminie jest mowa o:

Użytkowniku – oznacza to osobę fizyczną korzystającą z usługi po zalogowaniu się do niej (pracownik, student, doktorant, słuchacz);

koncie Użytkownika – oznacza to zbiór zasobów i uprawnień przypisanych Użytkownikowi w ramach usługi. Konto posiada unikalną nazwę i hasło;

logowaniu – oznacza to proces autoryzacji wymagający podania nazwy konta Użytkownika i hasła.

§ 2

1. Niniejszy Regulamin określa zasady korzystania z konta Użytkownika otrzymanego w ramach usługi MS Office365 w Uniwersytecie Wrocławskim.
2. W ramach usługi MS Office365 Użytkownik otrzymuje dostęp do:
   1/ programów Word, Excel, Power Point, OneNote w wersji Office Web Apps,
   2/ skrzynki pocztowej na serwerze o wielkości 50 GB oraz wspólnych kalendarzy,
   3/ narzędzi umożliwiających tworzenie stron internetowych i blogów,
   4/ wirtualnego dysku w usłudze OneDrive o wielkości 1 TB do przechowywania dokumentów, prezentacji, zdjęć,
   5/ narzędzia umożliwiającego nawiązanie połączenia głosowego, chatu, wideokonferencji.
3. Obowiązek posiadania konta Użytkownika w usłudze MS Office365 posiadają:
   1/ pracownicy Uniwersytetu Wrocławskiego;
   2/ studenci, doktoranci i słuchacze Uniwersytetu Wrocławskiego.
4. Konto pracownika w usłudze MS Office 365 jest kontem służbowym, wykorzystywanym do pracy w Uniwersytecie Wrocławskiem. Konto pracownika służy także do kontaktu pracodawcy z pracownikiem.
5. Konto studenta, słuchacza lub doktoranta w usłudze MS Office365 wykorzystywane jest przez Użytkownika w celach realizacji usług edukacyjnych. Konto studenta, słuchacza lub doktoranta służy także do kontaktu z jego Użytkownikiem.

§ 3

1. Usługa MS Office365 posiada mechanizmy zabezpieczające przed nieautoryzowanym dostępem przez osoby trzecie. Zastosowane rozwiązania umożliwiają szyfrowane logowanie oraz komunikację z serwerem pocztowym, pod warunkiem odpowiedniego skonfigurowania programów stosowanych przez Użytkownika do obsługi konta poczty elektronicznej, zgodnie z Instrukcją Użytkownika, umieszczoną na stronie internetowej pod adresem: http://www.office365.uni.wroc.pl/.
2. Dostęp do konta Użytkownika jest chroniony hasłem. Z uwagi na konieczność zapewnienia bezpieczeństwa konta poczty elektronicznej oraz danych zgromadzonych przez Użytkownika, hasło musi być chronione i poufne. W przypadku podejrzenia utraty poufności hasła, należy niezwłocznie zmienić je na nowe.
3. Hasło musi spełniać następujące warunki:
   1/ zawierać co najmniej 8 znaków, alfanumerycznych oraz
   2/ zawierać co najmniej 1 dużą literę alfabetu polskiego [A,B,…,Z] oraz
   3/ zawierać co najmniej 1 małą literę alfabetu polskiego [a,b,…,z] oraz
   4/ zawierać co najmniej 1 cyfrę [0,1,…,9] oraz 1 znak specjalny [!, @, ^, &, (,), %, $, #, *].
4. Instrukcja informująca o sposobie dokonywania zmiany hasła dostępna jest na stronie internetowej pod adresem: http://www.office365.uni.wroc.pl/.

Użytkowanie Konta

§ 4

1. Dostęp do konta Użytkownika w usłudze MS Office365 możliwy jest za pomocą przeglądarki internetowej poprzez stronę internetową: http://portal.office.com/.
2. Każdy z Użytkowników ma obowiązek samodzielnie skonfigurować pocztę na podstawie Instrukcji dostępnej na stronie internetowej pod adresem: http://www.office365.uni.wroc.pl/.

§ 5

1. Szczegółowy opis obsługi usługi MS Office365 przez Użytkownika zawiera Instrukcja Użytkownika umieszczona na stronie internetowej pod adresem: http://www.office365.uni.wroc.pl/.
2. Użytkownik korzystający z usługi MS Office365 ma możliwość przenoszenia danych ze skrzynki pocztowej znajdujące się na serwerze lokalnym. Sposób przenoszenia danych znajduje się na stronie pod adresem: http://www.office365.uni.wroc.pl/.
3. Użytkownik korzystający z usługi MS Office365 ma możliwość przekierowywania wiadomości z dotychczasowej lokalnej skrzynki pocztowej na nowe konto pocztowe w domenie www.uwr.edu.pl. Włączenia usługi przekierowywania dokonują administratorzy poszczególnych serwerów pocztowych.

§ 6

Zaleca się Użytkownikom okresowe wykonywanie kopii zapasowych poczty znajdującej się na własnym komputerze, tj. archiwizowania, kompaktowania poczty oraz archiwizowania ustawień klienta pocztowego i książki adresowej.

§ 7

1. Użytkownik może zgłaszać uwagi, komentarze oraz pytania dotyczące jakości działania serwisu poczty elektronicznej pod adresem: helpdesk@uwr.edu.pl.
2. Użytkownik będzie otrzymywać na adres konta email korespondencje istotne z punktu widzenia działalności Uniwersytetu lub systemu poczty elektronicznej.

§ 8

1. Użytkownik ma prawo korzystać z konta Użytkownika w usłudze MS Office365 w pełnym zakresie jego funkcjonalności przestrzegając obowiązującego prawa, norm społecznych i obyczajowych w Polsce.
2. Korzystając z konta Office365, Użytkownik zobowiązuje się, że nie będzie działał w sposób naruszający prawa innych Użytkowników oraz nie będzie przenosił prawa do korzystania ze swojego konta Użytkownika na inne osoby.

§ 9

Użytkownik ponosi odpowiedzialność za treść i zawartość swojego konta w usłudze MS Office365.

Zasady odpowiedzialności

§ 10

Uniwersytet zastrzega sobie prawo do:

1/ zmiany zasad funkcjonowania usługi MS Office365 (w tym poczty elektronicznej). Zmiany będą podawane do wiadomości Użytkownikom za pomocą poczty elektronicznej. Aktualna i obowiązująca treść zasad jest dostępna na stronach internetowych pod adresem: http://www.office365.uni.wroc.pl/,

2/ zamykania kont osób, które przestają być pracownikami Uniwersytetu Wrocławskiego, z dniem rozwiązania umowy,

3/ zablokowania konta w przypadkach wykorzystania go w sposób niezgodny z przeznaczeniem, w szczególności w sytuacjach:

a/ odstępowania uprawnień dotyczących posiadanego konta innym osobom,

b/ wykorzystywania bezpłatnych kont w celach zarobkowych,
c/ rozpowszechniania i udostępniania materiałów sprzecznych z prawem lub dobrymi obyczajami akademickimi,
d/ podejmowania działań mających na celu niezgodne z obowiązującym prawem udostępnianie, kopiowanie, rozpowszechnianie utworów objętych prawem autorskim,
e/ przetwarzania danych osobowych niezgodnie z ustawą o ochronie danych osobowych oraz z zarządzeniem w sprawie ochrony danych osobowych w Uniwersytecie Wrocławskim,
f/ podejmowania działań mogących narazić na uszczerbek dobre imię Uczelni,
g/ wysyłania masowej poczty kierowanej do losowych odbiorców (spam).

§ 11

Uniwersytet nie ponosi odpowiedzialności za:
1/ skutki wejścia przez osoby trzecie w posiadanie hasła umożliwiającego korzystanie z konta Użytkownika w usłudze MS Office365,
2/ utratę danych spowodowaną awarią sprzętu, lub innymi okolicznościami niezależnymi od Uniwersytetu,
3/ przerwy w funkcjonowaniu usługi MS Office365 zaistniałe z przyczyn technicznych spowodowanych w szczególności konserwacją lub wymianą sprzętu,
4/ treści przesyłane i przechowywane w usłudze MS Office365.

Helpdesk i rozwiązywanie problemów

§ 12

1. Dział Usług Informatycznych sprawuje nadzór i opiekę techniczną nad systemem poczty elektronicznej, a także zapewnia opiekę i wsparcie w zakresie problemów z logowaniem się do usługi MS Office365 dla administratorów lokalnych, w dni robocze w godzinach 8:30 – 15:30, zgodnie z informacjami umieszczonymi na stronie internetowej pod adresem: http://www.office365.uni.wroc.pl/.
2. Firma Microsoft zapewnia opiekę i wsparcie w zakresie obsługi pakietu Office365 i problemów z dostępem do usług po zalogowaniu.

   w języku polskim : poniedziałek – piątek w godzinach 8:00 – 16:00
   w języku angielskim : 24 h, 7 dni w tygodniu

   Numery telefonów: 0048 800 70 23 20
   0048 223 06 05 17

   Kontakt email: plisvd@microsoft.com.
3. Administratorzy zapewniają opiekę i wsparcie, odpowiednio dla pracowników, studentów, słuchaczy i doktorantów, w dni robocze w godzinach 8:30-15:30, w zakresie wystąpienia problemów w trakcie:
   a/ logowania się do portalu http://portal.office.com;
   b/ zmiany hasła w usłudze Office365, zgodnie z informacjami opublikowanymi na stronie http://www.office365.uni.wroc.pl/;
   c/ obsługi pakietu Office365 i problemów z dostępem do usług po zalogowaniu, zgodnie z informacjami opublikowanymi na stronie projektu http://www.office365.uni.wroc.pl/.

   Wykaz administratorów wraz z danymi kontaktowymi dostępny jest na stronie internetowej pod adresem http://www.office365.uni.wroc.pl/.

Załącznik Nr 6
do Regulaminu

Zasady tworzenia adresów poczty elektronicznej w Uniwersytecie Wrocławskim

§ 1

1. Obowiązek posiadania (służbowego) konta poczty elektronicznej w domenie uwr.edu.pl mają:
   1/ wydziały oraz jednostki pozawydziałowe;
   2/ pracownicy Uniwersytetu Wrocławskiego;
   3/ osoby funkcyjne;
   4/ studenci, doktoranci i słuchacze Uniwersytetu Wrocławskiego.
2. Dział Usług Informatycznych administruje nadanym kontem poczty elektronicznej.
3. Zobowiązuje się wszystkich pracowników Uczelni do posługiwania się nadanym kontem do prowadzenia elektronicznej korespondencji służbowej oraz do regularnego sprawdzania poczty elektronicznej.
4. Nauczyciele akademiccy mają możliwość posiadania również dotychczasowego konta na serwerze pocztowym znajdującym się w zasobach lokalnych Uniwersytetu Wrocławskiego.
5. Informacja o służbowym adresie e-mail pracownika, osoby sprawującej funkcję w Uniwersytecie Wrocławskim oraz jednostki organizacyjnej jest jawna i dostępna powszechnie w tym, na stronie internetowej Uniwersytetu.

