Załącznik do Zarządzenia nr …/2023

Rektora UPP z dnia 27 listopada 2023 r.

Regulamin użytkowania i zarządzania komputerami służbowymi oraz Uczelnianą Siecią Komputerową UPNet Uniwersytetu Przyrodniczego w Poznaniu

§1
Postanowienia ogólne

1. Niniejszy regulamin określa zasady użytkowania i zarządzania komputerami służbowymi w Uczelnianej Sieci Komputerowej Uniwersytetu Przyrodniczego w Poznaniu (UPP), zwaną dalej UPNet.
2. Zadaniem UPNet jest wspomaganie działalności naukowej, dydaktycznej i administracyjnej prowadzonej w Uniwersytecie Przyrodniczym w Poznaniu.
3. Użytkownikami UPNet mogą być pracownicy, doktoranci i studenci Uniwersytetu Przyrodniczego w Poznaniu oraz przedstawiciele innych uczelni związani tymczasowo swoją działalnością z Uniwersytetem Przyrodniczym w Poznaniu. Użytkownikami komputerów służbowych UPP mogą być pracownicy, doktoranci i studenci Uniwersytetu Przyrodniczego w Poznaniu.
4. Użytkownicy UPNet oraz komputerów służbowych UPP mają obowiązek stosować się do wymogów niniejszego Regulaminu oraz zaleceń Ośrodka Informatyki w zakresie spraw dotyczących UPNet oraz użytkowania komputerów służbowych.
5. Każde działanie w ramach UPNet musi być zgodne z prawem polskim, europejskim, międzynarodowym, zasadami etyki i współżycia społecznego oraz mieć na uwadze zachowanie bezpieczeństwa i poufności informacji.
6. Utwory w formie elektronicznej, których dotyczy prawo autorskie lub prawa pokrewne, odnośnie własności intelektualnej i prawnej do: oprogramowania, muzyki, filmów i innych utworów, podlegają specjalnemu nadzorowi w sieci UPNet, ze względu na łatwość naruszenia praw do tych utworów.

§2
Organizacja i zarządzanie UPNet

1. Sieć UPNet tworzą:
   a) sieć światłowodowa,
   b) główne i lokalne węzły dostępowe umiejscowione w budynkach Uniwersytetu Przyrodniczego w Poznaniu,
   c) zasoby sieciowe w postaci: serwerów, okablowania strukturalnego oraz oprogramowania sieciowego, baz danych i usług sieciowych, zainstalowanych na serwerach Ośrodka Informatyki,
   d) lokalne sieci komputerowe poszczególnych budynków,
   e) stacje robocze użytkowników wraz z oprogramowaniem.
2. Administratorem sieci UPNet jest Ośrodek Informatyki.
3. Ośrodek Informatyki ma prawo do wykorzystywania programów do analizy ruchu sieciowego, w celach diagnostycznych, związanych z bezpieczeństwem sieci.
4. Ośrodek Informatyki jest jedyną jednostką upoważnioną do przydzielania adresów sieciowych i nazw komputerów włączanych do UPNet.
5. Serwery usług zlokalizowane są w Centrum Sieciowym i zarządzane przez Ośrodek Informatyki. W szczególnych przypadkach jednostki organizacyjne, mające zamiar

uruchomić serwer usług w sieci UPNet, zobowiązane są do złożenia wniosku, zawierającego uzasadnienie potrzeby uruchomienia, w Ośrodku Informatyki i opracowania w porozumieniu z Ośrodkiem polityki bezpieczeństwa dla tego serwera. Uprawniony pracownik Ośrodka musi mieć dostęp do konta na serwerze z prawem do odczytu wszystkich plików konfiguracyjnych.

6. Opiekę nad sieciami lokalnymi, w rozumieniu okablowania i stacji sieciowych z oprogramowaniem, sprawują lokalni opiekunowie IT budynków, wydziałów lub katedr, w oparciu o pisemną umowę, pomiędzy opiekunem a UPP, zawierającą zakres obowiązków i odpowiedzialności.
7. Ośrodek Informatyki pełni rolę doradczą dla opiekunów sieci lokalnych i pomaga im w rozwiązywaniu problemów.
8. Ośrodek Informatyki opiekuje się wszystkimi stanowiskami komputerowymi administracji centralnej Uniwersytetu Przyrodniczego w Poznaniu i ma prawo do instalowania na tych stanowiskach oprogramowania wykorzystywanego do monitorowania bezpieczeństwa systemów komputerowych, oprogramowania weryfikującego legalność oprogramowania i oprogramowania wykorzystywanego do pomocy zdalnej.
9. Ośrodek Informatyki opiniuje zakupy sprzętu komputerowego i oprogramowania dla administracji centralnej (stacji roboczych, terminali, drukarek itp.), pod kątem zgodności z założeniami technologiczno-technicznymi, strukturą sieci i założeniami funkcjonalnymi stanowisk.
10. Osoba odpowiedzialna za organizację wydarzenia z użyciem sieci bezprzewodowej jest zobowiązana do kontaktu z odpowiednim wyprzedzeniem (min. 10 dni roboczych przed wydarzeniem) z administratorami sieci poprzez system zgłoszeń.

