

Załącznik Nr 4 do Zarządzenia Nr 150/18

Prezydenta Miasta Szczecin

z dnia 6 kwietnia 2018 r.

Regulamin korzystania z zasobów informatycznych Urzędu Miasta Szczecin

§ 1. 1. Na komputerowym stanowisku pracy dozwolona jest eksploatacja oprogramowania przydzielonego dla danej stacji roboczej, które zostało zakupione przez Urząd Miasta Szczecin i zaewidencjonowane w rejestrze oprogramowania, prowadzonym przez WInf w formie licencji, usługi, dzierżawy, subskrypcji itp.

2. Nośniki instalacyjne oprogramowania, dokumenty poświadczające posiadanie licencji oraz inne dowody poświadczające prawo korzystania z oprogramowania przechowuje WInf w miejscu niedostępnym dla osób nieupoważnionych.

3. Oprogramowanie musi być użytkowane wyłącznie na podstawie przydzielonych jednostek organizacyjnej licencji, usługi, dzierżawy, subskrypcji itp., zarówno w zakresie ilości jak i wersji. Licencje przydziela WInf.

4. Zabrania się instalacji i eksploatacji oprogramowania innego, niż wymienione w ust. 1. W szczególności zabrania się pobierania i instalacji oprogramowania z Internetu, płyt CD, innych nośników danych stanowiących załącznik do literatury i czasopism informatycznych lub pochodzących z innych źródeł.

5. Instalacja oprogramowania we własnym zakresie (przez pracownika nie będącego pracownikiem WInf) wymaga pisemnej zgody dyrektora WInf lub osoby upoważnionej. Powyższe dotyczy również składników systemu operacyjnego (np. wygaszaczy ekranu itp.).

6. Każda zmiana dotycząca oprogramowania zainstalowanego na stacji roboczej wymaga zgłoszenia wniosku w formie pisemnej do WInf, zaakceptowanego przez kierownika osoby zgłaszającej wniosek. Forma pisemna nie musi być zachowana w przypadku problemu z oprogramowaniem - wówczas należy niezwłocznie zgłosić ten fakt pod numer wskazany jako numer interwencyjny WInf.

7. W Urzędzie decyzje o obowiązującym standardzie oprogramowania dla stacji roboczych podejmuje WInf.

8. Zabrania się pracy z komputerem bez zainstalowanego i aktywnego oprogramowania antywirusowego.

§ 2. 1. Zabrania się rozbudowy i wprowadzania zmian w użytkowanym sprzęcie komputerowym oraz ingerencji w okablowanie strukturalne.

2. Zabrania się wykorzystywania sprzętu i wyposażenia innego niż dostarczony przez WInf.

3. Zabrania się wykorzystywania gniazd energetycznych infrastruktury informatycznej do celów innych, niż zasilanie stacji roboczych i urządzeń peryferyjnych. W szczególności zabrania się podłączania urządzeń o wysokim poborze mocy – czajniki, wentylatory, grzejniki itp.

4. Zlecenie konfiguracji komputera, wszelkie zmiany w stacjach roboczych, urządzeniach peryferyjnych i okablowaniu strukturalnych wykonują uprawnieni pracownicy WInf zgodnie z pisemnym wnioskiem, zaakceptowanym przez kierownika. Forma pisemna nie musi być zachowana w przypadku nagłego uszkodzenia ww. urządzeń – wówczas należy niezwłocznie zgłosić ten fakt pod numer wskazany jako numer interwencyjny WInf.

§ 3. 1. Każdy użytkownik ma prawo i obowiązek pracy przy wykorzystaniu wyłącznie własnego, indywidualnego konta w systemach informatycznych. Obowiązuje zakaz pracy z wykorzystaniem cudzego konta. W przypadku zauważenia takiego faktu należy niezwłocznie poinformować o tym WInf lub ABI.

2. Użytkowników obowiązuje bezwzględny zakaz ujawniania jakichkolwiek haseł własnych lub cudzych komukolwiek i kiedykolwiek.

3. Zakładanie i usuwanie kont użytkowników oraz modyfikacja uprawnień uregulowane jest zgodnie z Załącznikiem nr 24 do Zarządzenia.