§ 2

1. Wydziały oraz jednostki pozawydziałowe mają obowiązek posiadania ogólnego adresu e-mail w domenie uwr.edu.pl. Adres e-mail jednostki nie jest kontem, lecz grupą dystrybucyjną - poczta wysyłana na ten adres jest automatycznie kierowana na konta osób wskazanych przez kierownika na stosownym formularzu znajdującym się na stronie internetowej pod adresem www.uwr.edu.pl/office365.
2. Adres email jednostki organizacyjnej ma postać: symbolorganizacyjny@uwr.edu.pl.
3. Jednostki organizacyjne administracji nie mają obowiązku posiadania ogólnego adresu e-mail w domenie uwr.edu.pl. Na pisemny wniosek kierownika, Dział Usług Informatycznych przydziela jednostce organizacyjnej administracji ogólny adres e-mail, który otrzymuje postać: symbolorganizacyjny@uwr.edu.pl. Adres e-mail jednostki organizacyjnej administracji nie jest kontem, lecz grupą dystrybucyjną - poczta wysyłana na ten adres jest automatycznie kierowana na konta osób wskazanych przez kierownika na stosownym formularzu znajdującym się na stronie internetowej pod adresem www.uwr.edu.pl/office365. Informacja o służbowym adresie e-mail jednostki organizacyjnej administracji jest jawna i dostępna powszechnie, w tym na stronie internetowej Uniwersytetu.
4. Na pisemny wniosek kierownika jednostki organizacyjnej administracji lub jednostki organizacyjnej Dział Usług Informatycznych przydziela ogólny adres e-mail, np. promocja@uwr.edu.pl. Informacja o adresie e-mail jest jawna i dostępna powszechnie, w tym na stronie internetowej Uniwersytetu.
5. Odbieranie poczty nadsyłanej na konto jednostki organizacyjnej oraz posługiwanie się nim we wszelkiej elektronicznej korespondencji służbowej jest obowiązkowe.
6. Adresy e-mail jednostek organizacyjnych Uczelni przydziela Administrator Systemu Office365.
7. Adresy osób funkcyjnych są tworzone na identycznych zasadach jak adresy jednostek organizacyjnych.
8. Adresy dziekanów tworzone są według wzoru: dsymbolorganizacyjnywydziału@uwr.edu.pl.

§ 3

Nowoprzyjęci pracownicy informacje o koncie mailowym otrzymują w Dziale Spraw Pracowniczych, w trakcie przyjęcia do pracy. Konto staje się aktywnie od pierwszego dnia zatrudnienia, a dezaktywuje się automatycznie po ostatnim dniu pracy.

Załącznik Nr 7
do Regulaminu

Regulamin korzystania z systemu obsługi zgłoszeń informatycznych Logsystem

§ 1

1. Logsystem jest systemem typu Helpdesk, umożliwiającym koordynację wsparcia informatycznego udzielanego:
   1/ pracownikom Uniwersytetu Wrocławskiego,
   2/ studentom i doktorantom Uniwersytetu Wrocławskiego,
   3/ pozostałym osobom korzystającym z centralnych systemów informatycznych UWr.
2. System Logsystem zarządza zgłoszeniami Użytkowników dotyczącymi wszelkich problemów powstałych podczas pracy z następującymi systemami informatycznymi:
   1/ MS Office365,
   2/ EGERIA,
   3/ TETA BI,
   4/ TETA EDU,
   5/ EZD,
   6/ PKZP,
   7/ Portal Pracowniczy

   oraz problemów związanych z eksploatacją sprzętu komputerowego i sieciowego administrowanego przez Dział Usług Informatycznych.

§ 2

1. Zgłoszenia incydentów oraz problemów dokonuje się poprzez platformę helpdesk Logsystem:
   1/ stronę internetową: https://www.pomoc.uwr.edu.pl
   Na wskazanej stronie, po zalogowaniu, można śledzić postęp realizacji poszczególnych zgłoszeń. Logowanie do systemu Logsystem odbywa się z wykorzystaniem danych dostępowych do konta w domenie @uwr.edu.pl Wszystkie zgłoszenia zarejestrowane na platformie helpdesk Logsystem będą rozwiązywane w pierwszej kolejności;
   2/ wysyłając e-mail na jeden ze wskazanych poniżej adresów:
   helpdesk@uwr.edu.pl – dla studentów
   pomoc@uwr.edu.pl – dla pracowników.
2. Więcej informacji o systemie Logsystem można znaleźć na stronie internetowej www.uni.wroc.pl w zakładce „Informatyzacja”.

§ 3

1. Zgłoszenie do systemu Logsystem powinno zawierać:
   1/ hasłowy opis problemu zawierający scenariusz powstawania / generowania incydentu lub problemu,
   2/ załączniki; np. zrzut ekranu z błędem, raport z zaznaczonym błędem, itp.
2. Zgłoszenie zawierające niepełne informacje, wymagane do zdiagnozowania incydentu lub problemu będzie odsyłane do Zgłaszającego celem uzupełnienia.
3. Pracownicy Działu Usług Informatycznych, przydzieleni do rozwiązania danego zgłoszenia, komunikują się ze zgłaszającym poprzez system Logsystem (poprzez email lub komentarz w zgłoszeniu).
4. Każde zgłoszenie zarejestrowane w systemie Logsystem zawiera pełną historię korespondencji pomiędzy zgłaszającym, a pracownikiem Działu Usług Informatycznych, przydzielonym do rozwiązania zgłoszonego problemu – tj. załączniki lub notatki wewnętrzne dokumentujące etapy rozwiązywania zgłoszonego problemu.

§ 4

Zgłoszenia dotyczące incydentów i problemów, przekazywane do Działu Usług Informatycznych z pominięciem systemu Logsystem, nie będą przyjmowane do realizacji.

Załącznik Nr 8
do Regulaminu

Zasady zgłaszania awarii sprzętu komputerowego i oprogramowania oraz przeprowadzania czynności serwisowych w jednostkach organizacyjnych administracji centralnej

1. Awarie sprzętu komputerowego i oprogramowania jednostek organizacyjnych administracji centralnej zgłaszają administratorom lokalnej sieci komputerowej poprzez system Logsystem.
2. Wykonawca realizujący naprawy, przeglądy techniczne, konserwacje, czyszczenia lub modernizację sprzętu, zwane dalej czynnościami serwisowymi ma obowiązek przystąpić do usuwania awarii tego samego dnia roboczego, jeśli awaria zostanie zgłoszona do godz. 12 oraz na drugi dzień roboczy, jeśli awaria zostanie zgłoszona po godz. 12.
3. Wykonawca ma obowiązek usunąć awarię w terminie pięciu dni roboczych.
4. Wykonawca nie dokonuje napraw i modernizacji sprzętu komputerowego objętego gwarancją.
5. Wykonawca czynności serwisowych uzgadnia termin przeprowadzania powyższych czynności z kierownikiem danej jednostki administracji centralnej.
6. Przeprowadzanie czynności serwisowych po godzinach pracy jednostki wymaga zgody jej kierownika. Kierownik jednostki organizacyjnej administracji centralnej informuje pracownika Działu Ochrony Mienia obsługującego portiernię o udzieleniu zgody i terminach przebywania w pomieszczeniach pracowników Wykonawcy.
7. Każdorazowe przeprowadzenie czynności serwisowych Wykonawca odnotowuje *w karcie przeglądu technicznego, konserwacji i czyszczenia*, której wzór stanowi Załącznik Nr 1 do niniejszych zasad. Kierownik jednostki organizacyjnej administracji centralnej potwierdza wykonanie usługi poprzez złożenie podpisu *na karcie przeglądu technicznego, konserwacji i czyszczenia.*
8. Materiały niezbędne do wykonania czynności serwisowych Wykonawca dostarcza i nabywa na własny koszt.
9. Wydanie sprzętu komputerowego Wykonawcy, celem przeprowadzenia czynności serwisowych poza budynkiem danej jednostki organizacyjnej administracji centralnej, wymaga wypełnienia *formularza wydania sprzętu*, zwanego dalej formularzem wydania, którego wzór stanowi Załącznik Nr 2 do niniejszych zasad. Formularz wydania podpisują: Wykonawca, kierownik jednostki organizacyjnej administracji centralnej oraz osoba odpowiedzialna materialnie za wydawany sprzęt. Kopie formularza wydania kierownik jednostki przekazuje, najpóźniej w następnym dniu roboczym, administratorom lokalnej sieci komputerowej oraz osobie materialnie odpowiedzialnej za wydany sprzęt.
10. Wynosząc sprzęt komputerowy poza daną jednostkę organizacyjną administracji centralnej, Wykonawca zobowiązany jest do wymontowania i przekazania kierownikowi jednostki wszystkich nośników danych osobowych lub usunięcia danych w sposób uniemożliwiający ich odzyskanie.
11. Kierownik jednostki organizacyjnej administracji centralnej oraz osoba materialnie odpowiedzialna za sprzęt potwierdza na formularzu wydania zwrot sprzętu komputerowego przez Wykonawcę.
12. Lokalni administratorzy sieci komputerowej mają obowiązek kontrolowania i zabezpieczania prawidłowości przebiegu czynności serwisowych w podległych systemach informatycznych.

Załącznik Nr 1
do zasad

SPRZĘT KOMPUTEROWY **- KARTA PRZEGLĄDU TECHNICZNEGO, KONSERWACJI I CZYSZCZENIA**

Nazwa jednostki: ……

Adres, nr pokoju: ……

Kierownik jednostki: ……

Nazwa sprzętu	Nr inwentarzowy - podstawowy	Data przeglądu technicznego, konserwacji i czyszczenia	Podpis Wykonawcy	Podpis Kierownika jednostki	Uwagi

Data, pieczęć i czytelny podpis Kierownika jednostki organizacyjnej administracji centralnej

Załącznik Nr 2
do zasad

Formularz wydania sprzętu

data wydania .....

Nazwa jednostki organizacyjnej ac: ..... tel.: .....
Adres: ..... pok.: .....
Rodzaj sprzętu:

☐ Jednostka centralna - nr inwentarzowy: .....

☐ Monitor - nr inwentarzowy: .....

☐ Klawiatura - nr inwentarzowy: .....

☐ Myszka - nr inwentarzowy: .....

☐ Drukarka - nr inwentarzowy: .....

☐ Skaner - nr inwentarzowy: .....

☐ Inne: .....

Sprzęt jest zabierany w celu dokonania:

☐ reinstalacji systemu

☐ naprawy przez firmę obsługującą Administrację Centralną

☐ naprawy gwarancyjnej przez firmę: .....

☐ inne: .....

☐ przeniesienia sprzętu z .....
do .....

.....	.....	.....
pieczęć i czytelny podpis osoby przyjmującej sprzęt	czytelny podpis osoby odpowiedzialnej materialnie za sprzęt	pieczęć i czytelny podpis osoby wydającej sprzęt

---

data zdania .....

Uwagi:
.....
.....
.....
.....
.....
.....
.....
.....
.....

.....	.....	.....
pieczęć i czytelny podpis osoby przyjmującej sprzęt	czytelny podpis osoby odpowiedzialnej materialnie za sprzęt	pieczęć i czytelny podpis osoby zdającej sprzęt

Załącznik Nr 9
do Regulaminu

Regulamin bezpieczeństwa informatycznego dla urządzeń mobilnych w Uniwersytecie Wrocławskim

§ 1
Postanowienia ogólne

1. Ilekroć w Regulaminie jest mowa o **urządzeniach mobilnych** oznacza to przede wszystkim: telefony, tablety, smartphony działające pod systemami operacyjnymi w wersji mobilnej między innymi Android, iOS i Windows.
2. Niniejszy Regulamin określa zasady bezpieczeństwa informatycznego dla wszystkich służbowych urządzeń mobilnych użytkowanych przez pracowników Uniwersytetu Wrocławskiego, którzy wnioskują lub posiadają dostęp do aplikacji UWr za pośrednictwem sieci przewodowych lub wnioskują o dostęp do bezprzewodowego WiFi.
3. Niniejszy Regulamin nie dotyczy sieci bezprzewodowej Eduroam.
4. Każde służbowe urządzenie mobilne, które uzyska dostęp do sieci komputerowej UWr należy opisać i wprowadzić do centralnej bazy danych urządzeń mobilnych.
5. Administrator lokalnej sieci komputerowej, zwany dalej **Administratorem lokalnym**, zobowiązany jest wprowadzić do bazy danych urządzeń mobilnych następujące informacje: nazwę urządzenia, dane Użytkownika urządzenia, numer seryjny urządzenia, numer IMEI urządzenia i adres MAC karty sieciowej urządzenia.
6. W przypadku urządzeń niespełniających wymagań technicznych wskazanych w § 2 lub wymagań formalnych zawartych w § 3, Administrator lokalny lub Administrator uczelnianej sieci komputerowej mają prawo zdalnie zablokować dostęp tego urządzenia mobilnego do zasobów sieci komputerowej UWr.
7. Przed podłączeniem urządzenia do sieci komputerowej UWr, Administrator lokalny ma obowiązek zainstalować licencjonowaną aplikację antywirusową, a urządzenie powinno spełniać wymagania techniczne określone w § 2.
8. Wnioskując o podłączenie służbowego urządzenia mobilnego do sieci komputerowej UWr Użytkownik automatycznie wyraża zgodę na instalację aplikacji antywirusowej w urządzeniu, na lokalizację urządzenia przez GPS, na zdalne blokowanie i odblokowywanie ekranu przez Administratora lokalnego w sytuacjach kryzysowych i na zdalne przywracanie ustawień fabrycznych urządzenia.
9. Aplikacja antywirusowa monitoruje zainstalowane na urządzeniu aplikacje, ustawione zabezpieczenia, wysyłane i odbierane wiadomości tekstowe oraz wykonywane połączenia.