§ 3
Zasady podłączania komputerów do sieci i odłączania od sieci

1. Włączenie komputera służbowego administracji centralnej do sieci kablowej możliwe jest po zgłoszeniu przez system zgłoszeń do Ośrodka Informatyki, adresu MAC karty sieciowej danego komputera, jego lokalizacji, danych osobowych użytkownika, odpowiedzialnego za wszelkie działania podjęte z komputera.
2. Włączenie komputera służbowego pozostałych jednostek do sieci kablowej możliwe jest po zgłoszeniu przez system zgłoszeń do Ośrodka Informatyki, lokalizacji danego komputera, danych osobowych użytkownika, odpowiedzialnego za wszelkie działania podjęte z komputera.
3. Na podstawie otrzymanych danych Ośrodek Informatyki przydziela dla komputera administracji centralnej adres IP i unikalną nazwę w ramach domeny dc.puls.edu.pl oraz dokonuje konfiguracji urządzeń sieciowych. Ośrodek Informatyki może dokonać konfiguracji karty sieciowej podłączanego do sieci komputera. Dla pozostałych komputerów służbowych adres IP jest przydzielany automatycznie.
4. Każda zmiana lokalizacji komputera służbowego administracji centralnej, użytkownika komputera lub wymiana karty sieciowej wymaga zgłoszenia w Ośrodku Informatyki, pod rygorem wyłączenia dostępu do sieci UPNet.
5. Każdy komputer służbowy pracujący w sieci UPnet musi posiadać oprogramowanie, które określa Ośrodek Informatyki:
   a) do weryfikacji legalności oprogramowania,
   b) pomocy zdalnej
   c) program antywirusowy.

6. Pracownie komputerowe dostępne dla studentów podłączane są do wydzielonych segmentów sieci. Ze względu na bezpieczeństwo sieci nie należy udostępniać studentom komputerów podłączonych do UPNet.
7. Ośrodek Informatyki ma prawo odłączyć komputer od sieci UPNet w przypadkach:
   a) naruszenia przez użytkownika komputera zasad korzystania z sieci określonych w niniejszym regulaminie,
   b) wykrycia działań pochodzących z tego komputera wpływających negatywnie na bezpieczeństwo lub stabilność pracy sieci,
   c) podłączenia komputera administracji centralnej do sieci bez uprzedniego zgłoszenia tego faktu Ośrodkowi Informatyki.

§ 4
Procedura nadawania i odbierania uprawnień do przetwarzania danych osobowych

1. Konto użytkownika na serwerze zakłada administrator serwera na podstawie zgłoszenia przełożonego danego pracownika w systemie zgłoszeń oraz upoważnienia do przetwarzania danych osobowych, nadając unikalną nazwę użytkownika i hasło. Pracownik Ośrodka Informatyki otrzymuje drogą mailową informację od Inspektora Ochrony Danych o otrzymanej zgodzie na przetwarzanie danych osobowych.
2. Przydzielone dane logowania przekazywane są osobiście lub innymi zweryfikowanymi kanałami (MS Teams, imienne służbowe konto pocztowe, telefonicznie).
3. Ustanie stosunku pracy skutkuje usunięciem jego konta, a nazwa użytkownika nie może być przydzielona innej osobie.
4. Administrator serwera jest użytkownikiem uprzywilejowanym, posiadającym najwyższe uprawnienia w Systemie Informatycznym.
5. Konto użytkownika uprzywilejowanego jest używane tylko w uzasadnionych przypadkach.
6. Hasło administratora serwera jest przechowywane w zaszyfrowanych bazach znajdujących się na serwerach UPP
7. Administrator systemów (programów) oprogramowania nadaje uprawnienia użytkownikom do poszczególnych systemów (programów) zgodnie z wnioskowanymi przez przełożonego uprawnieniami.

