PREZYDENT MIASTA OTWOCKA

ZARZĄDZENIE NR 120/2020 PREZYDENTA MIASTA OTWOCKA

z dnia 30 kwietnia 2020 r.

w sprawie wprowadzenia Regulaminu korzystania z komputerowych stanowisk pracy w Urzędzie Miasta Otwocka

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz. U. z 2020 r., poz. 713), zarządza się, co następuje:

§ 1. Wprowadza się Regulamin korzystania z komputerowych stanowisk pracy w Urzędzie Miasta Otwocka, zwany dalej Regulaminem, stanowiący załącznik do niniejszego Zarządzenia.

§ 2. 1. Pracownikom Urzędu Miasta Otwocka umożliwia się zapoznanie z tekstem Regulaminu.

2. Po zapoznaniu się z jego treścią, pracownik jest zobowiązany do podpisania Oświadczenia o zapoznaniu się z jego treścią, którego wzór stanowi załącznik do Regulaminu.

§ 3. Wykonanie zarządzenia powierza się Sekretarzowi Miasta Otwocka oraz Naczelnikowi Wydziału Informatyki i Naczelnikowi Wydziału Organizacyjnego i Spraw Pracowniczych.

§ 4. Zarządzenie wchodzi w życie po upływie dwóch tygodni od dnia ogłoszenia.

PREZYDENT
MIASTA OTWOCKA
Jarosław Tomasz Margielski

Załącznik Nr 1 do zarządzenia Nr 120/2020

Prezydenta Miasta Otwocka

z dnia 30 kwietnia 2020 r.

Regulamin korzystania z komputerowych stanowisk pracy w Urzędzie Miasta Otwocka

§ 1. Celem wdrożenia Regulaminu jest:

1) poprawa jakości i zgodności z procedurami obowiązującymi w Urzędzie wykonywania pracy przez pracowników;

2) zabezpieczenie uzasadnionych interesów Pracodawcy;

3) ochrona bezpieczeństwa Urzędu;

4) zabezpieczenie danych oraz mienia Pracodawcy;

§ 2. Ilekroć w Regulaminie jest mowa o:

1) Urzędzie, należy przez to rozumieć Urząd Miasta Otwocka,

2) Pracodawcy, należy przez to rozumieć Urząd;

3) komórce organizacyjnej, należy przez to rozumieć wydział, biuro, Urząd Stanu Cywilnego oraz samodzielne stanowisko pracy,

4) kierowniku komórki organizacyjnej - należy przez to rozumieć naczelnika wydziału, kierownika biura oraz koordynatora wieloosobowego stanowiska pracy,

5) użytkowniku, należy przez to rozumieć podmiot posiadający unikatową nazwę służącą do jego identyfikacji w celu umożliwienia dostępu do systemu informatycznego Urzędu oraz korzystania z jego zasobów;

6) Wydziale, należy przez to rozumieć Wydział Informatyki Urzędu;

7) informatyku, należy przez to rozumieć pracownika Wydziału.

Zarządzanie uprawnieniami - procedura rozpoczęcia, zawieszenia i zakończenia pracy

§ 3. 1. Każdy użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.

2. Tworzenie kont użytkowników wraz z uprawnieniami (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) odbywa się na polecenie przełożonych a wykonywane przez informatyków-administratorów.

3. Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na swoim komputerze).

4. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.

5. Zabrania się pracy wielu użytkowników na wspólnym koncie.

6. Użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę z użyciem identyfikatora i hasła.

7. Użytkownik jest zobowiązany do powiadomienia informatyków-administratorów o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.

8. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym informatyków-administratorów.

9. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. Polityka czystego ekranu.

10. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.

11. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako pracownik działu informatyki. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.

12. Po zakończeniu pracy, użytkownik zobowiązany jest:

a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy.

b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki elektroniczne, magnetyczne i optyczne, na których znajdują się dane osobowe.

Zasady korzystania z oprogramowania

§ 4. 1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi.

2. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na Sprzęcie IT przez Pracodawcę na swoje własne potrzeby ani na potrzeby osób trzecich.