§ 2
Wymagania techniczne

1. Urządzenia mobilne łączące się z zasobami sieci komputerowej UWr muszą spełniać wymagania techniczne aplikacji antywirusowej rekomendowanej przez Dział Usług Informatycznych.
2. System operacyjny każdego urządzenia mobilnego powinien być systematycznie uaktualniany przez Użytkownika do jego najnowszej oficjalnej wersji dostarczanej przez producenta.
3. Niedozwolone jest korzystanie z nieoficjalnej wersji systemu operacyjnego lub jego modyfikowanie tak, aby:
    1) uzyskać tzw. dostęp root lub jailbreak do urządzenia w celu złamania ograniczeń producenta lub
    2) uzyskać możliwość ingerowania w system operacyjny lub
    3) instalować oprogramowanie nieautoryzowane.

§ 3
Obowiązki Użytkowników urządzeń mobilnych

1. Użytkownicy urządzeń mobilnych mogą instalować aplikacje wyłącznie:
   1) w porozumieniu z Administratorem lokalnym oraz
   2) pochodzące z oficjalnego źródła oraz
   3) figurujące w spisie programów sporządzanych przez Administratorów lokalnych.
2. Instalacja innych aplikacji, spoza spisu autoryzowanego przez Administratora lokalnego, będzie możliwa jedynie po wcześniejszym ich zatwierdzeniu przez Administratora lokalnego.
3. Administrator lokalny odpowiada za aktualizację aplikacji antywirusowej oraz sygnatur baz wirusów.
4. Użytkownicy urządzeń mobilnych są odpowiedzialni za poufność swoich danych dostępowych oraz danych wytwarzanych przez siebie w ramach obowiązków pracy.
5. Na służbowych urządzeniach mobilnych, które uzyskują dostęp do zasobów sieci komputerowej UWr przechowuje się tylko dane służące do wykonywania obowiązków służbowych.
6. Użytkownik urządzenia mobilnego jest zobowiązany niezwłocznie powiadomić:
   1) Policję oraz Rektora lub właściwego Prorektora, Dziekana, Dyrektora Generalnego, Kierownika/Dyrektora jednostki pozawydziałowej, zgodnie z podległością służbową wynikającą ze struktury organizacyjnej - w przypadku uzasadnionego podejrzenia kradzieży urządzenia służbowego,
   2) Inspektora Ochrony Danych UWr, w przypadku uzasadnionego podejrzenia kradzieży lub wycieku danych osobowych oraz zgłoszenia tego faktu do systemu Logsystem zgodnie z zarządzeniem Rektora Uniwersytetu Wrocławskiego w sprawie ochrony danych osobowych w Uniwersytecie Wrocławskim,
   3) Rektora lub właściwego Prorektora, Dziekana, Dyrektora Generalnego, Kierownika/Dyrektora jednostki pozawydziałowej, zgodnie z podległością służbową wynikającą ze struktury organizacyjnej - w przypadku uzasadnionego podejrzenia kradzieży lub wycieku danych stanowiących tajemnicę przedsiębiorstwa (w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji),
   4) Administratora lokalnego w sytuacjach określonych w pkt 1, 2 lub 3. Zgłoszenie sytuacji, o których mowa w pkt 1, 2 lub 3 powinno być skierowane na adres mailowy Administratora lokalnego lub na adres lokalnego systemu helpdesk i powinno zawierać w szczególności: miejsce i datę zdarzenia oraz jego okoliczności.
7. Każde urządzenie mobilne musi być zabezpieczone przez co najmniej jedną z następujących metod blokowania ekranu:
   1) **Wzór:** złożoność wzoru to minimalnie 6 punktów;
   2) **Kod PIN:** składa się co najmniej z 4 cyfr;
   3) **Hasło:** składa się z co najmniej 8 znaków i zawiera co najmniej trzy z poniższych wymagań co do złożoności znaków: mała litera, duża litera, cyfra, znak specjalny, np. „#";
   4) jeżeli możliwości techniczne urządzenia mobilnego na to pozwalają, zaleca się używanie blokady ekranu w innej dostępnej w danym urządzeniu postaci zapewniającej ochronę przed nieautoryzowanym dostępem osób trzecich np. skanera biometrycznego (linii papilarnych). Należy pamiętać, aby w tym wypadku ustawić również hasło alternatywne.

§ 4
Obowiązki Administratorów lokalnych

1. Administrator lokalny ma obowiązek szkolić Użytkowników urządzeń mobilnych w zakresie bezpieczeństwa, dostępu i łączenia się z zasobami sieci komputerowej UWr.
2. Administrator lokalny ma obowiązek niezwłocznego reagowania na powiadomienia o kradzieży, zgubieniu, wycieku danych lub wystąpieniu innych incydentów

związanych z użytkowaniem urządzeń mobilnych oraz powinien bezzwłocznie:
1) zapisywać zdarzenia w elektronicznym dzienniku zdarzeń,
2) zgłaszać incydenty do Administratora uczelnianej sieci komputerowej na adres pomoc@uwr.edu.pl.

3. Administrator lokalny ma obowiązek sporządzać, udostępniać i aktualizować spis aplikacji, które Użytkownik może instalować na urządzeniach mobilnych łączących się z zasobami sieci komputerowej UWr.

Załącznik Nr 10
do Regulaminu

Zasady użytkowania systemu TETA EDU w Uniwersytecie Wrocławskim

§ 1

W celu zapewnienia właściwej obsługi systemu informatycznego TETA EDU, zwanego dalej systemem, ustanawia się w Uniwersytecie Wrocławskim:

1/ Administratora merytorycznego systemu, w osobie Głównego Księgowego i w jego zastępstwie Zastępcę Głównego Księgowego odpowiedzialnego za:
   a/ funkcjonowanie, jakość, właściwe użycie i bezpieczeństwo informacji w systemie,
   b/ zatwierdzanie zmian dotyczących parametryzacji systemu,
   c/ zatwierdzanie propozycji dotyczących rozwoju systemu,
   d/ opracowanie strategii rozwoju systemu i stały nadzór nad jego rozwojem.

2/ Administratorów informatycznych sytemu – osoby wyznaczone przez Kierownika Działu Usług Informatycznych, będące pracownikami Zespołu Aplikacji Komputerowych. Administrator informatyczny jest odpowiedzialny za:
   a/ zarządzanie użytkownikami, w tym zakładanie i blokowanie kont użytkowników oraz za nadawanie, zmianę i usuwanie uprawnień,
   b/ zakładanie profili użytkowników i ich modyfikację,
   c/ obsługę zgłoszeń użytkowników w systemie LOGSYSTEM dotyczących problemów z dostępem do oraz działaniem systemu,
   d/ zgłaszanie błędów w aplikacji do zewnętrznego dostawcy i monitorowanie procesu ich usuwania,
   e/ zarządzanie procesem zmiany w tym instalację poprawek oraz ich testowanie,
   f/ zarządzanie dostępem firm i konsultantów zewnętrznych do poszczególnych instancji systemu,
   g/ nadzór nad procesem archiwizowania danych oraz kopiami bezpieczeństwa, w tym tworzeniem, kasowaniem i odtwarzaniem poszczególnych instancji systemu zgodnie z obowiązującą w tym obszarze polityką dla tego oprogramowania,
   h/ tworzenie mechanizmów oraz zarządzanie mechanizmami wymiany danych z innymi aplikacjami używanymi w Uniwersytecie Wrocławskim (np. EGERIA, USOS, TETA BI),
   i/ zarządzanie zasadami udostępniania aplikacji w Intranecie oraz Internecie,
   j/ zarządzanie środowiskiem sprzętowo-programowym aplikacji.

§ 2

1. Dostęp do systemu Teta EDU mogą posiadać:
   a/ pracownicy – w zakresie niezbędnym do wykonywania powierzonych im czynności służbowych,
   b/ wykonawcy usług z firm zewnętrznych oraz dostawcy oprogramowania – w zakresie koniecznym do realizowania usługi lub wykonania określonych czynności w systemie
2. Dostęp nadawany jest na podstawie wniosku, którego wzór stanowi Załącznik Nr 1 do niniejszych Zasad.
3. Wniosek o dostęp:
   a/ pracownicy – w zakresie niezbędnym do wykonywania powierzonych im czynności służbowych,
   b/ wykonawcy usług z firm zewnętrznych oraz dostawcy oprogramowania – w zakresie koniecznym do realizowania usługi lub wykonania określonych czynności w systemie
4. Uprawnienia użytkownika w systemie nadawane są poprzez przypisanie profili. Lista profili stanowi Załącznik Nr 2 do niniejszych Zasad

5. Wniosek podlega zatwierdzeniu przez Główną Księgową lub Zastępcę Głównej Księgowej.

§ 3

Konto w systemie tworzone jest przez administratora informatycznego dla każdego użytkownika indywidualnie. Logowanie do systemu odbywa się z użyciem danych dostępowych do konta w usłudze MS OFFICE365.

§ 4

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wynikające z przeprowadzanych analiz ryzyka w systemie TETA EDU obowiązuje wysoki poziom bezpieczeństwa przetwarzania danych osobowych.

§ 5

1. Kierownik jednostki organizacyjnej zobowiązany jest do niezwłocznego informowania Administratora informatycznego systemu o konieczności zablokowania dostępu, odebrania lub zmiany uprawnień użytkownika. Zgłoszenia dokonuje składając wniosek w systemie helpdeskowym dostępnym pod adresem https://pomoc.uwr.edu.pl.
2. Administrator informatyczny blokuje dostęp do konta systemu TETA EDU niezwłocznie:
   1/ po zakończeniu stosunku pracy z użytkownikiem systemu,
   2/ po zmianie miejsca zatrudnienia użytkownika systemu,
   3/ po wygaśnięciu umowy z wykonawcą usługi,
   4/ po otrzymaniu informacji dotyczącej zagrożenia bezpieczeństwa danych zgromadzonych w systemie.

§6

Zobowiązuje się administratora informatycznego systemu TETA EDU do:

1/ przeprowadzania nie rzadziej niż raz na 24 m-ce weryfikacji, czy zestaw przyznanych pracownikowi uprawnień jest odpowiedni dla zadań realizowanych przez pracownika (wynikających m.in. z karty stanowiska pracy)
2/ przeprowadzenia powyższej weryfikacji dla wszystkich aktywnych kont użytkowników systemu w ciągu 30 dni od wejścia w życie niniejszego Regulaminu.