§ 5
Metody i środki uwierzytelnienia

1. Uwierzytelnienie użytkownika w Systemie Informatycznym następuje po podaniu nazwy użytkownika i hasła.
2. Hasła użytkowników są szyfrowane.
3. Użytkownik nie może udostępniać swojej nazwy użytkownika i hasła innej osobie.
4. Hasło składa się z minimum 10 dowolnych znaków (w tym minimum jedna litera i dwie cyfry):
   a) w przypadku usług HMS/e-HMS/jHMS/WD wielkich liter, małych liter, znaków specjalnych, cyfr, minimum 10 znaków,
   b) w przypadku usług domenowych, pocztowych, helpdesk, dostęp do sieci UPPOZ_sec przynajmniej 10 znaków, wielkich liter, małych liter oraz cyfr,
   c) hasło nie może być takie samo jak nazwa użytkownika oraz nie powinno zawierać zwrotów słownikowych,
   d) hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych (polecamy programy typu menedżer haseł np. Keepass)
   e) w przypadku usług HMS/e-HMS/jHMS/WD użytkownik ma obowiązek zmieniać hasło nie rzadziej niż co 180 dni.

§ 6
Zasady użytkowania komputerów służbowych UPP

1. Komputer powierzony Pracownikowi stanowi własność Uniwersytetu Przyrodniczego w Poznaniu i jako narzędzie pracy powinien być do niej wykorzystywany.
2. Osobami uprawnionymi do korzystania z komputera jest wyłącznie pracownik, doktorant oraz student UPP.
3. UPP może powierzyć komputer do korzystania w swojej siedzibie lub poza nią. Pracodawca udostępnia Pracownikom komputery z zainstalowanym oprogramowaniem oraz zapoznaje Pracownika z obowiązującymi w UPP zasadami korzystania z takiego sprzętu.
4. Korzystanie z komputerów, Internetu i programów użytkowych ma służyć Pracownikom wyłącznie do celów naukowych, edukacyjnych, informacyjnych i administracyjnych, związanych z wykonywaniem zadań i obowiązków służbowych.
5. Pracownik, doktorant oraz student są zobowiązani właściwie eksploatować i dbać o powierzony im komputer oraz utrzymać go w stanie nie gorszym, niż wynika to ze zwykłego zużycia eksploatacyjnego.
6. Pracownik zobowiązany jest zabezpieczyć dostęp do komputera w sposób uniemożliwiający zalogowanie się do systemu osobom nieuprawnionym.
7. Pracownik jest zobligowany do dokonywania kopii zapasowych własnych danych w ramach służbowego konta na MS OneDrive.
8. Pracownik jest zobligowany do zalogowania się na komputerze służbowym w usłudze Office 365 (np. poprzez aplikację MS Teams).
9. Wszystkie dane zapisane w komputerze (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje i dane) związane z wykonywanymi zadaniami służbowymi są własnością UPP.
10. W przypadku używania zewnętrznych nośników danych na komputerze służbowym Pracownik zobowiązany jest wcześniej wykonać skanowanie programem antywirusowym wszystkich danych na nośniku.
11. Komputer służbowy, na którym przetwarzane są dane osobowe musi być skonfigurowany do pracy przez Ośrodek Informatyki i dołączony do domeny Windows.
12. Żaden z pracowników nie powinien pracować na komputerze służbowym na koncie z uprawnieniami administratora.
13. Każdy Pracownik posiada założone konto w systemie zgłoszeń. Jego założenie jest powiązane z wcześniejszym założeniem konta na serwerze pocztowym i na serwerze domeny. Informację o kontach w systemie zgłoszeń są synchronizowane z serwerem domeny raz na dobę lub w szczególnych przypadkach na żądanie administratora usługi. Login i hasło do usługi są tożsame z kontami na serwerze domeny Windows.
14. Jednostki organizacyjne zobligowane są do regularnego planowania zakupu komputerów oraz programów dla swoich pracowników tak, by możliwe było utrzymywanie na nich aktualnych i posiadających wsparcie techniczne systemów operacyjnych.

§ 7
Zasady korzystania z oprogramowania

1. Każda jednostka UPP ma obowiązek posiadania i przechowywania dowodów legalności oprogramowania zainstalowanego na komputerach będących na jej stanie, zgodnie z obowiązującymi uregulowaniami prawnymi dot. ochrony własności intelektualnej wyrażonej w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych oraz przepisami Kodeksu Karnego.

2. Dokumenty potwierdzające legalność oprogramowania muszą być przechowywane w sposób zapewniający zabezpieczenie ich przed nieupoważnionym dostępem, zniszczeniem lub uszkodzeniem.
3. Pracownikom zabrania się instalowania na komputerze służbowym jakiegokolwiek oprogramowania bez wymaganej licencji i niezgodnego z potrzebami służbowymi,
4. Pracownik może korzystać z oprogramowania stanowiącego jego prywatną własność zainstalowanego na służbowym komputerze pod warunkiem, że licencja programu zezwala na takie jego wykorzystanie.
5. Pracownik korzystający ze sprzętu komputerowego jest odpowiedzialny za zainstalowane na nim oprogramowanie.

