Regulamin korzystania z zasobów informatycznych Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie

§ 1. Wstęp

Uniwersytet chroni przynależne mu zasoby informatyczne (włączając sprzęt komputerowy, oprogramowanie, sieci, system telefoniczny, dane itp.) przed nieautoryzowanym oraz niewłaściwym użyciem.

1. Niniejszy regulamin dotyczy wszystkich pracowników Uniwersytetu, oraz osób wykonujących pracę na rzecz Uniwersytetu na podstawie umów cywilno prawnych, ich pomocników oraz związanych z nimi osób.
2. Nie ogranicza się dostępu pracownika do zasobów komputerowych. Celem Uniwersytetu jako pracodawcy jest udostępnienie pracownikom środowiska pracy z minimalną możliwą liczbą barier. Niemniej jednak, każdy pracownik ma ważną rolę we wspieraniu i stosowaniu się do tego regulaminu. Naruszenie regulaminu może spowodować podjęcie działań korygujących, ze zwolnieniem pracownika włącznie.
3. Centrum Systemów Informatycznych Uniwersytetu, zwane dalej CSI jest jednostką zajmującą się kompleksową obsługą zasobów informatycznych Uniwersytetu oraz ich rozbudową.
4. Wszelkie wnioski o zakup lub przydzielenie sprzętu komputerowego, oprogramowania czy dostępu do systemów informatycznych, powinny być w pierwszej kolejności kierowane do 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, dane, jak i wszystkie dane przepływające przez sieć Uniwersytecką. Do tych danych zalicza się wiadomości poczty elektronicznej i głosowej (włączając osobiste wiadomości przesyłane na służbowy adres) oraz wszystkie dane elektroniczne przechowywane w jakiejkolwiek formie na jakimkolwiek nośniku.
2. CSI 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 Rektorowi, Prorektorom lub Kanclerzowi.
3. Od pracowników Uniwersytetu wymaga się, aby – na wniosek kierownika CSI, zaakceptowany przez ABI – udostępnili wszelkie dane zapisane na powierzonym im przez Uniwersytet nośniku**.**

§ 3. Uprawnienia

1. Pracownicy, których zadania wymagają dostępu do kont z większymi uprawnieniami niż konta zwykłego pracownika (rozumiane tu jako konta administratora systemu) są przedmiotem dodatkowych wymagań związanych z używaniem i bezpiecznym utrzymywaniem tych kont. Pracownicy, którzy wymagają tego specjalnego dostępu muszą wypełnić i podpisać stosowny wniosek i umowę odpowiedzialności.
2. Aby uzyskać dostęp do zasobu, należy dostarczyć do CSI pisemny wniosek od właściciela zasobu, upoważniający pracownika do uzyskania dostępu do tego zasobu.
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 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 nie związanych 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 itp.,
7. usuwania lub przerabiania oznaczeń z nr inwentarzowymi, licencyjnymi lub innymi, którymi sprzęt został oznaczony,
8. zmiany lokalizacji sprzętu komputerowego bez uzgodnienia z CSI oraz Działem Administracyjno – Gospodarczym.