Załącznik Nr 1 do Zasad

Wniosek o nadanie/zmianę/odebranie* uprawnień do systemów teleinformatycznych

(wzór wydruku elektronicznego wniosku - w miejscach wykropkowanych system podpowiada dozwolone opcje do wyboru)

Nazwa systemu informatycznego lub usługi:

…………………………….………………………………….

Nr wniosku: ………………………………….

Data wypełnienia przez wnioskującego: ………………………………….

Rodzaj zmiany: …………………………….………………………………….

(nadanie, zmiana, odebranie dostępu do systemów)

Użytkownik: ………………………………. , …………………………….………………………………….

(imię i nazwisko) (nazwa jednostka organizacyjna UWr)

…………………………….………………………………….

(e-mail służbowy:)

Opis uprawnień:

……………………………………………………………………….., data od — data do ***

(nazwa profilu, zakresu danych, bazy danych)** (zakres dat obowiązywania uprawnień)

……

……

(opis uprawnień specjalnych)

Oświadczam, że użytkownik został upoważniony do przetwarzania danych osobowych w zakresie adekwatnym do zadań, które ma wykonywać w systemie.

Proszę o nadanie uprawnień

....

(data, podpis wnioskującego)

Wyrażam zgodę

....

(data, podpis administratora merytorycznego systemu)

Zrealizowano

....

(data, podpis administratora informatycznego systemu)

* niepotrzebne skreślić.

** lista profili dostępowych znajduje się w załączniku nr 1.

*** w przypadku umów na czas określony należy obowiązkowo podać datę zakończenia współpracy.

**** w przypadku braku wiedzy w wyżej wymienionym temacie przed wypełnieniem wniosku należy skontaktować się z DUI poprzez https://pomoc.uwr.edu.pl

Załącznik Nr 2

do Zasad

Lista profili dla systemów TETA EDU/TETA WEB

Nazwa profilu	Opis profilu	Uwagi
UWR E-KANCELARIA	Profil pozwalający użytkownikowi z tymi uprawnieniami na: • ewidencjonowanie korespondencji przychodzącej i wychodzącej w UWr, • rejestrowanie przez jednostki UWr spraw zgodnie z obowiązującą w Uczelni Instrukcją Kancelaryjną oraz Jednolitym Rzeczowym Wykazem Akt UWr. Korespondencja wychodząca może być korespondencją adresowaną na zewnątrz lub korespondencją wewnętrzną - pomiędzy jednostkami UWr.	
UWR E-UMOWY	Profil pozwalający użytkownikowi z tymi uprawnieniami na obsługę umów zgodnie z przyjętym obiegiem. Rejestruje kolejne etapy powstawania umowy oraz jak przebiegał proces akceptacyjny ze wszystkimi uwagami i kolejnymi wersjami umów aż do podpisania ostatecznej umowy. Wspiera użytkownika na kolejnych etapach obiegu dokumentu oraz posiada wstępnie zaakceptowane szablony przykładowych umów.	
UWR DELEGACJE	Profil pozwalający użytkownikowi z tymi uprawnieniami na prowadzenie nadzoru procesu wprowadzonych delegacji w TC.	
UWR INWENTARYZACJA	Profil pozwalający użytkownikowi z tymi uprawnieniami na realizację procesu rejestracji inwentaryzacji.	
UWR LG_INDEKSY	Profil pozwalający użytkownikowi z tymi uprawnieniami do wprowadzania indeksów materiałowych.	
UWR LG_MAGAZYN	Profil pozwalający użytkownikowi z tymi uprawnieniami na ewidencji operacji na magazynach: • przyjęć, • rozchodów, • inwentaryzacji. Użytkownik ma dostęp również do dokumentów zakupu, z których może wygenerować dokumenty przyjęcia.	
UWR LG_SEKCJA	Profil pozwalający użytkownikowi z tymi uprawnieniami na wprowadzanie wniosków	

ZAOPATRZENIA	zakupowych (parametryzacja zakupu do Wniosków zakupowych w TETA WEB).	
UWR LG_SPRZEDAŻ	Profil pozwalający użytkownikowi z tymi uprawnieniami do: • obsługi procesu sprzedaży, • wystawiania faktur (faktury zaliczkowe i walutowe), • wystawiania not księgowych, • prowadzenia rozliczeń wewnętrznych, • wprowadzenia i obsługi umów sprzedaży.	
UWR LG_SPRZEDAŻ + KASA	Profil pozwalający użytkownikowi z tymi uprawnieniami na wykonywanie wszystkich czynności zawartych w profilu LG_SPRZEDAŻ z dodatkowymi uprawnieniami pozwalającymi na ewidencjonowanie operacji gotówkowych na raportach kasowych.	Wykorzystywany w jednostkach, gdzie istnieje obrót gotówką, m.in. muzea, akademiki.
UWR LG_ZAKUP	Profil pozwalający użytkownikowi z tymi uprawnieniami na: • ewidencjonowanie faktur zakupu, • ewidencjonowanie innych dokumentów zakupu (rachunków, not). Umożliwia rozbicie obiektowe pozycji dokumentów zakupu.	
UWR LG_ZAKUP RR	Profil pozwalający użytkownikowi z tymi uprawnieniami na: • ewidencjonowanie faktur zakupu od rolników, • ewidencjonowanie innych dokumentów zakupu (rachunków, not). Umożliwia rozbicie obiektowe pozycji dokumentów zakupu.	
UWR LG_ZAKUP+OPER_WB	Profil pozwalający użytkownikowi z tymi uprawnieniami na wykonywanie wszystkich czynności zawartych w profilu LG_ZAKUP poszerzona o wtyczki: • Rachunki bankowe • Operacje wyciągów bankowych.	Profil stworzony na potrzeby pracowników Zespołu Dokumentacji Obrotu Zagranicznego
UWR LOGISTYK	Profil pozwalający użytkownikowi z tymi uprawnieniami na parametryzację i zarządzanie logistyką.	
UWR TRANSPORT	Profil pozwalający użytkownikowi z tymi uprawnieniami na ewidencję i rozliczanie tras pojazdów.	
UWR FK MT LG ZP BIG	Profil pozwalający użytkownikowi z tymi uprawnieniami na: • dekretację dokumentów pochodzących z innych modułów, • wprowadzanie dokumentów	Główny profil wykorzystywany w Dziale Księgowości Głównej, Dziale Księgowości Projektowej i Dziale

	księgowych (m.in. PK), • tworzenie rejestrów księgowych; • obsługę wyciągów bankowych i operacji kasowych, wraz z windykacją; • obsługę majątku trwałego; • obsługę deklaracji VAT. Zawiera ewidencję projektów: • dodawanie projektu, • uzupełnianie danych, • wersjonowanie, • wprowadzanie informacje związanych z budżetem, Posiada narzędzia do kontroli dostępnych środków w budżecie (BAM).	Kosztów.
UWR FK MT LG ZP BIG 2	Profil pozwalający użytkownikowi z tymi uprawnieniami na wykonywanie wszystkich czynności zawartych w profilu UWR FK MT LG ZP BIG poszerzona o: • możliwość obsługi obiektów ewidencyjnych, • tworzenia grup OE, • dodawania / zmiany pozycji w grupach OE.	
UWR FK PLAN KONT	Profil pozwalający użytkownikowi z tymi uprawnieniami na przeglądanie planu kont.	
UWR FINANSE	Profil pozwalający użytkownikowi z tymi uprawnieniami do: • obsługi rozrachunków, • płatności, • operacji bankowych, • windykacji • opisania obiektowo dokumentów zakupu. Nie zawiera obsługi modułu VAT. Nie pozwala na dekretację dokumentów zakupu, sprzedaży, WB i dokumentów z MT.	
UWR FINANSE + VAT	Profil pozwalający użytkownikowi z tymi uprawnieniami na wykonywanie wszystkich czynności zawartych w profilu UWR Finanse poszerzony o: • obsługę deklaracji VAT, • obsługę MT, • dekretację dokumentów zakupu sprzedaży, WB i dokumentów z MT.	
UWR FINANSE-PODGLĄD	Profil pozwalający użytkownikowi z tymi uprawnieniami na wykonywanie wszystkich operacji zawartych w profilu UWR Finanse + VAT jedynie do podglądu danych i generowania raportów.	
UWR FINANSE-PODGLĄD+SPRAWOZDAWCZOŚĆ	Profil pozwalający użytkownikowi z tymi uprawnieniami na wykonywanie wszystkich operacji zawartych w profilu UWR Finanse + VAT jedynie do podglądu danych i generowania raportów oraz	

	podgląd do sprawozdawczości.	
UWR FK STATYSTYKA	Profil pozwalający na dostęp do rejestrów księgowych i do ewidencji zarządczej.	
UWR KASA	Profil pozwalający użytkownikowi z tymi uprawnieniami do obsługi operacji kasowych: • przyjmowania i wydawania gotówki, • generowania dokumentów kasowych, • tworzenia raportów kasowych.	
UWR PEŁNOMOCNICTWO REKTORA	Profil pozwalający na sprawdzenie Obiektów Ewidencyjnych oraz na sprawdzenie zastępstw i zależności służbowych.	
UWR MAJĄTEK TRWAŁY	Profil pozwalający użytkownikowi z tymi uprawnieniami do: • ewidencjonowania i obsługi składników majątku trwałego, • naliczania amortyzacji, przeprowadzania inwentaryzacji.	
UWR MAJĄTEK TRWAŁY – PRZEGLĄDANIE	Profil pozwalający użytkownikowi z tymi uprawnieniami na wykonywanie wszystkich operacji zawartych w profilu UWR Majątek Trwały - przeznaczony tylko do odczytu.	
UWR WYCIĄGI BANKOWE	Profil pozwalający użytkownikowi z tymi uprawnieniami do obsługę wyciągów bankowych poprzez: • zarządzanie płatnościami, • tworzenie paczek z przelewami, • wczytywanie wyciągów bankowych oraz ich opisanie i dekretację.	
UWR KONTRAHENCI	Profil pozwalający użytkownikowi z tymi uprawnieniami do wprowadzania i edycji kontrahentów.	
UWR WINDYKACJA	Profil pozwalający użytkownikowi z tymi uprawnieniami do obsługi procesów windykacyjnych.	
UWR WŁADZE UCZELNI	Profil pozwalający użytkownikowi z tymi uprawnieniami na wykonywanie wszystkich operacji zawartych w profilu UWR FK MT LG ZP BIG - przeznaczony tylko do odczytu.	
UWR ZARZĄDZANIE - DELEGACJE	Profil pozwalający użytkownikowi z tymi uprawnieniami do zarządzania delegacjami.	TETA EDU
UWR ZP_BAM	Profil pozwalający użytkownikowi z tymi uprawnieniami na dostęp do modułu BAM.	

UWR ZP_PROJEKTY	Profil pozwalający użytkownikowi z tymi uprawnieniami na: • dodawanie projektu, • uzupełnianie danych, • wersjonowanie, • wprowadzanie informacji związanych z budżetem, itp. Zawiera również wtyczki pozwalające na kontrole dostępnych środków w budżecie (BAM).	
UWR PROJEKTY - PRZEGLĄDANIE DANYCH + WYDRUKI	Profil pozwalający użytkownikowi z tymi uprawnieniami na: • przeglądanie danych, bez możliwości edycji. • wgląd do projektów, • wgląd do kosztów i przychodów przypisanych do projektów, wydziałów, jednostek. Zawiera również wtyczki pozwalające na kontrole dostępnych środków w budżecie (BAM).	Profil przeznaczony dla pełnomocników i innych pracowników jednostek do raportowania.
UWR ZARZĄDZANIE NIERUCHOMOŚCIAMI	Profil pozwalający użytkownikowi z tymi uprawnieniami na ewidencję nieruchomości pod kontem formalno-technicznym.	Profil dedykowany dla zarządzania nieruchomościami, wykorzystywany głównie przez Dział Gospodarki Nieruchomościami.
UWR PRACOWNIK - DELEGACJE	Profil pozwalający użytkownikowi z tymi uprawnieniami na rejestrację delegacji przez pracowników wydziałów i jednostek.	TETA WEB
UWR BANKI	Profil przeznaczony do obsługi webservice'ów bankowych.	
UWR LICZNIKI	Profil do obsługi liczników; Profil wykorzystywany przez Dział Gospodarowania Nieruchomościami.	
UWR PRZEKAZY	Profil do pobierania danych z list płac i drukowania przekazów pocztowych.	

