REGULAMIN KORZYSTANIA Z ZASOBÓW INFORMATYCZNYCH
Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie

§ 1.
Wstęp

1. Niniejszy Regulamin dotyczy wszystkich pracowników i studentów Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, zwanego dalej „Uniwersytetem" albo „Uczelnią" albo „UKSW" oraz osób wykonujących pracę na rzecz Uniwersytetu na podstawie umów cywilno-prawnych, wolontariatu lub B2B oraz związanych z nimi osób.
2. Uniwersytet zabezpiecza przynależne mu zasoby informatyczne (włączając sprzęt komputerowy, oprogramowanie, sieci, system telefoniczny, dane itp.) przed nieautoryzowanym oraz niewłaściwym użyciem.
3. Uniwersytet jako pracodawca udostępnienia pracownikom środowisko pracy z minimalną możliwą liczbą barier. Niemniej jednak, każdy pracownik ma ważną rolę we wspieraniu i stosowaniu się do niniejszego Regulaminu, którego naruszenie może spowodować podjęcie działań korygujących, ze zwolnieniem pracownika włącznie.
4. Centrum Systemów Informatycznych, zwane dalej „CSI", jest jednostką zajmującą się kompleksową obsługą zasobów informatycznych Uniwersytetu oraz ich rozbudową i administracją.
5. Wszelkie wnioski o zakup lub przydzielenie sprzętu IT/AV z zasobów Uczelni, w tym komputerów, oprogramowania czy dostępu do systemów informatycznych, powinny być w pierwszej kolejności konsultowane z CSI w celu weryfikacji ich spójności z istniejącą infrastrukturą informatyczną Uniwersytetu.

§ 2.
Zasoby

1. Uniwersytet jest właścicielem treści wszystkich zasobów i aktywów, włączając: sprzęt komputerowy, oprogramowanie, sieci, system telefoniczny, jak i wszystkie dane przepływające przez sieć Uniwersytecką. Do tych danych zalicza się służbowe wiadomości poczty elektronicznej i głosowej oraz wszystkie dane elektroniczne przechowywane w jakiejkolwiek formie na jakimkolwiek nośniku powstałe w wyniku realizacji obowiązków służbowych.
2. CSI, w odniesieniu do Polityki Bezpieczeństwa Informacji UKSW, ma dostęp do wszystkich zasobów informatycznych będących własnością Uniwersytetu, w celu ich ochrony, konserwacji lub z innych powodów ważnych dla funkcjonowania Uniwersytetu. W szczególności CSI ma dostęp do każdej informacji zawartej w tych zasobach i może ją ujawnić na polecenie Rektora.

§ 3.
Uprawnienia

1. Pracownicy, których zadania wymagają dostępu do kont z większymi uprawnieniami niż konta zwykłego użytkownika (rozumiane tu jako konta administratora systemu), potrzebują dodatkowych wymagań związanych z używaniem i bezpiecznym utrzymywaniem tych kont. Pracownicy, o których mowa w pkt. 1 muszą przesłać do kierownika CSI stosowne pisemne uzasadnienie podlegające weryfikacji technicznej. Po akceptacji uzasadnienia, zostanie zawarta umowa, której wzór stanowi Załącznik nr 1 do niniejszego Zarządzenia.

2. Aby uzyskać dostęp do zasobu przynależnego do innej jednostki, należy złożyć do CSI pisemny wniosek (dostępny w serwisie wnioski.uksw.edu.pl) upoważniający pracownika do uzyskania dostępu do tego zasobu. Wniosek musi zostać zaakceptowany przez osobę zarządzającej danym zasobem.
3. Aby uzyskać dostęp do zasobu zawierającego dane osobowe, należy postępować zgodnie z wytycznymi Polityki Bezpieczeństwa Informacji na UKSW.

§ 4.
Ograniczenia

Zabrania się pracownikom Uniwersytetu:

1) samodzielnej naprawy, przeróbki, rozbudowy lub ingerencji w podstawową konfigurację sprzętu komputerowego oraz systemów informatycznych;
2) instalowania lub usuwania oprogramowania bez uzgodnienia z CSI;
3) wykorzystywania sieci firmowej do nielegalnego ściągania i przesyłania materiałów chronionych prawem autorskim oraz przechowywania w zasobach informatycznych Uniwersytetu takich materiałów;
4) przesyłania danych i dokumentów firmowych przez komunikatory internetowe i sieci P2P;
5) korzystania w trakcie pracy z serwisów ewidentnie niezwiązanych w zakresem wykonywanych obowiązków służbowych (np. serwisy randkowe, pornograficzne oraz udostępniające treści zakazane prawem lub treści chronione prawem autorskim);
6) podłączania do gniazdek lub listw zasilających sprzęt komputerowy urządzeń o dużym poborze mocy, takich jak: czajniki elektryczne, grzejniki, radia itp.;
7) usuwania lub przerabiania oznaczeń z numerami inwentarzowymi, licencyjnymi lub innymi, którymi sprzęt został oznaczony;
8) zmiany lokalizacji sprzętu komputerowego bez zachowania procedury zarządzania majątkiem w systemie HSM.