3. Instalowanie jakiegokolwiek oprogramowania na Sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną.

4. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Pracodawcę. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.

5. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną.

6. Pracodawca zastrzega sobie prawo kontrolowania zawartości dysku twardego i wglądu w treść zapisanych informacji służbowych. Jeśli pracownik zabezpieczył je hasłem, to na żądanie pracodawcy musi je udostępnić. Prywatne materiały pracownik może zapisywać na komputerze tylko za zgodą przełożonego.

7. W przypadku naruszenia któregokolwiek z powyższych postanowień Pracodawca ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

Polityka haseł

§ 5. 1. Hasła powinny składać się z minimum 8 znaków.

2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).

3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.

4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.

5. W przypadku ujawnienia hasła – należy natychmiast go zmienić.

6. Hasła muszą być zmieniane co 30 dni.

7. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.

8. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym organizacji.

9. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.

10. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

Zasady wynoszenia nośników z danymi poza Urząd

§ 6. 1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora Danych Osobowych. Do takich nośników zalicza się: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.

2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki).

3. Zabrania się wynoszenia poza obszar Urzędu Miasta wymiennych nośników informacji a w szczególności twardych dysków z zapisanymi danymi osobowymi i pendrive bez zgody Administratora Danych Osobowych.

4. W sytuacji przekazywania nośników z danymi osobowymi poza Urząd Miasta Otwocka można stosować następujące zasady bezpieczeństwa:

a) adresat powinien zostać powiadomiony o przesyłce,

b) dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą,

c) stosować bezpieczne koperty depozytowe,

d) przesyłkę należy przesyłać przez kuriera.

Zasady korzystania z internetu

§ 7. 1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.

2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach

3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.

4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).

5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

8. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo). Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci.

Zasady korzystania z poczty elektronicznej

§ 8. 1. Przesyłanie danych osobowych z użyciem maila poza Urząd Miasta Otwocka może odbywać się tylko przez osoby do tego upoważnione.

2. W przypadku przesyłania danych osobowych poza Urząd Miasta należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy telefonicznie lub SMS.

3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 12 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.

4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

6. **WAŻNE:** Nie otwierać podejrzanych załączników otrzymanych w mailach, w szczególności spoza Urzędu!!!!! Są to często „wirusy", które infekują komputer oraz pozostałe komputery w sieci. WYSOKIE RYZYKO UTRATY BEZPOWROTNEJ UTRATY DANYCH.

7. **WAŻNE:** Nie wolno „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami". Użytkownik „klikając" na taki hiperlink infekuje komputer oraz inne komputery w sieci. WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH.

8. Należy zgłaszać informatykowi przypadki podejrzanych e-maili .

9. Podczas wysyłania maili do wielu adresatów jednocześnie, w szczególności na zewnątrz Urzędu, należy użyć metody **„Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"**!.

10. Użytkownicy powinni okresowo kasować niepotrzebne maile.

11. Konta pocztowe służbowe są odseparowane od poczty prywatnej.

12. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.

13. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.

14. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.

15. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.

16. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze niezgodnym z obowiązkami pracownika samorządowego, obraźliwym, niemoralnym lub sprzecznym z zasadami współżycia społecznego.

17. Użytkownik bez zgody Administratora Danych Osobowych nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące pracowników Pracodawcy, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

Ochrona antywirusowa

§ 9. 1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.

2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.

3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka.

§ 10. 1. Zabronione jest wykorzystywanie przez użytkownika komputera służbowego do celów prywatnych.

2. Zabronione jest instalowanie i wykorzystywanie jakiegokolwiek oprogramowania bez wiedzy i udziału osób odpowiedzialnych za tego rodzaju czynności w Urzędzie. Wszelkie działania użytkownika w tym zakresie będą monitorowane.

3. Zabronione jest zapisywanie, przechowywanie na dyskach lokalnych lub zasobach sieciowych wszelkich plików multimedialnych niezwiązanych z wykonywaniem czynności służbowych.

4. Zabronione jest używanie sprzętu komputerowego poza siedzibami Urzędu bez wcześniejszego powiadomienia Naczelnika Wydziału.