Załącznik Nr 11
Do Regulaminu

Regulamin użytkowania systemu Huesca w Uniwersytecie Wrocławskim

§ 1

W celu zapewnienia obsługi systemu informacji naukowej Huesca, zwanego dalej systemem, ustanawia się w Uniwersytecie Wrocławskim:

1/ Administratora merytorycznego systemu, powołanego przez Rektora na wniosek Dyrektora ds. informatycznych. Administrator merytoryczny systemu podlega bezpośrednio Dyrektorowi ds. informatycznych i jest odpowiedzialny za:
   a/ pomoc bibliotekarzom posiadającym uprawnienia w systemie,
   b/ obsługę zgłoszeń związanych z pracą merytoryczną w systemie,
   c/ szkolenie, we współpracy z bibliotekarzem-eksporterem, bibliotekarzy z danej jednostki,
   d/ śledzenie zmian w bazie PBN i przygotowanie propozycji modyfikacji systemu Huesca w celu zapewnienia zgodności z bazą PBN,
   e/ składanie propozycji dotyczących rozwoju systemu.
2/ Administratora informatycznego powołanego przez Dyrektora ds. informatycznych odpowiedzialnego za:
   a/ zarządzanie użytkownikami, w tym zakładanie i blokowanie kont użytkowników oraz nadawanie, zmianę i usuwanie uprawnień,
   b/ obsługę zgłoszeń użytkowników w systemie LOGSYSTEM dotyczących problemów z dostępem do oraz z działaniem systemu Huesca,
   c/ aktualizowanie punktowanych list ministerialnych,
   d/ zarządzanie dostępem firm i konsultantów zewnętrznych do poszczególnych instancji systemu Huesca,
   e/ zarządzanie procedurami archiwizowania danych oraz kopiami bezpieczeństwa,
   w tym odtwarzanie poszczególnych instancji systemu Huesca,
   f/ obsługę procesu wymiany danych z systemu Egeria,
   g/ zarządzanie zasadami udostępniania aplikacji w Intranecie oraz Internecie,
   h/ zarządzanie środowiskiem sprzętowo-programowym aplikacji,
   i/ przeprowadzanie cyklicznej weryfikacji kont użytkowników, nie rzadziej niż raz na 24 miesiące.

§ 2

1. Uprawnienia poszczególnym użytkownikom systemu nadawane są na podstawie wniosku, którego wzór stanowi Załącznik do niniejszego Regulaminu, z zastrzeżeniem ust. 7.
2. Wniosek składa, w formie pisemnej lub elektronicznej w systemie LOGSYSTEM, kierownik jednostki organizacyjnej.
3. Uprawnienia do edycji zapisów w systemie otrzymują przeszkoleni bibliotekarze, po akceptacji Administratora merytorycznego.
4. Bibliotekarze, o których mowa w ust. 3, są odpowiedzialni za prawidłowe i terminowe wprowadzanie danych z danej jednostki do systemu.
5. Uprawnienia do modułu eksportu w bazie systemu Huesca otrzymują bibliotekarze-eksporterzy wyznaczeni przez kierowników jednostek, po akceptacji Administratora merytorycznego.

6. Wyznaczeni bibliotekarze mogą uzyskać dodatkowo uprawnienia do modułu statystycznego i modułu ostrzeżeń.
7. Dziekani, prodziekani i przewodniczący rad dyscyplin naukowych otrzymują automatycznie uprawnienia obserwatora w odpowiadającej danemu wydziałowi instancji systemu Huesca na okres pełnienia funkcji. Do przyznania uprawnień niezbędne jest posiadanie upoważnienia do przetwarzania danych osobowych.
8. Wniosek zgłoszeniowy użytkownika systemu Huesca ważny jest wyłącznie z przesłaną elektronicznie kopią upoważnienia do przetwarzania danych osobowych.

§ 3

Konto w systemie tworzone jest indywidualnie dla każdego użytkownika przez administratora informatycznego. Logowanie do systemu odbywa się z użyciem danych dostępowych do konta w usłudze MS OFFICE365.

§ 4

1. Kierownik jednostki organizacyjnej zobowiązany jest do informowania administratora informatycznego o konieczności zablokowania, odebrania lub zmiany uprawnień dostępu dla użytkownika.
2. Zgłoszenia dokonuje się składając wniosek w systemie .
3. Zablokowanie konta następuje niezwłocznie po otrzymaniu informacji:
   1/ o zakończeniu stosunku pracy z użytkownikiem systemu,
   2/ o zmianie jednostki organizacyjnej będącej miejscem zatrudnienia użytkownika systemu,
   3/ dotyczącej zagrożenia bezpieczeństwa danych zgromadzonych w systemie.

§ 5

Zobowiązuje się administratora informatycznego systemu Huesca do dezaktywacji konta oraz odebrania uprawnień dostępu dla użytkownika po otrzymaniu informacji o zakończeniu stosunku pracy z systemu kadrowo-płacowego Egeria.

Załącznik

do Regulaminu

Wniosek o nadanie uprawnień do systemów teleinformatycznych

Nr wniosku (wypełnia DUI)	
Data wpłynięcia do DUI (wypełnia DUI)	
Data wypełnienia przez wnioskującego	
Imię, nazwisko	
Jednostka organizacyjna UWr	
Adres e-mail w domenie uwr.edu.pl	
Rodzaj zmiany*	▪ Nadanie uprawnień ▪ Zmiana uprawnień ▪ Odebranie uprawnień
Nazwa systemu informatycznego lub usługi	**HUESCA**
Lista instancji**	
Opis uprawnień***	
Proszę o nadanie uprawnień	Akceptacja (jeśli jest wymagana)

…… (data, podpis przełożonego)	…… (data, podpis administratora merytorycznego systemu)
Zrealizował …… (data, podpis administratora informatycznego systemu)	

* niepotrzebne skreślić.

** System informacji naukowej Huesca został uruchomiony w dwunastu jednostkach. Wnioskując o dostęp dla pracownika należy wskazać jedną lub więcej instancji, do których pracownik ma otrzymać dostęp. W przypadku wnioskowania o dostęp dla pracownika z danej jednostki do innych instancji wolno wskazać tylko rolę obserwatora.

Lista instancji	**Opis**
https://csne.huesca.uni.wroc.pl	Centrum Studiów Niemieckich i Europejskich im. W. Brandta
https://wbt.huesca.uni.wroc.pl	Wydział Biotechnologii
https://wch.huesca.uni.wroc.pl	Wydział Chemii
https://wfil.huesca.uni.wroc.pl	Wydział Filologiczny
https://wfa.huesca.uni.wroc.pl	Wydział Fizyki i Astronomii

https://wmi.huesca.uni.wroc.pl	Wydział Matematyki i Informatyki
https://wnb.huesca.uni.wroc.pl	Wydział Nauk Biologicznych
https://wnhip.huesca.uni.wroc.pl	Wydział Nauk Historycznych i Pedagogicznych
https://wnzks.huesca.uni.wroc.pl	Wydział Nauk o Ziemi i Kształtowania Środowiska
https://wns.huesca.uni.wroc.pl	Wydział Nauk Społecznych
https://wpae.huesca.uni.wroc.pl	Wydział Prawa, Administracji i Ekonomii
https://buwr.huesca.uni.wroc.pl	Biblioteka UWr

***W systemie informacji naukowej Huesca uprawnienia występują na sześciu poziomach. Lista uprawnień wraz z krótkim opisem jest zawarta w poniższej tabeli.

Lista uprawnień	**Opis**
administrator	Pełne uprawnienia do obsługi, nadawania uprawnień i parametryzowania systemu
bibliotekarz-eksporter	Uprawnienia do edycji zapisów w bazie i eksportu publikacji do PBN
bibliotekarz-analityk	Uprawnienia do edycji zapisów w bazie i dostęp do modułu statystycznego
bibliotekarz-audytor	Uprawnienia do edycji zapisów w bazie i dostęp do modułu ostrzeżeń

bibliotekarz	Uprawnienia do edycji zapisów w bazie
obserwator	Uprawnienia tylko do odczytu informacji

Załącznik Nr 12
do Regulaminu

Regulamin nadawania uprawnień użytkownikom systemu ARIS

1. Ilekroć w niniejszym regulaminie jest mowa o:
   1) Administratorze merytorycznym (AM) rozumie się przez to Kierownika Biura ds. Strategii, Kontroli Zarządczej i Zarządzania Procesowego odpowiedzialnego za:
      a) wsparcie użytkowników systemu ARIS w obszarze obsługi systemu;
      b) szkolenie nowych użytkowników;
      c) akceptację wniosków o nadanie uprawnień użytkownikom w systemie ARIS;
      d) wskazywanie modeli dostępnych w ramach profili użytkowników.

   2) Administratorze informatycznym rozumie się przez to administratora systemu odpowiedzialnego za:
      a) zarządzanie użytkownikami, w tym zakładanie i blokowanie konta użytkownika oraz nadawanie, zmianę i usuwanie uprawnień,
      b) obsługę zgłoszeń użytkowników w systemie LOGSYSTEM dotyczących problemów z dostępem do oraz działaniem systemu ARIS,
      c) zgłaszanie błędów w aplikacji do zewnętrznego dostawcy w celu ich usunięcia,
      d) instalację poprawek oraz ich testowanie,
      e) zarządzanie dostępem firm i konsultantów zewnętrznych do poszczególnych instancji baz danych systemu ARIS,
      f) zarządzanie procedurami archiwizowania danych oraz kopiami bezpieczeństwa, w tym tworzenie, kasowanie i odtwarzanie poszczególnych instancji programu ARIS zgodnie z obowiązującą w tym obszarze polityką dla tego oprogramowania,
      g) zarządzanie zasadami udostępniania aplikacji w Intranecie oraz Internecie,
      h) zarządzanie środowiskiem sprzętowo-programowym aplikacji.

2. Wniosek o nadanie/zmianę/odebranie uprawnień do korzystania z systemu ARIS akceptuje Administrator Merytoryczny.

3. Uprawnienia poszczególnym użytkownikom systemu nadawane są na pisemny lub elektroniczny wniosek złożony w systemie LOGSYSTEM przez kierownika jednostki organizacyjnej, w której zatrudniony jest dany pracownik. Wzór wniosku o nadanie/zmianę/odebranie uprawnień w systemie ARIS stanowi Załącznik do niniejszego Regulaminu.

4. Konto w systemie ARIS jest tworzone indywidualnie dla każdego użytkownika przez Administratora informatycznego. Logowanie do systemu ARIS odbywa się z użyciem konta usługi MS OFFICE365.

5. W przypadku zakończenia stosunku pracy z pracownikiem lub zmiany zakresu jego obowiązków służbowych kierownik jednostki organizacyjnej zobowiązany jest niezwłocznie poinformować administratora informatycznego o tym fakcie,

składając pisemny lub elektroniczny wniosek w systemie LOGSYSTEM o odebranie lub zmianę uprawnień dostępowych do systemu ARIS dla wskazanego pracownika.

