

| | | | |
|--|---|--------------|------------|
|  | Instrukcja Bezpieczeństwa Danych Osobowych – Urząd Miasta w Radymnie | Strona | 1 z 9 |
| | | Wydanie | 1 |
| | | Data wydania | 11.07.2023 |

Załącznik Nr 1 do Zarządzenia Nr 53/2023 Burmistrza Miasta Radymno z dnia 11.07.2023 r. w sprawie wprowadzenia Instrukcji Bezpieczeństwa Danych Osobowych w Urzędzie Miasta Radymno.

INSTRUKCJA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

URZĄD MIASTA RADYMNA

RADYMNO, 2023 ROK



Instrukcja Bezpieczeństwa Danych Osobowych – Urząd Miasta w Radymnie

Strona 2 z 9

Wydanie 1

Data wydania 11.07.2023

1. WSTĘP

Niniejszy dokument ma za zadanie stanowić zbiór zasad postępowania w zakresie ochrony danych osobowych w Urzędzie Miasta w Radymnie (dalej jako „Jednostka”). Niniejszy dokument ma również na celu budowanie świadomości i prawidłowych nawyków w zakresie ochrony danych, ze szczególnym uwzględnieniem systemów informatycznych i pracy na urządzeniach elektronicznych.

Pracownicy¹ w ramach bieżącej pracy powinni przestrzegać następujących zasad:

2. RUCH OSOBOWY

- 2.1. W pomieszczeniach gdzie zlokalizowany jest sprzęt komputerowy mogą przebywać wyłącznie osoby upoważnione.
 - 2.1.1. Klienci Jednostki mogą przebywać w pomieszczeniach, gdzie zlokalizowany jest sprzęt komputerowy wyłącznie pod nadzorem pracowników Jednostki.
 - 2.1.2. Pozostałe osoby (inne niż pracownicy, współpracownicy i Klienci Jednostki) mogą przebywać w pomieszczeniach gdzie zlokalizowany jest sprzęt komputerowy oraz dane osobowe wyłącznie w pod nadzorem pracownika Jednostki lub na podstawie zgody udzielonej przez władną do tego osobę w Jednostce.
- 2.2. Dostęp do pomieszczeń może być możliwy wyłącznie w czasie pracy.
- 2.3. Osoby wykonujące czynności konserwacyjne, naprawcze lub serwisowe, które nie posiadają upoważnienia mogą przebywać w obszarach bezpiecznych pod nadzorem osób pracowników Jednostki.
- 2.4. Dokumenty tradycyjne w momencie przerwy lub zakończenia pracy powinny zostać zabezpieczone zgodnie z polityką czystego biurka (tj. zamknięte w meblach na klucz).

3. ROZPOCZĘCIE I ZAKOŃCZENIE PRACY W POMIESZCZENIACH, W KTÓRYCH PRZETWARZA SIĘ INFORMACJE

- 3.1. Przed przystąpieniem do pracy w systemie informatycznym należy sprawdzić stację roboczą (komputer) i stanowisko pracy zwracając uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia bezpieczeństwa informacji powodowanych czynnikami zewnętrznymi (np. Naruszenie zamków, krat, wybicie okna).
- 3.2. Pracownik zobowiązany jest do utrzymywania stałego porządku na swoim stanowisku pracy (dalej „biurko”), przechowywania na biurku tylko tych dokumentów, które są mu potrzebne do wykonywania pracy w danym momencie oraz niepozostawiania bez nadzoru pomieszczenia, w którym są przetwarzane dane osobowe.
- 3.3. Przed wyjściem z pomieszczenia należy upewnić się, że okna oraz miejsca, w których przechowuje się informacje podlegające ochronie zostały zamknięte.
- 3.4. Po zamknięciu pomieszczenia należy odpowiednio zabezpieczyć klucze przed nieuprawnionym użyciem, zgodnie z przyjętymi zasadami deponowania kluczy.

¹ **Pracownik** – każda osoba zatrudniona przez Administratora w jakiegokolwiek formie prawnej i upoważniona przez niego do przetwarzania danych osobowych, w szczególności pracownicy samorządowi w rozumieniu przepisów Ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych, pracownicy w rozumieniu Ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy, a także zleceniobiorcy, przyjmujący, stażyści, praktykanci i wolontariusze.



