REGULAMIN KORZYSTANIA Z LABORATORIÓW KOMPUTEROWYCH

Instytutu Bezpieczeństwa i Informatyki

1. Definicje

1. **Administrator techniczny infrastruktury laboratoryjnej -** Osoba lub zespół wyznaczony przez Instytut Bezpieczeństwa i Informatyki odpowiedzialny za utrzymanie, konfigurację, bezpieczeństwo oraz ciągłość działania infrastruktury laboratoryjnej oraz serwerowni Instytutu Bezpieczeństwa i Informatyki. Administrator techniczny może realizować swoje zadania samodzielnie lub za pośrednictwem upoważnionego podmiotu zewnętrznego.
2. **Podmiot zewnętrzny (operator infrastruktury) -** Wyspecjalizowany podmiot techniczny działający na podstawie umowy z Instytutem Bezpieczeństwa i Informatyki, odpowiedzialny za bieżące utrzymanie, administrację oraz rozwój infrastruktury laboratoryjnej i serwerowni Instytutu. Podmiot zewnętrzny wykonuje czynności administracyjne w zakresie określonym przez administratora technicznego.
3. **Prowadzący zajęcia -** Osoba prowadząca zajęcia dydaktyczne w laboratoriach Instytutu Bezpieczeństwa i Informatyki, odpowiedzialna za organizację i przebieg procesu dydaktycznego w trakcie zajęć laboratoryjnych.
4. **Infrastruktura laboratoryjna -** Zespół zasobów obejmujący w szczególności komputery laboratoryjne, urządzenia sieciowe, serwery, systemy wirtualizacji, usługi sieciowe oraz wydzielone segmenty sieciowe wykorzystywane w procesie dydaktycznym i badawczym. Infrastruktura laboratoryjna obejmuje również serwerownię Instytutu Bezpieczeństwa i Informatyki wraz z całą infrastrukturą sieciową, systemową i teleinformatyczną.
5. **Infrastruktura centralna uczelni -** Odrębna od infrastruktury laboratoryjnej infrastruktura teleinformatyczna zarządzana przez centralną jednostkę IT uczelni, obejmująca w szczególności sieć szkieletową, usługi centralne oraz systemy ogólnouczelniane.

2. Zasady ogólne

1. Laboratoria komputerowe służą wyłącznie do celów dydaktycznych, naukowych oraz badawczych.
2. Z laboratoriów mogą korzystać wyłącznie studenci, pracownicy oraz osoby upoważnione przez Uczelnię.
3. Korzystanie z laboratoriów możliwe jest wyłącznie w godzinach ich udostępnienia.
4. Laboratoria stanowią wydzielone środowisko dydaktyczno-badawcze wymagające odrębnych zasad administracji i bezpieczeństwa.

3. Korzystanie ze sprzętu

1. Używaj sprzętu zgodnie z jego przeznaczeniem.
2. Zabrania się instalowania, usuwania lub modyfikowania oprogramowania bez zgody prowadzącego zajęcia lub administratora infrastruktury.
3. Zabrania się zmiany konfiguracji systemów, sprzętu oraz usług sieciowych.
4. Wszelkie modyfikacje dozwolone są wyłącznie za zgodą prowadzącego zajęcia lub administratora infrastruktury.
5. Usterki należy zgłaszać prowadzącemu zajęcia lub administratorowi technicznemu.
6. Po zakończeniu pracy należy uporządkować stanowisko.