6. Zobowiązuje się Administratora informatycznego systemu ARIS do:
    1) zweryfikowania wszystkich dotychczas utworzonych kont użytkowników systemu w ciągu 30 dni od wejścia w życie Regulaminu;
    2) przeprowadzania cyklicznej weryfikacji kont użytkowników nie rzadziej niż raz na 24 m-ce.

7. obowiązuje się administratora informatycznego systemu ARIS do dezaktywacji kont oraz usuwania uprawnień użytkowników po otrzymaniu stosownych informacji z systemu EGERIA.
    1) Zablokowanie konta powinno nastąpić niezwłocznie po otrzymaniu informacji:
        a) o zakończeniu współpracy,
        b) o zmianie miejsca zatrudnienia,
        c) innego zgłoszenia dotyczącego bezpieczeństwa danych.
    2) Odebranie uprawnień musi nastąpić w nieprzekraczalnym terminie 2 dni roboczych od zablokowania konta.

Załącznik
do Regulaminu

Wniosek o nadanie/zmianę/odebranie* uprawnień do systemów teleinformatycznych

<table>
<tr><td>Nr wniosku (wypełnia DUI)</td><td colspan="2"></td></tr>
<tr><td>Data wpłynięcia do DUI (wypełnia DUI)</td><td colspan="2"></td></tr>
<tr><td>Data wypełnienia przez wnioskującego</td><td colspan="2"></td></tr>
<tr><td>Imię, nazwisko</td><td colspan="2"></td></tr>
<tr><td>Jednostka organizacyjna UWr</td><td colspan="2"></td></tr>
<tr><td>Adres e-mail w domenie uwr.edu.pl</td><td colspan="2"></td></tr>
<tr><td>Rodzaj zmiany</td><td colspan="2">▪ Nadanie uprawnień*
▪ Zmiana uprawnień*
▪ Odebranie uprawnień*</td></tr>
<tr><td>Nazwa systemu informatycznego lub usługi</td><td colspan="2">ARIS</td></tr>
<tr><td>Opis uprawnienia **</td><td colspan="2"></td></tr>
<tr><td>Profil***</td><td colspan="2"></td></tr>
<tr><td>Sposób zatrudnienia:
• umowa o pracę na czas określony/nieokreślony *</td><td>od /rrrr-mm-dd/</td><td>do /rrrr-mm-dd/ ****</td></tr>
<tr><td>Proszę o nadanie uprawnień

.....
(data, czytelny podpis Przełożonego)</td><td colspan="2">Wyrażam zgodę

.....
(data, czytelny podpis Administratora merytorycznego systemu)</td></tr>
<tr><td colspan="3">Zrealizował

.....
(data, czytelny podpis Administratora Systemu)</td></tr>
</table>

* niepotrzebne skreślić.

** lista przykładowych opisów uprawnień znajduje się w załączniku do wniosku.

*** lista baz danych, do których użytkownik ma mieć dostęp znajduje się w załączniku do wniosku.

**** w przypadku umów na czas określony należy obowiązkowo podać datę zakończenia stosunku pracy.

Załącznik do Wniosku o nadanie/zmianę/odebranie uprawnień do systemów teleinformatycznych

Zestawy uprawnień, o które można wnioskować (wersja z dnia 1 lutego 2021 r.)
(lista może się nieco zmieniać w zależności od potrzeb i rozwoju systemu)

l.p.	Opis uprawnienia	Opis	Grupa docelowa użytkowników
1	ARIS Connect	Uprawnienia do przeglądania zawartości udostępnionej bazy danych ARIS	Użytkownicy aplikacji ARIS
2	Aris Designer	Uprawnienia do przeglądania i pełnej edycji zawartości udostępnianej bazy danych ARIS	BSKZZP, AUDYT, użytkownicy kluczowi
3	ARIS Architect	Uprawnienia do przeglądania, pełnej edycji zawartości istniejących oraz tworzenia nowych baz danych ARIS	DUI, BSKZZP
4	Konsultant	Zakres uprawnień dostosowany do umowy z konsultantem	Konsultanci zewnętrzni zatrudnieni przez UWr
5	Administrator	Pełne uprawnienia do aplikacji i modeli	DUI
l.p.	**Profil**	**Opis**	**Grupa docelowa użytkowników**
1	UWr_WŁADZE	Baza zawierająca kompletne modele stanu JEST i stanu	Użytkownicy aplikacji ARIS

		DOCELOWY	
2	UWr_UŻYTKOWNIK	Baza zawierająca standardowy zakres modeli stanu JEST i stanu DOCELOWY	Użytkownicy aplikacji ARIS
3	UWr_AUDYT	Modele opracowane w ramach BAW	Audyt UWr
4	UWr_BSKZZP	Modele opracowane w ramach BSKZZP	BSKZZP
5	UWr_WYDZIAŁ_XX	Modele opracowane dla konkretnego Wydziału	Wydziały

Załącznik Nr 13
do Regulaminu

Regulamin nadawania uprawnień użytkownikom systemu Omega PSIR w Uniwersytecie Wrocławskim

§ 1

W celu zapewnienia właściwej obsługi systemu informatycznego **Omega PSIR**, zwanego dalej systemem, ustanawia się w Uniwersytecie Wrocławskim:

1/ **superadmin** systemu zwany dalej SA, w osobie Dyrektora ds. informatycznych, odpowiedzialnego za:
   a/ bezpieczeństwo informacji w systemie;
   b/ zatwierdzanie zmian dotyczących parametryzacji systemu;
   c/ zatwierdzanie propozycji dotyczących rozwoju systemu;
   d/ opracowywanie strategii rozwoju systemu i stały nadzór nad jego rozwojem;
   e/ nadzór nad pracami administratora merytorycznego,
2/ **administratora merytorycznego** systemu zwany dalej AM, w osobie wyznaczonej przez Dyrektora ds. informatycznych, odpowiedzialnego za:
   f/ jakość i bezpieczeństwo informacji w systemie;
   g/ przygotowywanie propozycji zmian dotyczących parametryzacji systemu;
   h/ przygotowywanie propozycji dotyczących rozwoju systemu;
3/ **administratorów informatycznych sytemu** zwany dalej AI – są to osoby wyznaczone przez Kierownika Działu Usług Informatycznych, będące pracownikami Zespołu Aplikacji Komputerowych. Administrator informatyczny jest odpowiedzialny za:
   a/ zarządzanie użytkownikami, w tym zakładanie i blokowanie kont użytkowników oraz za nadawanie, zmianę i usuwanie uprawnień;
   b/ zakładanie profili użytkowników i ich modyfikację;
   c/ obsługę zgłoszeń użytkowników w systemie LOGSYSTEM dotyczących problemów z dostępem oraz działaniem systemu;
   d/ zgłaszanie błędów w aplikacji do zewnętrznego dostawcy i monitorowanie procesu ich usuwania;
   e/ zarządzanie procesem zmiany, w tym instalację poprawek oraz ich testowanie;
   f/ zarządzanie dostępem firm i konsultantów zewnętrznych do poszczególnych instancji systemu;
   g/ zarządzanie procedurami archiwizowania danych oraz kopiami bezpieczeństwa, w tym tworzenie, kasowanie i odtwarzanie poszczególnych instancji systemu zgodnie z obowiązującą w tym obszarze polityką dla tego oprogramowania;
   h/ tworzenie mechanizmów/zarządzanie mechanizmami wymiany danych z innymi aplikacjami używanymi w Uniwersytecie Wrocławskim (np. EGERIA, USOS, HUESCa, Leopoldina), oraz z systemami zewnętrznymi takimi jak:
      - PBN,
      - Google Analytics,
      - Google Analytics - reporting API,
      - Google Maps Platform,
      - Orcid,
      - Scopus,
      - Web of Science,

- Sherpa Romeo,
- CrossRef,
- Google Scholar,
- Researchgate.net,
- ResearcherID,
- AddThis;

i/ zarządzanie zasadami udostępniania aplikacji w Intranecie oraz Internecie;
j/ zarządzanie środowiskiem sprzętowo-programowym aplikacji.

§ 2

1. Uprawnienia poszczególnym użytkownikom systemu nadawane są na podstawie wniosku, którego wzór stanowi **Załącznik Nr 1** do niniejszego Regulaminu.
2. W przypadku pracowników niebędących nauczycielami akademickimi wniosek w systemie LOGSYSTEM składa kierownik jednostki organizacyjnej, w której zatrudniony jest dany użytkownik.
3. W przypadku nauczycieli akademickich wniosek w systemie LOGSYSTEM składa sam zainteresowany w kontekście swojego profilu.
4. Uprawnienia w systemie przydzielane są poprzez przypisanie do użytkownika odpowiednich profili. Lista profili stanowi **Załącznik Nr 2** do niniejszego Regulaminu.
5. Złożony wniosek zatwierdza Dyrektor ds. informatycznych., który może delegować swoje uprawnienia w zakresie zatwierdzania wniosków wybranym pracownikom DUI.
6. Do wniosku należy dołączyć kopię upoważnienia do przetwarzania danych osobowych.

§ 3

Konto w systemie tworzone jest indywidualnie dla każdego użytkownika (pracownika) przez AI. Logowanie do systemu odbywa się z użyciem danych dostępowych do konta w usłudze MS OFFICE365.

§ 4

1. Kierownik jednostki organizacyjnej zobowiązany jest do niezwłocznego informowania AI o konieczności zablokowania, odebrania lub zmiany uprawnień dostępu dla użytkownika, z wyjątkiem użytkowników posiadających rolę naukowca (Załącznik Nr 2).
2. Zgłoszenia dokonuje się składając wniosek w systemie LOGSYSTEM.
3. Zablokowanie konta powinno nastąpić niezwłocznie po otrzymaniu informacji:
   1/ o zakończeniu stosunku pracy z użytkownikiem systemu;
   2/ o zmianie miejsca zatrudnienia użytkownika systemu;
   3/ dotyczącej zagrożenia bezpieczeństwa danych zgromadzonych w systemie.
4. Odebranie uprawnień następuje w nieprzekraczalnym terminie 2 dni roboczych od dnia zablokowania konta.

§ 5

Zobowiązuje się administratora informatycznego systemu **Omega PSIR** do:

1/ zweryfikowania wszystkich dotychczas utworzonych kont użytkowników systemu w ciągu 30 dni od wejścia w życie niniejszego Regulaminu;
2/ przeprowadzania cyklicznej weryfikacji kont użytkowników nie rzadziej niż raz na 24 m-ce.

Załącznik Nr 1 do Regulaminu

Wniosek o nadanie/zmianę/odebranie* uprawnień do systemów teleinformatycznych

<table>
<tr><td>Nr wniosku (wypełnia DUI)</td><td colspan="2"></td></tr>
<tr><td>Data wpłynięcia do DUI (wypełnia DUI)</td><td colspan="2"></td></tr>
<tr><td>Data wypełnienia przez wnioskującego</td><td colspan="2"></td></tr>
<tr><td>Imię, nazwisko</td><td colspan="2"></td></tr>
<tr><td>Jednostka organizacyjna UWr</td><td colspan="2"></td></tr>
<tr><td>Adres e-mail w domenie uwr.edu.pl</td><td colspan="2"></td></tr>
<tr><td>Rodzaj zmiany*</td><td colspan="2">▪ Nadanie uprawnień
▪ Zmiana uprawnień
▪ Odebranie uprawnień</td></tr>
<tr><td>Nazwa systemu informatycznego lub usługi</td><td colspan="2">Omega PSIR</td></tr>
<tr><td>Opis uprawnień

Wpisać docelowe skuteczne uprawnienia w postaci nazwy profilu** oraz odpowiedniej roli związanej z jednostką, magazynem bądź innym wyróżnikiem właściwym dla danego zakresu uprawnień****</td><td colspan="2"></td></tr>
<tr><td>Sposób zatrudnienia:

• umowa o pracę na czas określony/nieokreślony*</td><td>od /rrrr-mm-dd/</td><td>do /rrrr-mm-dd/***</td></tr>
<tr><td>Proszę o nadanie uprawnień

.....