§ 5.
Bezpieczeństwo

1. Wszystkich pracowników obowiązuje Polityka Bezpieczeństwa Informacji UKSW.
2. Pracownicy są zobowiązani do zachowania poufności swoich haseł komputerowych.
3. Pracownicy nie powinni zapisywać swoich haseł w pisemnej lub elektronicznej postaci, chyba że są to ich początkowe (startowe) lub ponownie wygenerowane hasła, które mają tymczasowy okres ważności.
4. Zabrania się przekazywania swoich danych identyfikacyjnych innym osobom oraz nieautoryzowanego używania identyfikacji systemowej, loginów czy przywilejów przypisanych do loginów dla celów innych niż służbowe.
5. Pracownicy, którzy próbują odkryć hasła, uzyskać dostęp do ograniczonych zasobów komputerowych, naruszają niniejszy regulamin i narażają się na działania korygujące, w tym możliwość zablokowania konta.
6. Zabrania się pracownikom nieautoryzowanego dostępu i modyfikacji plików komputerowych niebędących ich własnością, nawet, jeśli nie ma ograniczenia dostępu lub nie ma ochrony pliku.

Pracownik nie ma pozwolenia na dostęp lub modyfikację takich plików, chyba że posiada stosowne zezwolenie od właściciela pliku. Taki dostęp jest wykroczeniem, jest uważany za nieetyczny i może spowodować podjęcie działań dyscyplinarnych. Jeśli pracownik nie jest pewien, czy ma właściwe prawa dostępu do plików, powinien skonsultować się ze swoim przełożonym.

7. Osoby niezatrudnione w Uniwersytecie mają obowiązek uzyskać autoryzację do dostępu do zasobów firmowych poprzez podpisanie Klauzuli Poufności, zgodnie z Polityka Bezpieczeństwa Informacji UKSW.
8. Pracownicy i studenci mają obowiązek zgłaszać wszelkie sytuacje, które wskazują potencjalne ryzyko lub naruszenie bezpieczeństwa zasobów informatycznych bezpośrednio do CSI i administratora ochrony danych osobowych IOD poprzez wypełnienie formularza dostępnego pod adresem: https://uksw.edu.pl/pl/odo-naruszenia.

§ 6.
Odpowiedzialność

1. Pracownicy odpowiadają za powierzony im sprzęt komputerowy mają obowiązek chronić go przed negatywnym wpływem czynników zewnętrznych, zniszczeniem, utratą oraz modyfikacją lub skasowaniem danych przez osoby nieuprawnione.
2. Pracownicy mają obowiązek używania zasobów informatycznych Uniwersytetu zgodnie z ich przeznaczeniem, w sposób umiejętny i wydajny, w celu osiągnięcia celów służbowych.
3. Świadoma działalność pracownika o charakterze dywersyjnym, mająca na celu zakłócenie normalnej pracy w zasobach informatycznych Uniwersytetu, stanowi poważne naruszenie niniejszego regulaminu i może spowodować podjęcie działań dyscyplinarnych, ze zwolnieniem pracownika i innymi sankcjami prawnymi włącznie.
4. W wyjątkowych sytuacjach na wniosek pracownika, Uniwersytet dopuszcza używanie do celów służbowych prywatnego sprzętu komputerowego. Na prywatnym sprzęcie nie może być zainstalowane licencyjne oprogramowanie będące własnością Uniwersytetu, a pracownik używa prywatnego oprogramowania do celów służbowych na własne ryzyko i ponosi odpowiedzialność przed licencjodawcą tego oprogramowania.
5. Prywatny sprzęt powinien być oznaczony nalepką „Własność prywatna - Imię i nazwisko właściciela".
6. Przed rozpoczęciem pracy na prywatnym sprzęcie musi on zostać poddany audytowi bezpieczeństwa przez CSI, i jeśli to konieczne dodatkowo zabezpieczony na koszt właściciela. Na właścicielu sprzętu spoczywa obowiązek utrzymania bezpieczeństwa sprzętu na odpowiednim poziomie, pod rygorem pokrycia wszelkich szkód jakie ten sprzęt wyrządzi w zasobach informatycznych Uniwersytetu.

§ 7.
Poczta elektroniczna

Szczegółowe zasady korzystania z poczty elektronicznej określa Regulamin systemu poczty elektronicznej UKSW wprowadzony odrębnym Zarządzeniem Rektora.

§ 8.
Zgłaszanie i usuwanie usterek

1. Problemy ze sprzętem komputerowym lub systemem informatycznym należy zgłosić do sekcji „Helpdesk" CSI z zachowaniem kolejności podanych poniżej kanałów komunikacyjnych:

1) poprzez zgłoszenie elektroniczne dostępne pod adresem https://csi.uksw.edu.pl/zgloszenie/;
2) poprzez wysłania zgłoszenia opisującego problem na adres e-mail zgloszenia@uksw.edu.pl ;
3) w przypadku braku dostępności do sieci Internet telefonicznie pod nr 22 5618921 lub wew. 321.

2. Nie jest zalecane zgłaszanie usterek okazjonalnie spotkanym pracownikom CSI, jak również zgłaszanie problemów bezpośrednio na imienne maile pracowników. Czas obsługi takich zgłoszeń może się znacząco wydłużać, ponieważ pracownicy w pierwszej kolejności wykonują zlecenia, z terminowości których są rozliczani.
3. Zgłaszając usterkę należy podać:
   1) imię i nazwisko;
   2) dane kontaktowe np. numer telefonu, adres poczty elektronicznej;
   3) w miarę dokładny opis problemu;
   4) wskazanie numeru inwentarzowego sprzętu której usterka dotyczy (jak występuje);
   5) lokalizację, w której usterka wystąpiła.
4. Każde zgłoszenie techniczne jest rejestrowane w elektronicznym systemie zgłoszeń. Tylko zarejestrowane zgłoszenia podlegają reklamacji.
5. Niektóre zgłoszenia zanim zostaną przyjęte do realizacji (np. nadanie uprawnień do systemu informatycznego) wymagają dodatkowego wniosku w formie pisemnej. Generator wniosków dostępny w serwisie https://wnioski.uksw.edu.pl .