§ 4. 1. Stacje robocze, znajdujące się w miejscach dostępnych dla osób nieuprawnionych (w szczególności dla interesantów), muszą być chronione wygaszaczem ekranu zabezpieczonym hasłem, z czasem uaktywnienia wygaszacza nie dłuższym niż 5 minut. Ustawienie monitora powinno zapobiegać możliwości podglądania danych wyświetlanych na ekranie przez osoby nieuprawnione.

2. Zabrania się:

- 1) korzystania ze sprzętu niezgodnie z jego przeznaczeniem.
- 2) instalowania i używania programów deszyfrujących hasła, skanujących infrastrukturę, łamiących zabezpieczenia oprogramowania.
- 3) wykonywania innych działań mogących mieć wpływ na konfigurację komputerów / sieci oraz bezpieczeństwo organizacji.

3. Pracownicy WInf mają prawo i obowiązek do :

- 1) weryfikacji stanu eksploatowanego sprzętu i oprogramowania,
- 2) usuwania nieautoryzowanego oprogramowania bez konieczności uzyskania akceptacji użytkowników i ich kierowników,
- 3) blokowania konta w przypadku wykrycia naruszenia zasad bezpieczeństwa sieci lub wygaśnięcia konta użytkownika,
- 4) stałego monitoringu bezpieczeństwa sieci w tym ruchu internetowego.

§ 5. 1. Dostęp do Internetu dozwolony jest tylko z wykorzystaniem metod i łącz autoryzowanych przez WInf.

2. Zabrania się stosowania innych metod, w szczególności samodzielnego instalowania modemów i kreowania kanałów dostępu przez telefony komórkowe i inne urządzenia. Powyższe nie dotyczy sprzętu służbowego wykorzystywanego poza lokalizacjami Urzędu.

3. Bezwzględnie zabrania się przeglądania stron www o charakterze erotycznym, pornograficznym, o zasobach dyskryminujących lub mogących urazić inne osoby itp. oraz stron do pobierania oprogramowania.

§ 6. Korzystanie z zasobów.

1. Zabrania się umieszczania na dyskach lokalnych stacji roboczych i dyskach sieciowych jakichkolwiek prywatnych lub publicznych (np. dostępnych w internecie) plików multimedialnych (zdjęć, filmów, muzyki itp.).

2. W przypadku przechowywania plików multimedialnych przeznaczonych do zadań związanych z zakresem obowiązków pracownika (w tym prezentacji), zaleca się archiwizację tych plików po ich wykorzystaniu. Pliki multimedialne starsze niż 6 miesięcy mogą być usuwane z dysków sieciowych bez powiadomienia użytkownika.

§ 7. WInf na bieżąco będzie przysyłał informacje pozwalające użytkownikom doskonalić swoją wiedzę, wyjaśnienia i bieżące zalecenia dotyczące bezpieczeństwa sieci. Użytkownicy zobowiązani są te informacje przyswajać i bezwzględnie się do nich stosować. W razie pytań lub wątpliwości mają się zwrócić do pracowników WInf.

§ 8. Postanowienia końcowe:

1. Obowiązkiem każdego użytkownika zasobów informatycznych Urzędu jest ochrona tychże zasobów w sposób odpowiadający jego uprawnieniom, obowiązkom i możliwościom.

2. Urząd Miasta Szczecin ma prawo do bieżącej, zdalnej lub bezpośredniej kontroli zasobów oraz ingerencji w zasoby bez powiadomienia.

3. W przypadku stwierdzenia instalacji nieautoryzowanego oprogramowania, modyfikacji sprzętu lub oprogramowania lub innych naruszeń postanowień niniejszego regulaminu sporządza się notatkę służbową.

4. Notatka zawiera oznaczenie stacji roboczej, dane identyfikujące pracownika, na którego stanie znajduje się stacja robocza, datę stwierdzenia opisywanych faktów, wykaz nieautoryzowanego oprogramowania i inne informacje identyfikujące zdarzenie. Notatkę przedkłada się Dyrektorowi Winf.

5. Zawartość zasobów informatycznych (w tym poczty elektronicznej) jest własnością Urzędu. Jakiegokolwiek ich wykorzystywanie niezgodnie z zadaniami wynikającymi z obowiązków służbowych jest zabronione, w szczególności zabrania się udostępniania danych z zasobów Urzędu osobom nieupoważnionym bez pisemnej zgody przełożonych.

6. Udokumentowane naruszenie postanowień niniejszego regulaminu może stanowić podstawę do wyciągnięcia konsekwencji służbowych.