(data, podpis Przełożonego)</td><td colspan="2">Wyrażam zgodę

.....

(data, podpis Dyrektor ds. informatycznych)</td></tr>
<tr><td colspan="3">Zrealizował

.....

(data, czytelny podpis Administratora Informatycznego Systemu)</td></tr>
</table>

* niepotrzebne skreślić.

** lista profili dostępowych znajduje się w załączniku nr 1.

*** w przypadku umów na czas określony należy obowiązkowo podać datę zakończenia współpracy.

**** w przypadku braku wiedzy w wyżej wymienionym temacie przed wypełnieniem wniosku należy skontaktować się z DUI poprzez https://pomoc.uwr.edu.pl

Załącznik Nr 2 do Regulaminu

Lista profili dla systemu Omega PSIR

Profil	Uprawnienia	Uwagi
Superadmin	Superadmin	Rola przeznaczona dla Rektora/Dyrektora ds. Informatycznych
Administrator techniczny	admin	
Administrator merytoryczny	Statisticsview, financeview, XMLexport, selfeditiom, selfimport	Rola przeznaczona dla Dyrektora ds. Informatycznych Podgląd, również finansowy
Kierownik dyscypliny	Statisticsview, XMLexport, selfeditiom, selfimport	**Poziom dostępu do edycji dla całego UWR**
Bibliotekarz-eksporter	Superdataentry, PBNexport, POLonexport, XMLexport statisticsview, verifier, superdownload	**Poziom dostępu do edycji dla całego UWR**
Bibliotekarz-koordynator	Superdataentry, XMLexport statisticsview, verifier	**Poziom dostępu do edycji dla całego UWr**
Bibliotekarz	Dataentry, publications, diplomas	**Poziom dostępu do edycji tylko dla Wydziału**
Pracownik ds. projektów	Superdataentry ,projects, technology, financeview, patents, infrastructure/labs	**Poziom dostępu do edycji dla całego UWr**
Naukowiec (pracownik)	selfeditiom, selfimport	
Dziekan	Statisticsview, XMLexport, financeview	**Poziom dostępu do edycji tylko dla Wydziału**
Pracownik ds. komunikacji	Dataentry, media, events/press, acitivites/achivments, artworks	**Poziom dostępu do edycji dla całego UWR**

Załącznik Nr 14
do zarządzenia Nr 142/2019
z dnia 19 listopada 2019 r.

Regulamin nadawania uprawnień użytkownikom systemu EGERIA w Uniwersytecie Wrocławskim

§ 1

W celu zapewnienia właściwej obsługi systemu informatycznego EGERIA, zwanego dalej systemem, ustanawia się w Uniwersytecie Wrocławskim:

3/ Administratora merytorycznego systemu EGERIA, wyznaczanego przez Dyrektora Generalnego, odpowiedzialnego za:
   e/ funkcjonowanie, jakość, właściwe użycie i bezpieczeństwo informacji w systemie,
   f/ zatwierdzanie zmian dotyczących parametryzacji systemu,
   g/ zatwierdzanie propozycji dotyczących rozwoju systemu,
   h/ opracowanie strategii rozwoju systemu i stały nadzór nad rozwojem systemu;

4/ Administratorów informatycznych systemu EGERIA wyznaczanych przez Kierownika Działu Usług Informatycznych, odpowiedzialnych za zarządzanie użytkownikami, w tym:
   a. nadawanie, na wniosek kierownika właściwej jednostki, użytkownikowi dostępu do systemu;
   b. blokowanie użytkownikowi dostępu do systemu:
      i. na wniosek kierownika właściwej jednostki,
      ii. niezwłocznie po wygaśnięciu uprawnień użytkownika do użytkowania systemu,
   c. zmiana zestawu uprawnień w systemie w oparciu o treść wniosku o dostęp do systemu.

   k/ nadawanie użytkownikowi dostępu do różnych baz danych systemu:
      a. domyślnie do bazy produkcyjnej, testowej i szkoleniowej,
      b. do innych baz testowych na pisemny wniosek kierownika jednostki,
      c. do baz archiwalnych na pisemny wniosek kierownika jednostki,
   l/ nadawanie/odbieranie użytkownikowi dostępu do raportu w systemie na podstawie zgłoszenia Administratora merytorycznego lub osoby przez niego wskazanej,
   m/ nadawanie/odbieranie użytkownikowi uprawnień do tworzenia raportów na pisemny wniosek Administratora merytorycznego lub osoby przez niego wskazanej,
   n/ kastomizacja sposobu pracy użytkownika w systemie (np. ograniczanie uprawnień użytkownika do pracy wyłącznie w trybie „odczyt", przynależność do grup użytkowników, stosowanie filtrów lokalnych, nadawanie uprawnień do: operacji grupowych, do wglądu w pola definiowalne, do używania katalogów systemu plików, dostępu do struktury organizacyjnej),
   o/ obsługa zgłoszeń użytkowników zarejestrowanych w systemie helpdesk dostępnym pod adresem https://pomoc.uwr.edu.pl dotyczących problemów z dostępem oraz działaniem systemu EGERIA,
   p/ zgłaszanie do zewnętrznego dostawcy błędów w systemie i monitorowanie procesu ich usuwania,
   q/ zarządzanie procesem zmiany, w tym procesem instalacji poprawek,
   r/ testowanie zainstalowanych poprawek pod względem technicznym,
   s/ zarządzanie dostępem konsultantów firm zewnętrznych do poszczególnych instancji systemu,

t/ nadzór nad procesem archiwizowania danych oraz kopiami bezpieczeństwa, w tym tworzeniem, kasowaniem i odtwarzaniem poszczególnych instancji systemu zgodnie z obowiązującą w tym obszarze polityką dla tego oprogramowania,
u/ tworzenie mechanizmów i zarządzanie mechanizmami wymiany danych systemu z innymi aplikacjami używanymi w Uniwersytecie Wrocławskim (m.in. TETA EDU, USOS, TETA BI, Portal Pracowniczy, HUESCA, Omega-Psir, strona główna www UWr),
v/ zarządzanie mechanizmami udostępniania danych z systemu EGERIA w Intranecie oraz Internecie,
w/ zarządzanie środowiskiem sprzętowo-programowym systemu.

§ 2

6. Dostęp do systemu EGERIA mogą posiadać:
   a. pracownicy – w zakresie niezbędnym do wykonywania powierzonych im czynności służbowych;
   b. dostawcy oprogramowania oraz wykonawcy usług z firm zewnętrznych – w zakresie koniecznym do realizowania usługi lub wykonania określonych czynności w systemie.
7. Dostęp nadawany jest na podstawie wniosku, którego wzór stanowi Załącznik Nr 1 do niniejszego Regulaminu.
8. Wniosek o dostęp:
   a. w imieniu pracownika składa w systemie helpdesk dostępnym pod adresem https://pomoc.uwr.edu.pl kierownik jednostki organizacyjnej;
   b. dla wykonawcy z firmy zewnętrznej składa w systemie helpdesk kierownik jednostki organizacyjnej odpowiedzialnej za realizację umowy z firmą zewnętrzną.
9. Uprawnienia użytkownika w systemie nadawane są poprzez przypisanie zestawu uprawnień. Lista zestawów uprawnień znajduje się w Załączniku Nr 2 do niniejszego Regulaminu.
10. Wniosek podlega zatwierdzeniu przez Administratora merytorycznego systemu oraz Inspektora Ochrony Danych Osobowych.

§ 3

Dla każdego użytkownika (pracownika lub pracownika firmy zewnętrznej) w systemie EGERIA tworzone jest indywidualne konto imienne.

§ 4

1. W systemie EGERIA przetwarzane są informacje dotyczące:
   1/ pracowników,
   2/ byłych pracowników,
   3/ osób wykonujących umowy cywilnoprawne,
   4/ kontrahentów;
2. W systemie EGERIA przetwarzane są w szczególności dane:
   1/ identyfikacyjne,
   2/ adresowe,
   3/ o wykształceniu,
   4/ o przebiegu pracy,
   5/ o zakresie obowiązków,
   6/ o stawce wynagrodzenia,
   7/ o karach i nagrodach,
   8/ o stopniu niepełnosprawności,
   9/ o absencjach,
   10/oraz inne dane wymagane zgodnie z Kodeksem pracy.

3. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wynikające z przeprowadzanych analiz ryzyka, wprowadza się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie.

§ 5

3. Kierownik jednostki organizacyjnej zobowiązany jest do niezwłocznego informowania Administratora informatycznego systemu o konieczności zablokowania dostępu, odebrania lub zmiany uprawnień użytkownika, będącego jego podwładnym. Zgłoszenia dokonuje składając wniosek w systemie helpdesk dostępnym pod adresem https://pomoc.uwr.edu.pl.
4. Administrator informatyczny blokuje dostęp konta w systemie EGERIA niezwłocznie:
   1/ po zakończeniu stosunku pracy z użytkownikiem systemu;
   2/ po otrzymaniu informacji o zmianie miejsca zatrudnienia użytkownika systemu;
   3/ po otrzymaniu informacji dotyczącej zagrożenia bezpieczeństwa danych zgromadzonych w systemie.
5. Zablokowanie konta może nastąpić także w przypadku nieużywania konta przez okres trzech miesięcy. Odblokowanie konta następuję w oparciu o procedurę, o której mowa w § 2 ust. 2 i ust. 3.

§ 6

Zobowiązuje się Administratora informatycznego systemu EGERIA do:

3/ przeprowadzania nie rzadziej niż raz na 24 m-ce weryfikacji, czy zestaw przyznanych pracownikowi uprawnień jest odpowiedni dla zadań realizowanych przez pracownika (wynikających m.in. z karty stanowiska pracy);
4/ przeprowadzenia powyższej weryfikacji dla wszystkich aktywnych kont użytkowników systemu w ciągu 30 dni od wejścia w życie niniejszego Regulaminu.

Załącznik Nr 1 do Regulaminu

Wniosek o nadanie/odebranie dostępu do systemów teleinformatycznych UWr

(wzór wydruku elektronicznego wniosku - w miejscach wykropkowanych system podpowiada dozwolone opcje do wyboru)

Nazwa systemu informatycznego lub usługi:

……

Nr wniosku: …….
Data wypełnienia przez wnioskującego: …….
Rodzaj zmiany: ……
(nadanie, odebranie dostępu do systemów)

Użytkownik:

……. , …….
(imię i nazwisko) (nazwa jednostka organizacyjna UWr)

…….
(e-mail służbowy: imię.nazwisko@uwr.edu.pl)

Opis uprawnień:

……., data OD — data DO
(nazwa zestawu uprawnień, roli, zakresu danych, bazy danych) (zakres dat obowiązywania uprawnień)

……
……
(opis uprawnień specjalnych)

Oświadczam, że pracownik został upoważniony do przetwarzania danych osobowych w zakresie adekwatnym do zadań, które ma wykonywać w systemie.

