Uniwersytet Wrocławski

WYDZIAŁ NAUK O ZIEMI I KSZTAŁTOWANIA ŚRODOWISKA

DZIEKANAT
ul. Kuźnicza 35
50-138 Wrocław

tel. +48 71 375 27 89 | +48 71 375 24 62

dziekan.wnzks@uwr.edu.pl | www.wznoz.uni.wroc.pl

ZARZĄDZENIE Nr 8/2018

Dziekana Wydziału Nauk o Ziemi i Kształtowania Środowiska UWr
z dnia 16 kwietnia 2018 r.

w sprawie wprowadzenia wewnętrznego regulaminu użytkowania sieci lokalnej na Wydziale Nauk o Ziemi i Kształtowania Środowiska Uniwersytetu Wrocławskiego

Na podstawie Zarządzeniem Rektora UWr Nr 142/2017 z dnia 14 grudnia 2017 r (§ 4 ust. 2 Załącznika Nr 2) do Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasady korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego zarządza się , co następuje

§1

Wprowadza się wewnętrzny regulamin użytkowania sieci lokalnej na Wydziale Nauk o Ziemi i Kształtowania Środowiska Uniwersytetu Wrocławskiego , który stanowi załącznik do niniejszego zarządzenia.

§2

Obowiązki administratora lokalnej sieci komputerowej powierza się wydziałowemu informatykowi .

§3

1. Zarządzenie wchodzi w życie z dniem ogłoszenia.
2. Nadzór nad wykonaniem zarządzenia powierza się prodziekanowi ds. studenckich

Dziekan

dr hab. Henryk Marszałek prof. UWr

Załącznik

Wewnętrzny regulamin użytkowania sieci lokalnej

Regulamin ustala szczegółowe zasady korzystania z infrastruktury informatycznej na Wydziale Nauk o Ziemi i Kształtowania Środowiska.

Postanowienia Regulaminu są zgodne z przepisami obowiązującymi w Uczelni, w szczególności z Zarządzeniem Rektora nr 142/2017 z dnia 14 grudnia 2017 roku w sprawie wprowadzenia Regulaminu bezpieczeństwa informacji przetwarzanych w systemach informatycznych oraz zasad korzystania z infrastruktury informatycznej Uniwersytetu Wrocławskiego.

Wszyscy użytkownicy zobowiązani są do zapoznania się z regulaminem i przestrzegania jego zapisów, korzystania z sieci zgodnie z zadaniami, do których została utworzona.

W przypadku nie przestrzegania zasad, zawartych w zarządzeniu i wewnętrznym regulaminie, administrator sieci w drodze decyzji może czasowo ograniczyć lub zablokować dostęp do sieci. O naruszeniu obowiązujących zasad użytkownika powiadamiany jest bezpośredni przełożony użytkownika (w przypadku studentów i doktorantów - dziekan).

Za funkcjonowanie sieci lokalnej w obiektach należących do wydziału odpowiada **wydziałowy informatyk**, który w tym przedmiocie pełni rolę **administratora lokalnej sieci komputerowej**.

Podstawowe definicje

1.**Lokalna sieć komputerowa** - wydzielony fragment Sieci Uczelnianej administrowany przez jednostkę organizacyjną, obejmuje komputery, serwery i infrastrukturę komunikacyjną jednostki organizacyjnej, który podlega kierownikowi jednostki.

2. **Administrator lokalny-** osoba upoważniona i zobowiązana do realizacji zadań związanych z zarządzaniem systemami informatycznymi

3.**Stacja robocza** - komputer (stacjonarny lub przenośny), na którym zainstalowano system operacyjny zawierający profil użytkownika,

4**. Administrator stacji roboczej** - administrator lokalny lub użytkownik , któremu nadano uprawnienia administracyjne do danej stacji roboczej tzw. **użytkownik zaawansowany**

5.**Użytkownik** - osoba, która ma uprawnienia do korzystania z danego systemu informatycznego zgodnie z przeznaczeniem, bez uprawnień administracyjnych.

<u>Odpowiedzialność</u>

1. Każdy pracownik ma obowiązek zachować w tajemnicy przetwarzane dane osobowe oraz informacje o sposobach ich zabezpieczenia.
2. Za bezpieczeństwo informacji przetwarzanych w sieciach lokalnych podległych jednostek odpowiada dziekan, w tym w zakresie :

- posiadania informacji o sprzęcie komputerowym i oprogramowaniu,

- aktualizacji oprogramowania, w tym programów zabezpieczających i systemów operacyjnych,
- kontroli legalności zainstalowanego oprogramowania i plików,
- stosowania mechanizmów bezpieczeństwa informatycznego, w tym nadawania i odbierania uprawnień, wykrywania nieautoryzowanych działań, wykrywania złośliwych aplikacji, rejestracji incydentów i usuwania ich przyczyn,
- przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności przetwarzanych danych oraz podejmowania działań minimalizujących to ryzyko.

Zarządzanie uprawnieniami

1. Wszystkie osoby, które korzystają ze służbowych komputerów będących na stanie inwentarzowym Wydziału , są użytkownikami przypisanych do nich stacji roboczych. Komputery przenośne , które są własnością Uniwersytetu podlegają tym samym regułom ochrony jak komputery stacjonarne.
2. W przypadku korzystania z przenośnej stacji roboczej poza miejscem pracy Użytkownik zobowiązany jest do przestrzegania zasad bezpiecznego użytkowania w szczególności nie dopuszczania osób trzecich do użytkowania sprzętu i podłączania go wyłącznie do chronionych sieci bezprzewodowych.
3. Status użytkownika zaawansowanego tj. administratora stacji roboczej nadaje się wszystkim osobom indywidualnie użytkującym sprzęt.
1. W odniesieniu do komputerów , do których dostęp ma więcej niż jeden użytkownik w:
    - pracowniach komputerowych
    - na salach dydaktycznych
    - w bibliotekach

oraz w sekretariatach instytutów i dziekanacie administratora stacji roboczych wyznacza kierownik jednostki.