4. Zasady bezpieczeństwa i etyki

1. Użytkownicy korzystają wyłącznie z własnych kont.
2. Zabrania się udostępniania danych logowania.
3. Zabrania się:
    1. instalowania gier,
    2. działań komercyjnych,
    3. działań niezgodnych z prawem,
    4. omijania zabezpieczeń systemów i infrastruktury uczelnianej lub laboratoryjnej,
    5. prób nieautoryzowanego dostępu do systemów, usług lub urządzeń sieciowych,
    6. skanowania sieci, portów oraz usług,
    7. wykonywania działań ofensywnych (w tym prób ataków, eksploitacji, podsłuchiwania ruchu sieciowego, przechwytywania danych lub eskalacji uprawnień).
4. Działania związane z analizą bezpieczeństwa, testami penetracyjnymi, skanowaniem, symulacją ataków oraz innymi technikami cyberbezpieczeństwa mogą być realizowane wyłącznie:
    1. w ramach zajęć dydaktycznych,
    2. na wyraźne polecenie prowadzącego zajęcia,
    3. w zakresie i środowisku przez niego określonym,
    4. z wykorzystaniem infrastruktury laboratoryjnej przeznaczonej do tego celu.

5. Porządek i zachowanie

1. Należy zachować ciszę i kulturę osobistą.
2. Zabrania się spożywania jedzenia i napojów przy stanowiskach.

3. Rzeczy osobiste należy pozostawić w wyznaczonym miejscu.
4. Należy dbać o sprzęt i środowisko pracy.

6. Odpowiedzialność

1. Użytkownik ponosi odpowiedzialność materialną za szkody wyrządzone z jego winy.
2. Uczelnia nie odpowiada za dane pozostawione na komputerach.
3. Naruszenie regulaminu może skutkować utratą prawa do korzystania z laboratoriów oraz konsekwencjami dyscyplinarnymi.

7. Administracja i utrzymanie infrastruktury

1. Za utrzymanie, konfigurację, bezpieczeństwo oraz ciągłość działania infrastruktury laboratoryjnej i serwerowni Instytutu Bezpieczeństwa i Informatyki odpowiada administrator techniczny lub podmiot zewnętrzny.
2. Dostęp administracyjny do infrastruktury posiadają wyłącznie osoby upoważnione przez Instytut Bezpieczeństwa i Informatyki.
3. Centralna administracja uczelni nie dokonuje zmian w infrastrukturze laboratoryjnej bez uzgodnienia z administratorem technicznym.
4. Wszelkie zmiany konfiguracji infrastruktury wymagają akceptacji administratora technicznego.

8. Specyfika środowiska cyberbezpieczeństwa

1. Laboratoria wykorzystywane są do zajęć z zakresu cyberbezpieczeństwa, administracji systemami, analizy incydentów oraz testów bezpieczeństwa.
2. W trakcie zajęć infrastruktura może wymagać:
    1. izolacji sieciowej,
    2. rekonfiguracji usług,
    3. ograniczenia dostępu do Internetu,
    4. uruchamiania środowisk testowych.
3. Prowadzący zajęcia jest uprawniony do podejmowania decyzji operacyjnych dotyczących bieżącej konfiguracji środowiska laboratoryjnego.

9. Reagowanie na incydenty i ciągłość działania

1. Prowadzący zajęcia może natychmiastowo zdecydować o:

    1. izolacji sieci,
    2. odłączeniu od Internetu,
    3. blokowaniu ruchu,
    4. przywracaniu dostępu.
2. Administrator techniczny lub prowadzący zajęcia realizuje te decyzje niezwłocznie.
3. W przypadku incydentów bezpieczeństwa działania prowadzone są równolegle przez prowadzącego zajęcia i administratora technicznego.
4. Działania mają priorytet zapewnienia bezpieczeństwa i ciągłości dydaktyki.

10. Wymagania techniczne środowiska

1. Dopuszcza się stosowanie:
    1. systemów automatycznego wdrażania środowisk,
    2. usług provisioningowych,
    3. lokalnych usług zarządzania siecią,
    4. wydzielonych mechanizmów adresacji i konfiguracji,
    5. systemów monitorowania bezpieczeństwa.

11. Dostępność i wsparcie techniczne

1. Utrzymanie infrastruktury realizowane jest w trybie ciągłym, zgodnie z potrzebami dydaktycznymi i wymaganiami bezpieczeństwa.
2. Wsparcie techniczne realizuje administrator techniczny lub podmiot zewnętrzny.