§ 5. Bezpieczeństwo

1. Wszystkich pracowników obowiązuje Polityka Bezpieczeństwa Informacji.
2. Pracownicy są zobowiązani do zachowania poufności swoich haseł komputerowych. Hasło powinno się składać z minimum 8 znaków w tym przynajmniej z jednej cyfry i znaku specjalnego.
3. Pracownicy nie powinni zapisywać swoich haseł w pisemnej lub elektronicznej postaci, chyba, że są to ich początkowe lub ponownie ustalane hasła, które mają trzydniowy lub krótszy okres ważności.
4. Zabrania się nieautoryzowanego używania identyfikacji systemowej, loginów czy przywilejów przypisanych do loginów dla celów innych niż służbowe.
5. Pracownicy, którzy usiłują odkryć hasła, uzyskać dostęp do ograniczonych zasobów komputerowych naruszają niniejszy regulamin i narażają się na działania korygujące.
6. Zabrania się pracownikom nieautoryzowanego dostępu i modyfikacji plików komputerowych nie będących 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 korygujących. Jeśli pracownik nie jest pewien, czy ma właściwe prawa dostępu do plików, powinien skonsultować się ze swoim przełożonym.
7. Pracownicy, którzy przyczyniają się do dostępu do chronionych zasobów informatycznych Uniwersytetu przez nieuprawnione osoby naruszają niniejszy regulamin.
8. Osoby niezatrudnione w Uniwersytecie mają obowiązek uzyskać autoryzację do dostępu do zasobów firmowych poprzez podpisanie Klauzuli Poufności.
9. Pracownicy i studenci mają obowiązek zgłaszać wszelkie sytuacje, które wskazują potencjalne ryzyko lub naruszenie bezpieczeństwa zasobów informatycznych bezpośrednio do CSI.

§ 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 korygujących, 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, prywatny sprzęt musi zostać poddany audytowi bezpieczeństwa przez CSI, i jeśli to konieczne dodatkowo zabezpieczony. 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

1. Do obsługi służbowych wiadomości poczty elektronicznej, pracownik powinien posługiwać się kontem pocztowym w domenie będącej własnością Uniwersytetu, obsługiwanym przez wskazane przez CSI programy pocztowe.
2. Pracownik ma obowiązek dołożyć wszelkich starań, by przy przesyłaniu wiadomości poczty elektronicznej, programy pasożytnicze i niebezpieczne załączniki nie trafiły do systemów Uniwersytetu lub systemów adresatów tych wiadomości.
3. Zabrania się pracownikom automatycznego przekierowywania służbowej poczty elektronicznej na zewnętrzne konta nie będące kontami służbowymi. Zakaz dotyczy również automatycznego pobierania poczty służbowej poprzez konta nie będące kontami służbowymi Uniwersytetu.
4. Pracownicy powinni szanować przydzielony im służbowy adres poczty elektronicznej, w miarę możliwości ograniczyć podawanie go na stronach o wątpliwym poziomie zaufania. Wykradnięcie adresu przez systemy spamujące jest nieodwracalne i naraża systemy antyspamowe Uniwersytetu na duże obciążenie.

§ 8. Zgłaszanie i usuwanie usterek

1. Problemy ze sprzętem komputerowym lub systemem informatycznym należy zgłosić go do sekcji „Help Desk" CSI z zachowaniem w miarę dostępności, kolejności podanych poniżej kanałów komunikacyjnych:
   poprzez stronę internetową www.csi.uksw.edu.pl,
   telefonicznie, pod nr 888 lub 321,
   osobiście, ul. Dewajtis 5 pok. 102 starego gmachu,
   pocztą elektroniczną na adres helpdesk@csi.uksw.edu.pl .
   Nie jest zalecane zgłaszanie usterek okazjonalnie spotkanym pracownikom CSI. Czas obsługi takich zgłoszeń może się wydłużać, ponieważ pracownicy w pierwszej kolejności wykonują zlecenia, z terminowości których są rozliczani.
2. Zgłaszając usterkę należy podać:
   imię i nazwisko osoby lub jednostkę której usterka dotyczy,
   lokalizację w której usterka wystąpiła,
   w miarę dokładny opis problemu,
   dane kontaktowe np. numer telefonu, adres poczty elektronicznej.
3. Każde zgłoszenie jest rejestrowane w elektronicznym systemie zgłoszeń. Status zgłoszenia można sprawdzać na stronie CSI lub telefonicznie podając nr zgłoszenia.
4. Tylko zarejestrowane zgłoszenia podlegają reklamacji.
5. Niektóre zgłoszenia zanim zostaną przyjęte do realizacji (np. nadanie uprawnień do systemu informatycznego) wymagają specjalnego wniosku w formie pisemnej. Generator i szablony wniosków znajdują się na stronie internetowej CSI.