§ 8
Usługa poczty elektronicznej

1. Każdemu pracownikowi i doktorantowi Uniwersytetu Przyrodniczego w Poznaniu administrator systemu pocztowego zakłada konto mailowe znajdujące się na serwerze uczelnianym w domenie up.poznan.pl o standardowej wielkości 5GB, z możliwością powiększenia. Służbowy adres mailowy ma postać: imie.nazwisko@up.poznan.pl.
2. Prawo do posiadania konta pocztowego wygasa z chwilą rozwiązania umowy o pracę lub innego stosunku służbowego, a w wypadku doktorantów wraz z utratą statusu doktoranta.
3. Każdy student UPP ma prawo do posiadania konta na serwerze studenckim w domenie student.up.poznan.pl i student.puls.edu.pl. Konto ważne wygasa wraz z utratą statusu studenta UPP.

§ 9
Usługa WWW

1. Serwis WWW (zestaw stron) na serwerze uczelnianym może posiadać:
   a) każda jednostka, komórka organizacja lub stowarzyszenie działające w Uniwersytecie Przyrodniczym w Poznaniu,
   b) pracownik naukowy lub dydaktyczny.
2. Za zawartość stron WWW odpowiada osoba sprawująca merytoryczną opiekę nad usługą. W przypadku strony głównej UPP jest to webmaster, zatrudniony w Ośrodku Informatyki, w przypadku stron jednostek/komórek organizacyjnych jest to osoba wyznaczona przez kierownika jednostki/komórki organizacyjnej.
3. Każda jednostka/komórka organizacyjna posiadająca stronę internetową zobowiązana jest do przesłania listy stron WWW i danych osobowych opiekunów tych stron do Ośrodka Informatyki.
4. Nazwiska osób opiekujących się stronami WWW jednostek oraz dane kontaktowe (nr telefonu, adres e-mail) należy umieścić na stronie.
5. Strony WWW nie mogą zawierać:
   a) reklam i innych treści o charakterze komercyjnym, nie związanych w żaden sposób z UPP,
   b) treści naruszających obowiązujące prawo,
   c) odnośników do stron zawierających powyższe treści.
6. Na stronach WWW nie wolno umieszczać cudzych zdjęć, ilustracji, elementów graficznych, map itp., bez uzyskania zezwolenia właściciela praw autorskich.
7. Adresy pocztowe podawane na stronach WWW powinny być zabezpieczone przed odczytaniem przez roboty skanujące.

§ 10

1. Osoba odpowiedzialna za organizację wydarzenia na sali podlegającej Ośrodkowi Informatyki jest zobowiązana do kontaktu z odpowiednim wyprzedzeniem (na minimum 5 dni roboczych przed wydarzeniem) z osobami obsługującymi sprzęt audiowizualny podczas danego wydarzenia.
2. Osoby pracujące w portierni są odpowiedzialne za wydawanie sprzętu do sal wykładowych (mikrofony, prezentery, piloty, akumulatory) zbierając oświadczenia użytkowników w papierowym rejestrze pobrań.
3. Osoby pobierające sprzęt są zobowiązane do poświadczenia własnoręcznym podpisem pobrania w papierowym rejestrze pobrań, tym samym odpowiada za ewentualne braki sprzętowe po okresie użytkowania.
4. Szafki zawierające sprzęt będący na stałym wyposażeniu sal wykładowych mają być zamknięte i niedostępne dla użytkowników. Jeśli wymagana jest bezpośrednia ingerencja przy ich uruchomieniu, to użytkownik jest zobowiązany do kontaktu z osobami odpowiedzialnymi za daną salę.
5. Portiernia posiada na wyposażeniu wymienne akumulatory zasilające sprzęt potrzebny do użytkowania sal (mikrofony, prezentery, piloty).
6. W przypadku awarii sprzętu wykorzystywanego na sali wykładowej, użytkownik ma obowiązek poinformować o tym bezpośrednio Ośrodek Informatyki używając systemu zgłoszeń lub kontaktując się z pracownikiem Ośrodka Informatyki.
7. Sprzęt na wyposażeniu sal jest kompatybilny z urządzeniami podłączonymi przez Ośrodek Informatyki. Pracownicy Ośrodka Informatyki nie biorą odpowiedzialności za brak kompatybilności sprzętu prywatnego z systemem stworzonym w sali wykładowej.
8. Każda jednostka uczelniana, która opiekuje się salą komputerową, jest zobowiązana do przekazania listy sal komputerowych i danych osób opiekujących się tymi salami do Ośrodka Informatyki.