5. Zabronione jest wykorzystywanie połączenia z siecią internet do celów innych niż służbowe.

6. Zabroniona jest samodzielna zmiana konfiguracji sprzętowej zestawu i jego ustawień systemowych bez zgody Naczelnika Wydziału.

7. Zabronione jest udostępnianie innym użytkownikom haseł dostępowych i ich przechowywanie w łatwo dostępnych lub widocznych miejscach.

8. Zabronione jest używanie nośników danych nieznanego pochodzenia oraz nośników wymiany pamięci wcześniej nie zgłoszonych do Wydziału.

9. Zabrania się samodzielnego wykonywania napraw.

10. O każdej usterce sprzętu należy powiadomić Wydział.

11. Za dane i wykonywanie kopii danych przechowywanych na dyskach lokalnych odpowiada użytkownik zestawu komputerowego.

§ 11. Wszelkie czynności użytkownika w zakresie działań Pracodawcy zmierzających do poprawy jakości pracy z komputerem polegające, w szczególności na eliminowaniu możliwości pobierania określonych danych z Internetu, odciążeniu sieci informatycznej, poprzez ograniczenie możliwości transferu danych z lub do komputera pracownika, usuwaniu nielegalnego oprogramowania, blokowania dostępu do nielegalnych treści oraz kontroli antywirusowej związane są bezpośrednio z bezpieczeństwem Urzędu i ochroną danych osobowych, będą monitorowane.

§ 12. Monitorowanie pracy użytkowników przy wykorzystaniu komputerów służbowych będzie przeprowadzone na bazie dedykowanego oprogramowania, będącego własnością pracodawcy, który posiada do niego stosowaną licencję.

§ 13. Zakresem monitoringu w Urzędzie objęte są:

1) kontrola zdarzeń na komputerze użytkownika;

2) przesyłanie alertów na komputer pracownika przez administratora sieci informatycznej;

3) monitoring używanych przez pracownika aplikacji;

4) możliwość blokowania zbędnych aplikacji, lub stron internetowych;

5) monitoring wykonywanych przez pracowników wydruków;

6) monitoring odwiedzanych przez pracowników stron internetowych;

7) monitoring ruchu w sieci informatycznej (LAN, WAN) Urzędu;

8) monitoring legalności oprogramowania;

9) monitoring służbowych kont poczty email. Pracodawca zastrzega sobie prawo do kontroli treści wysłanych i otrzymanych e-maili z konta służbowego;

10) monitoring używania przenośnych nośników danych (pendrive, karty pamięci, CD-ROM, HDD, telefony, itp.) z możliwością blokowana, jak i odczytania ich treści;

11) monitoring posiadanego sprzętu w Urzędzie.

§ 14. Pracownicy wydziału informatyki mają prawo przejąć kontrolę nad stacją roboczą pracownika Urzędu Miasta Otwocka tzw. „zdalny pulpit" w celach prac serwisowych, konfiguracyjnych oraz naprawczych.

§ 15. 1. Każdemu użytkownikowi umożliwia się zapoznanie z tekstem Regulaminu.

2. Po zapoznaniu się z jego treścią, użytkownik jest zobowiązany do podpisania Oświadczenia o zapoznaniu się z jego treścią, którego wzór stanowi załącznik do Regulaminu.

PREZYDENT
MIASTA OTWOCKA
Jarosław Tomasz Margielski

Załącznik Nr 2 do zarządzenia Nr 120/2020

Prezydenta Miasta Otwocka

z dnia 30 kwietnia 2020 r.

OŚWIADCZENIE

Ja ..... niżej podpisana(y) informuję, że zapoznałem się z treścią „Regulaminu korzystania z komputerowych stanowisk pracy w Urzędzie Miasta Otwocka" zobowiązuje się do przestrzegania zapisów zamieszczonych w Regulaminie. Jednocześnie przyjmuję do wiadomości, iż Wydział Informatyki monitoruje wszelkie czynności wykonywane na komputerze, ruch internetowy, wydruki oraz ma możliwość zdalnej pracy na komputerze użytkownika.

PREZYDENT
MIASTA OTWOCKA

Jarosław Tomasz Margielski