Obowiązki i prawa administratora stacji roboczej i użytkownika

1. Administrator stacji roboczej zobowiązany jest do :

a. regularnego aktualizowania systemu operacyjnego oraz oprogramowania komputera,
b. tworzenia kopii zapasowych nie dłuższym odstępie czasu niż 14 dni roboczych, kopie powinny być przechowywane na zewnętrznym nośniku typu dysk HDD lub w usłudze OneDrive pakietu office 365 ,gdzie każdy z pracowników ma dostęp do przestrzeni o pojemności 1TB,
c. informowania administratora lokalnego o zakupie stacji roboczej lub oprogramowania - informacja powinna zawierać:
    - typ i numer ewidencyjny komputera
    - nazwę oprogramowania
    - informację o posiadanej licencji
    - datę zakupu i nr faktury
d. informowania administratora lokalnego o zmianie lokalizacji komputerów i innych urządzeń stacjonarnych podłączonych do sieci komputerowej,
e. zapewnienia - przy udziale informatyka wydziałowego - funkcjonowania oprogramowania do elektronicznej inwentaryzacji Kaseya.

2. **Użytkownik -** nie może , bez wiedzy i pisemnej zgody administratora sieci lokalnej:

a. podłączać do sieci lokalnej żadnych urządzeń typu: routery, access pointy, switche, za wyjątkiem urządzeń służbowych,

b. instalować oprogramowania nielegalnego oraz niezwiązanego merytorycznie z wykonywaną pracą a w szczególności oprogramowania, którego eksploatacja jest sprzeczna z Ustawą o prawach autorskich i prawach pokrewnych,

c. dokonywać jakichkolwiek zmian w konfiguracji sieciowej komputerów i innych urządzeń podłączonych do wydziałowej sieci w szczególności zmieniać adresów IP i MAC,

d. wykorzystywać sprzętu, sieci lub oprogramowania dla celów komercyjnych i nie związanych z zakresem działalności jednostki.

3. Dopuszcza się, instalowanie - w celach służbowych - oprogramowania darmowego (freewar-owego) .

Zestaw programów freeware akceptowalnych w sieci lokalnej znajduje się na stronie internetowej wydziału.

4. W celu zapobieżenia nieautoryzowanemu dostępowi do Systemu użytkownik:

a. nie może przechowywać danych służących do logowania do Systemu w miejscach dostępnych dla innych osób,

b. nie może ujawniać danych służących do logowania innym osobom.

Ochrona antywirusowa

1. Komputery i systemy pracujące w SI powinny mieć zainstalowane -wyłącznie - oprogramowania antywirusowego ESET **Endpoint Antivirus**
   - system operacyjny powinien mieć włączone aktualizacje automatyczne,
   - oprogramowanie antywirusowe powinno być skonfigurowane tak ,aby aktualizowało się automatycznie,
   - stacja robocza musi zostać przeskanowana przez administratora minimum raz w miesiącu,
2. Elektroniczne nośniki informacji należy każdorazowo sprawdzać programem antywirusowym przed użyciem, w trakcie użytkowania monitorować komunikaty pochodzące z oprogramowania antywirusowego zainstalowanego na stacji roboczej i reagować na nie.

3. W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia lub rozpozna tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z administratorem lokalnym.

4. Przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabronione jest otwieranie załączników i wiadomości poczty elektronicznej od „niezaufanych” nadawców.

Zabezpieczenie elektronicznych nośników informacji

Użytkownicy zobowiązani są do ochrony plików zawierających dane osobowe . W każdym przypadku muszą mieć pewność , że dostęp do tych plików jest zaszyfrowany.

Lista dopuszczalnych programów szyfrujących znajduje się na stronie internetowej wydziału.

Usuwanie danych z urządzeń/nośników

1. Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania.

2. W sytuacji gdy sprzęt lub nośniki, na których znajdują się dane osobowe, mają zostać:

- przekazane innej jednostce organizacyjnej;
- przekazane do naprawy wraz z nośnikami, na których zapisane są dane osobowe bez zapewnienia zawarcia umowy o poufności z firmą serwisującą;
- przekazane do zniszczenia

należy zadbać o skuteczne usunięcie danych zebranych na tych nośnikach poprzez wymontowanie lub wyczyszczenie.

3. Wybór sposobu kasowania danych należy do użytkownika.

4. Nośniki danych przeznaczone do utylizacji - po wcześniejszym usunięciu z nich wszystkich danych - należy przekazać do administratora lokalnego.

Zgłaszanie incydentów, usterek i awarii

1. W przypadku stwierdzenia naruszenia ochrony informacji, w szczególności zaistnienia zdarzenia zagrażających bezpieczeństwu danych pracownik zobowiązany jest natychmiast powiadomić o zaistniałym zdarzeniu bezpośredniego przełożonego i administratora sieci lokalnej.

2. Administrator lokalny odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia, i ma obowiązek kontrolowania i zabezpieczenia prawidłowości przebiegu czynności serwisowych.

3. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

Dziekan: dr hab. Henryk Marszałek prof. UWr