

Regulamin określający zasady i procedury korzystania z legalnego oprogramowania, sprzętu komputerowego i sieci teleinformatycznej oraz poczty elektronicznej w Urzędzie

I. Zasady korzystania z oprogramowania.

1. Zobowiązuję pracowników do korzystania tylko z legalnego oprogramowania wymienionego w ewidencji, za prowadzenie której odpowiedzialny jest Naczelnik Wydziału Organizacyjnego.
2. Instalacje oprogramowania na stanowiskach komputerowych mogą być dokonywane z nośników znajdujących się w zasobach Urzędu. Ich instalacja może być dokonywana wyłącznie przez ASI.
3. Pracownik może dokonać tylko autoryzowanej instalacji. Autoryzowanie instalacji następuje po wydaniu zgody przez ASI, zinwentaryzowaniu oprogramowania i dopisaniu go do ewidencji oprogramowania.
4. Oprogramowanie w wersjach testowych lub w jakikolwiek inny sposób ograniczone umowami licencyjnymi może być użytkowane wyłącznie zgodnie z jego przeznaczeniem i w czasie określonym w umowie licencyjnej.
5. Zabrania się pobierania i kopiowania z Internetu wszelkich utworów (programów komputerowych, utworów muzycznych, filmów, gier komputerowych, itp.), będących przedmiotem ochrony praw autorskich.
6. Naruszenia wyżej wymienionych ustaleń, ze względu na obowiązujące przepisy prawne, stanowią poważne naruszenie dyscypliny pracy.

II. Zarządzanie oprogramowaniem.

1. W Urzędzie obowiązuje centralizacja zakupów oprogramowania komputerowego – procedury Systemu Zarządzania Jakością.
2. W Urzędzie obowiązuje wyłącznie pisemna forma wszelkich poleceń dotyczących zakupu oprogramowania.
3. Decyzję o zakupie nowego oprogramowania w Urzędzie podejmuje wyłącznie Prezydent Miasta na wniosek Sekretarza.
4. Pracownicy nie mogą samodzielnie dokonywać zakupu oprogramowania.
5. Za prowadzenie dokumentacji licencyjnej zakupionego oprogramowania odpowiedzialny jest ASI.
6. Nośniki instalacyjne oprogramowania znajdują się w zamkniętej szafie lub na serwerze zasobów, do których dostęp mają ASI. Nośniki oprogramowania nie mogą być przechowywane w żadnym innym miejscu, a szczególnie nie mogą być kopiowane, wypożyczane lub w żaden inny sposób przekazywane osobom trzecim. Dotyczy to również kodów aktywacyjnych produktów.
7. Przypadki instalowania i uruchamiania oprogramowania niedopuszczonego do użycia przez Urząd (w tym np. oprogramowania skopiowanego własnoręcznie z Internetu), w szczególności, gdy jego uruchomienie wywołuje działania niedozwolone, po ich potwierdzeniu, będą podlegały szczegółowej analizie i mogą być traktowane jako celowe i świadome działanie zmierzające do zwiększenia ryzyka działania zasobów i sieci teleinformatycznej Urzędu.

III. Zasady korzystania ze sprzętu komputerowego.

1. Sprzęt komputerowy powierza się pracownikom wyłącznie w celu wykonywania obowiązków służbowych.
2. W Urzędzie Pracownikowi zabrania się korzystania ze sprzętu komputerowego, do którego Pracodawca nie jest uprawniony.
3. Powierzenie sprzętu następuje na podstawie protokołu przekazania sprzętu komputerowego.
4. Zabrania się dokonywania bez autoryzacji ASI zmian w ustawieniach systemowych komputerów, w szczególności: ustawień BIOS-u, ustawień systemu operacyjnego (w tym instalowania urządzeń), ustawień sieci teleinformatycznej.
5. Zabrania się samodzielnego otwierania obudowy komputera oraz innych części komputerowych (np. monitorów, drukarek, myszy).
6. Uprawnionymi do dokonywania czynności, o których mowa w ust. 4 i 5 na warunkach określonych warunkami gwarancji sprzętu, jest ASI.

7. Pracownik, w którego dyspozycji pozostaje sprzęt komputerowy ma obowiązek wyłączyć go po zakończeniu pracy.
8. Korzystanie z nośników danych dopuszczalne jest po wcześniejszym sprawdzeniu ich programem antywirusowym.
9. Pracownik ma obowiązek bez wiedzy i zgody ASI:
 - 1) wymienić toner, tusz, taśmę i inne materiały eksploatacyjne,
 - 2) usunąć zakleszczony papier.
10. Zezwala się Pracownikom na korzystanie z przenośnego komputera służbowego poza miejscem pracy, na zasadach wymienionych w odrębnych przepisach wewnętrznych.