Proszę o nadanie uprawnień

……
(data, podpis wnioskującego - przełożonego pracownika)

Wyrażam zgodę

…… ……
(data, podpis administratora merytorycznego systemu) (data, podpis Inspektora Ochrony Danych Osobowych)

Zrealizowano

……
(data, podpis administratora informatycznego systemu)

Załącznik Nr 2 do Regulaminu

Lp.	Symbol	Nazwa zestawu uprawnień	Jednostki stosujące Zestaw
1	ZU_ANALIZY	Planowanie i analizy finansowe	Dział Planowania i Analiz Finansowych
2	ZU_BHP	BHP komplet	Dział Bezpieczeństwa i Higieny Pracy oraz Ochrony Przeciwpożarowej, Zespół do spraw Bezpieczeństwa i Higieny Pracy
3	ZU_GENRAP	Dostęp do raportów	Sekcja Prac Bibliograficzno-Dokumentacyjnych
4	ZU_GK_OBSERWATOR	Główny Księgowy Obserwator	Główny Księgowy, Zastępca Głównego Księgowego
5	ZU_IT_X_ADMIN	IT Administrowanie systemem	Zespół Aplikacji Centralnych
6	ZU_IT_X_ANALITYK	IT Analizy	Zespół Analityków IT
7	ZU_IT_X_DEVELOPER	IT Programowanie aplikacji pomocniczych	Zespół Aplikacji Centralnych
8	ZU_IT_X_OPERATOR	IT Administrowanie pomocnicze systemem	Dział Usług Informatycznych
9	ZU_KADRY_1_KIER	Sprawy pracownicze, zestaw 1 kierownictwo	Dział Spraw Pracowniczych
10	ZU_KADRY_2_ZAT_I_PPK	Sprawy pracownicze, zestaw 2 zatrudnienia i PPK	Dział Spraw Pracowniczych
11	ZU_KADRY_3_ABS	Sprawy pracownicze, zestaw 3 absencje	Dział Spraw Pracowniczych
12	ZU_KADRY_4_EWID	Sprawy pracownicze, zestaw 4 ewidencja pracowników	Dział Spraw Pracowniczych
13	ZU_KADRY_5_REKRUT	Sprawy pracownicze, zestaw 5 rekrutacja	Sekcja Rekrutacji i Rozwoju Pracowników
14	ZU_KAL_ABS	Kalendarze i absencje	Biblioteka Instytutu Filologii Angielskiej, Biblioteka Instytutu Filologii Germańskiej, Biblioteka Instytutu Filologii Polskiej, Biblioteka Instytutu Filologii Romańskiej, Biblioteka Instytutu Geografii i Rozwoju Regionalnego, Biblioteka Instytutu Historycznego
15	ZU_KAL_ABS_BAD_LEK	Kalendarze i absencje oraz badania lekarskie	Dział Transportu
16	ZU_KAL_ABS_STAZE	Kalendarze i absencje oraz podgląd staży	Dział Ochrony Mienia
17	ZU_ODZIEZ_ROBOCZA	Odzież robocza	Dział Zakupów
18	ZU_PKZP	Obsługa Pracowniczej Kasy Zapomogowo-Pożyczkowej	Sekcja ds. Obsługi Pracowniczej Kasy Zapomogowo-Pożyczkowej
19	ZU_PLACE_1A_KIER	Płace, zestaw 1A, kierownictwo	Dział Płac
20	ZU_PLACE_1B_OS	Płace, zestaw 1B, płace osobowe	Dział Płac
21	ZU_PLACE_2A_WB	Płace, zestaw 2A, wynagrodzenia bezosobowe	Dział Wynagrodzeń Bezosobowych
22	ZU_PLACE_2B_WB	Płace, zestaw 2B, wynagrodzenia bezosobowe	Dział Wynagrodzeń Bezosobowych
23	ZU_PLACE_2C_WB	Płace, zestaw 2C, wynagrodzenia bezosobowe	Dział Wynagrodzeń Bezosobowych
24	ZU_SPRAWY_SOC	Obsługa spraw socjalnych	Sekcja ds. Socjalnych
25	ZU_STRUKTURA	Obsługa struktury organizacyjnej	Dział Organizacyjny
26	ZU_WYPOS_GOSP_NIER	Wyposażenie - gospodarka nieruchomościami	Dział Gospodarki Nieruchomościami, Zespół do spraw Gospodarki Budynkami, Zespół do spraw

			Gospodarki Gruntami
27	ZU_WYPOS_KAMP_GR	Wyposażenie - obsługa Kampusu Grunwaldzkiego	Dział Utrzymania Majątku
28	ZU_WYPOS_OBS_GMACH_GL	Wyposażenie - obsługa Gmachu Głównego	Zespół ds. Obsługi Gmachu Głównego
29	ZU_WYPOS_OBS_INW	Wyposażenie - obsługa inwentaryzacji	Dział Inwentaryzacji
30	ZU_X_ADM_MER	Administracja merytoryczna systemem EGERIA	Dyrektor Generalny
31	ZU_ZESP_FINANS_1	Zespół Finansowy, zestaw 1	Dział Finansowy
32	ZU_ZESP_FINANS_2	Zespół Finansowy, zestaw 2	Dział Finansowy
33	ZU_ZF_X_COMARCH	Zewnętrzna firma: Konsultanci COMARCH	Firma Comarch

Zestaw uprawnień zawiera całość uprawnień użytkownika. Użytkownicy, którym przyznano ten sam zestaw uprawnień posiadają takie same szczegółowe uprawnienia.

Zasady zmiany zawartości dowolnego zestawu uprawnień są opisane w „Procedurze zmiany zestawów uprawnień systemu Egeria”.

Załącznik Nr 15
do zarządzenia Nr 142/2019
z dnia 19 listopada 2019 r.

Zasady użytkowania systemu Pulpity dla Kierowników Projektów w Uniwersytecie Wrocławskim

§ 1

W celu zapewnienia właściwej obsługi systemu informatycznego Pulpity dla Kierowników Projektów zwanego dalej systemem, ustanawia się w Uniwersytecie Wrocławskim:

1. Administratora merytorycznego systemu - w osobie Kierownika Biura Projektów, odpowiedzialnego za:
   a. zatwierdzanie zmian dotyczących parametryzacji systemu,
   b. zatwierdzanie propozycji dotyczących rozwoju systemu,
   c. opracowanie planu rozwoju systemu i stały nadzór nad jego rozwojem,
   d. akceptacja wniosków o nadanie, zmianę, odbiór uprawnień,
2. Administratorów informatycznych systemu – osoby wyznaczone przez Kierownika Działu Usług Informatycznych, będące pracownikami Zespołu Aplikacji Centralnych, odpowiedzialnych za:
   a. zarządzanie użytkownikami, w tym zakładanie i blokowanie kont użytkowników oraz za nadawanie, zmianę i usuwanie uprawnień,
   b. zakładanie profili użytkowników i ich modyfikację,
   c. obsługę zgłoszeń użytkowników w systemie helpdeskowym dotyczących problemów
      z dostępem do oraz działaniem systemu,
   d. zarządzanie procesem zmiany w tym instalację poprawek oraz ich testowanie,
   e. zarządzanie procedurami archiwizowania danych oraz kopiami bezpieczeństwa, w tym tworzenie, kasowanie i odtwarzanie poszczególnych instancji systemu zgodnie z obowiązującą w tym obszarze polityką dla tego oprogramowania,
   f. tworzenie/zarządzanie mechanizmów/mechanizmami wymiany danych z innymi aplikacjami używanymi w Uniwersytecie Wrocławskim (EGERIA, TETA EDU),
   g. zarządzanie zasadami udostępniania aplikacji w Intranecie,
   h. zarządzanie środowiskiem sprzętowo-programowym aplikacji.

§ 2

1. Uprawnienia poszczególnym użytkownikom systemu nadawane są na podstawie wniosku elektronicznego.
2. Wniosek w systemie helpdeskowym składa Kierownik Projektu lub przełożony pracownika występującego o dostęp.
3. Uprawnienia w systemie przydzielane są poprzez przypisanie do użytkownika odpowiedniego profilu uprawnień. Lista profili jest dostępna dla użytkowników składających wnioski w systemie helpdeskowym – Załącznik nr 1.
4. Konta użytkowników są tworzone na okres wskazany we wniosku.

§ 3

1. Konto w systemie tworzone jest indywidualnie dla każdego użytkownika (pracownika) przez administratora informatycznego. Jeden pracownik może posiadać tylko 1 profil uprawnień. Logowanie do systemu odbywa się z użyciem danych dostępowych do konta w usłudze M365.

2. Dostęp poza siecią UWr jest możliwy tylko przy wykorzystaniu aplikacji GlobalProtect (VPN).

§ 4

Uwzględniając kategorię przetwarzanych danych oraz zagrożenia wynikające z przeprowadzanych analiz ryzyka wprowadza się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

§ 5

1. Blokowanie konta użytkownika powinno nastąpić niezwłocznie po otrzymaniu informacji:
    a. o zakończeniu stosunku pracy z użytkownikiem systemu,
    b. o zmianie miejsca zatrudnienia użytkownika systemu,
    c. dotyczącej zagrożenia bezpieczeństwa danych zgromadzonych w systemie.
2. Odebranie uprawnień następuje w nieprzekraczalnym terminie 2 dni roboczych od dnia zablokowania konta.
3. W przypadku wystąpienia sytuacji określonej w § 5 ust. 1, wniosek o zablokowanie dostępu składa kierownik projektu lub przełożony pracownika posiadającego dostęp.

§ 6

Zobowiązuje się administratorów informatycznych systemu Pulpity dla Kierowników Projektów do:

1. Zweryfikowania wszystkich dotychczas utworzonych kont użytkowników systemu w ciągu 30 dni od wejścia w życie niniejszego Regulaminu. Powyższa weryfikacja obejmować będzie sprawdzenie czy pracownik posiadający dostęp figuruje w rejestrze AD oraz czy istniejący już użytkownicy mają dostęp na podstawie wniosków o dostęp.
2. Przeprowadzania cyklicznej weryfikacji kont użytkowników nie rzadziej niż raz na 24 m-ce potwierdzonej protokołem przechowywanym w DUI.

Załącznik Nr 1 do Zasady użytkowania systemu Pulpity dla Kierowników Projektów w Uniwersytecie Wrocławskim

Lista profili dla aplikacji Pulpity dla kierowników

Nazwa profilu	Opis profilu	Uwagi
Kierownik projektu	Użytkownik sprawujący bezpośredni nadzór nad projektem. W ramach systemu widzi tylko przypisane do jego osoby projekty i rozliczenia finansowe. Lista przypisanych projektów wynika z zapisów w systemie TETA.	
Kierownik Biura Projektów	Posiada dostęp do przeglądania wszystkich projektów zapisanych w systemie (otwartych i archiwalnych).	
Księgowa/y	Użytkownik występujący jako uczestnik projektu z określoną funkcją w module Projekty w Teta EDU. W ramach systemu widzi tylko przypisane do jego osoby projekty i rozliczenia finansowe. Lista przypisanych projektów wynika z zapisów w systemie TETA.	
Pracownik adm. wydziału	Użytkownik występujący jako uczestnik projektu z określoną funkcją w module Projekty w Teta EDU. W ramach systemu widzi tylko przypisane do jego osoby projekty i rozliczenia finansowe. Lista przypisanych projektów wynika z zapisów w systemie TETA.	
Pracownik BPR ZPZ	Użytkownik występujący jako uczestnik projektu z określoną funkcją w module Projekty w Teta EDU. W ramach systemu widzi tylko przypisane do jego osoby projekty i rozliczenia finansowe. Lista przypisanych projektów wynika z zapisów w systemie TETA.	
Pracownik BPR ZPK	Użytkownik występujący jako uczestnik projektu z określoną funkcją w module Projekty w Teta EDU. W ramach systemu widzi tylko przypisane do jego osoby projekty i rozliczenia finansowe. Lista przypisanych projektów wynika z zapisów w systemie TETA.	
Pracownik BWM	Użytkownik występujący jako uczestnik projektu z określoną funkcją w module Projekty w Teta EDU. W ramach systemu widzi tylko przypisane do jego osoby projekty i rozliczenia finansowe. Lista przypisanych projektów wynika z zapisów w systemie TETA.	