§ 11
Czynności zabronione

1. Zmiana przyznanego adresu IP, adresu serwera DNS lub zmiana adresu MAC karty sieciowej komputera.
2. Odstępowanie uprawnień dotyczących posiadanego konta innym użytkownikom oraz osobom trzecim.
3. Pozostawianie włączonego komputera bez nadzoru w stanie pozwalającym na bezpośrednie korzystanie z usług sieciowych lub bezpośredni dostęp do sieci.
4. Podejmowanie prób wykorzystania obcego konta i uruchamianie oprogramowania deszyfrującego hasła zarówno w obrębie UPNet, jak i w sieciach zewnętrznych, modyfikowanie cudzych plików i stron WWW.
5. Uruchamianie oprogramowania skanującego lub monitorującego sieć/testującego podatności, tak w zakresie UPNet, jak i sieciach zewnętrznych, mającego na celu przechwytywanie informacji lub rozpoznanie infrastruktury oraz poznawanie słabych stron bez względu na cel działania.
6. Podejmowanie prób atakowania elementów sieci lub komputerów poprzez ataki typu DDoS, w szczególności: nieuzasadnione przeciążanie łącz sieciowych, uniemożliwianie dostępu do usług sieciowych bądź zdalne uniemożliwianie lub utrudnianie prawidłowej pracy usług.

7. Uruchamianie przez użytkowników nadmiarowych usług (DNS, DHCP) lub urządzeń, które mogą zakłócać prawidłową pracę sieci lub umożliwiać tworzenie własnych podsieci (wraz z własnymi zasadami dostępu w tym segmencie).
8. Wysyłanie masowej niechcianej i niezamawianej korespondencji (spam).
9. Rozsyłanie wirusów, robaków internetowych, koni trojańskich, bomb czasowych i innych zagrożeń oraz innych niebezpiecznych aplikacji/skryptów/usług.
10. Kopiowanie, rozpowszechnianie lub publikowanie programów komputerowych prawnie chronionych.
11. Używanie aplikacji wymiany plików typu p2p do pobierania treści chronionych prawem autorskim (np. filmów, muzyki, gier, obrazów systemów operacyjnych).
12. Wykorzystywanie zasobów sieci do prowadzenia działalności komercyjnej oraz udostępnianie ich osobom nieupoważnionym:
    a) umieszczanie adresów pocztowych i WWW z domen należących do UPP na wizytówkach innych firm,
    b) wykorzystywanie usług e-mail i WWW do pracy zarobkowej (np. reklama działalności gospodarczej, usługowej, realizacja działań na rzecz firm trzecich),
    c) wykorzystywanie zasobów sprzętowo-programowych (np. licencjonowanego oprogramowania) w działaniach komercyjnych.
13. Wskazywanie na serwery uczelni z użyciem adresów domenowych, bez wcześniejszej pisemnej zgody Kierownika Ośrodka Informatyki.

§ 12
Zalecenia dotyczące bezpieczeństwa

1. Zaleca się blokowanie stacji roboczej przed odejściem od komputera.
2. Należy regularnie instalować poprawki programowe (patch) i pakiety naprawcze (service pack) oraz uaktualnienia oprogramowania (update), w szczególności systemu operacyjnego, przeglądarki internetowej, klienta pocztowego i pakietów biurowych. Programy te najbezpieczniej pobierać ze strony producenta danego oprogramowania lub ze stron wskazanych przez Ośrodek Informatyki.
3. W systemach MS Windows należy używać wbudowanej internetowej zapory przeciwogniowej (firewall) lub innego licencjonowanego oprogramowania tego typu.
4. Należy unikać przesyłania danych w formatach nieodpornych na zarażenie wirusami, takich jak np. exe, com, bat, ps1, sh.
5. Nie należy instalować nierekomendowanych lub nieznanych programów, otrzymanych pocztą elektroniczną lub pobranych z witryn WWW.
6. Należy zachować szczególną ostrożność przy otwieraniu poczty elektronicznej spoza naszej organizacji w zakresie załączników w takich mailach.

§ 13
Postanowienia końcowe

1. W wypadku, gdy wskutek działań niezgodnych z regulaminem użytkownik naruszy obowiązujące prawo, ponosi on pełną odpowiedzialność służbową, cywilną i karną.
2. W wypadku powstania strat z powodu złamania zasad określonych w niniejszym regulaminie, użytkownik zostanie obciążony związanymi z tym faktem kosztami.