IV. Zasady korzystania z sieci komputerowej (teleinformatycznej) i poczty elektronicznej.

1. Do sieci teleinformatycznej może być podłączony tylko sprzęt będący własnością Pracodawcy, z zastrzeżeniem ust. 2.
2. Inny sprzęt komputerowy podłączany jest wyłącznie za zgodą ASI.
3. Zabrania się samowolnego podłączania do sieci komputerów lub innych urządzeń.
4. O rozdziale adresów IP decyduje ASI.
5. Zabrania się wykorzystywania gniazd elektrycznych sieci teleinformatycznej w celu zasilania innych urządzeń niż komputery i peryferia komputerowe.
6. W celu zapewnienia bezpieczeństwa mechanizmom sieci teleinformatycznej Urzędu oraz dla jej użytkowników Pracownikowi zabrania się dokonywania na niej działań o charakterze nielegalnym, a w szczególności:
 - 1) umieszczania lub uruchamiania programów i innych obiektów niebezpiecznych, w tym „koni trojańskich” czy innych programów realizujących niepożądane lub wrogie działania,
 - 2) skanowania sieci teleinformatycznej Urzędu,
 - 3) prowadzenia ataków, włamań, itp., innych czynności związanych z ingerencją w działanie lub zasoby sieci teleinformatycznej Urzędu, lub Internetu,
 - 4) naruszania w jakikolwiek sposób bezpieczeństwa serwerów i ich bezawaryjnej pracy, a zwłaszcza logowania się do serwerów, jeżeli zakres obowiązków tego nie wymaga,
 - 5) anonimowego wysyłania poczty elektronicznej z sieci teleinformatycznej Urzędu,
 - 6) gromadzenia na stanowisku pracy, tj. stacji roboczej lub na zasobie dyskowym udostępnionym w sieci LAN, w dowolnej, cyfrowej formie materiałów lub treści niezgodnych z obowiązującym prawem lub naruszających dobre obyczaje,
 - 7) uruchamiania programów z komputerowych nośników zewnętrznych, tj. z płyt CD/DVD lub nośników typu pendrive, itp.,
 - 8) rozpowszechnia nielegalnych plików do Internetu, tj. przesyłania zdjęć, filmów, tekstów czy innych formatów plików.
7. Pracownikowi zakazuje się umożliwiania osobom postronnym dostępu do sieci teleinformatycznej Urzędu, np. umożliwienia pracy na identyfikatorach i hasłach Pracownika.
8. Zabrania się Pracownikom Urzędu wykonywania następujących czynności przy użyciu sprzętu i oprogramowania należącego do Pracodawcy :
 - 1) używania poczty elektronicznej Urzędu do celów innych niż służbowe,
 - 2) wysyłania wiadomości pocztowych (e-mail), typu reklamy, „łańcuszki szczęścia”, pornograficznych, itp.,
 - 3) logowania się w celach prywatnych lub komercyjnych na stronach WWW czy uczestniczenia w portalach o charakterze społecznościowym, zwłaszcza towarzyskim, komercyjnych, itp.,
 - 4) używania w celach prywatnych lub komercyjnych komunikatorów internetowych w rodzaju Skype, Gadu-Gadu, Tlen, itp.,
 - 5) korzystania z serwisów internetowych niezwiązanych z obowiązkami Pracownika, np. oferujących gry internetowe i losowe, hazard, prywatne aukcje, rozrywkę, prywatne listy dyskusyjne., itp.,
 - 6) przetwarzania na komputerach, materiałów do których Pracodawca nie posiada praw autorskich,
 - 7) korzystania z serwisów internetowych zawierających treści niecenzuralne lub jakiekolwiek łamiące prawo obowiązujące na terenie Rzeczypospolitej Polskiej,

V. Procedury kontrolne dotyczące komputerowego stanowiska pracy w Urzędzie.

1. Na wniosek Sekretarza ruch w sieci teleinformatycznej Urzędu, generowany przez Pracownika, może podlegać monitoringowi z automatycznym zapisem dostępu do stron WWW.
2. Informacje statystyczne potwierdzające: adresy sieciowe, czas dostępu do najczęściej odwiedzanych przez Pracowników serwisów internetowych, gromadzonych plików oraz uruchamianych aplikacji mogą:
 - 1) podlegać analizie i przekazaniu do kierowników komórek organizacyjnych,
 - 2) stanowić podstawę do dalszych kroków podejmowanych na drodze służbowej.
3. Zasady gromadzenia danych, o których mowa w ust. 2, określono w odrębnych przepisach wewnętrznych.