**Instrukcja Bezpieczeństwa Danych
Osobowych – Urząd Miasta w
Radymnie**

Strona 3 z 9

Wydanie 1

Data wydania 11.07.2023

4. ZASADY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

- 4.1. Przed uruchomieniem stacji roboczej tam gdzie jest to możliwe, należy upewnić się, że okablowanie jest odpowiednio podłączone i nie zostały uszkodzone gniazda prądowe.
- 4.2. Aby zawiesić pracę (tymczasowa przerwa w pracy w systemie informatycznym) należy zablokować stację kombinacją klawiszy „Microsoft + L”. Dokumenty tradycyjne powinny zostać zabezpieczone zgodnie z polityką czystego biurka.
- 4.3. Kończąc pracę należy wylogować się z systemu informatycznego, zamknąć wszystkie aplikacje i upewnić się, że system operacyjny stacji roboczej zamknął się prawidłowo.

5. BEZPIECZEŃSTWO WYDRUKÓW, NOTATEK I INNYCH DOKUMENTÓW NIESTANOWIĄCYCH AKT

- 5.1. Podczas drukowania należy zachować szczególną ostrożność wybierając drukarkę, na którą mają zostać wydrukowane dokumenty, aby wydruk przez pomyłkę nie dostał się do osób nieupoważnionych.
- 5.2. Wydruki należy niezwłocznie odebrać, aby wydrukowane dokumenty nie pozostały na podajnikach.
- 5.3. W przypadku, gdy wydruki blokują się w kolejkach wydruku, należy o zdarzeniu poinformować osobę odpowiedzialną za działanie drukarek. Nie należy uruchamiać kolejnych wydruków, jeżeli poprzedni wydruk się nie powiódł.
- 5.4. Dokumenty zbędne w bieżącej działalności muszą być niszczone w urządzeniu do tego przeznaczonym – dokumenty takie nie mogą zostać wyrzucone bezpośrednio do kosza na śmieci.

6. ROZMOWY TELEFONICZNE I FAKS

- 6.1. Pracownicy zobowiązani są do przestrzegania zakazu prowadzenia rozmów telefonicznych, podczas których może dochodzić do wymiany informacji chronionych, jeśli rozmowy te odbywają się w miejscach publicznych (np. Pociągach, poczekalniach) oraz takich, które nie gwarantują zachowania poufności rozmów.
- 6.2. Pracownikom zabrania się zapisywania w systemach poczty głosowej informacji wrażliwych (tzn. Takich, które są istotne i chronione na najwyższym poziomie).
- 6.3. Odczytanie indywidualnych wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła.
- 6.4. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
- 6.5. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających informacje chronione jest zabronione.

7. ZASADY TRANSMISJI PLIKÓW W SIECI TELEINFORMATYCZNEJ

- 7.1. Informacje o wysokiej istotności (np. Dane osobowe), wysyłane poza sieć wewnętrzną muszą zostać zaszyfrowane.
- 7.2. Proponuje się wykorzystanie programów 7zip lub winrar, które dają możliwość zaszyfrowania plików, które chcemy wysłać pocztą elektroniczną.
- 7.3. Hasło do zaszyfrowanego pliku należy przekazać SMS'em lub telefonicznie. Zabronione jest wysyłanie hasła do maila - w mailu do tej osoby.



**Instrukcja Bezpieczeństwa Danych
Osobowych – Urząd Miasta w
Radymnie**

Strona 4 z 9

Wydanie 1

Data wydania 11.07.2023

- 7.4. Jeżeli pracownik nie dysponuje techniczną możliwością wysłania hasła, o którym mowa w punkcie 7.3., zaszyfrowane hasło przekazywane jest na adres poczty elektronicznej inny niż ten, na który wysłano zaszyfrowany plik. Hasło w odrębnej wiadomości może być przesłane otwartym tekstem.
- 7.5. Jeżeli używany program do edycji tekstu (np. MS Word lub Excel) daje możliwość zaszyfrowania pliku hasłem – można skorzystać z tej funkcjonalności zamiast rozwiązania opisanego w punkcie 7.2.

8. BEZPIECZNA POCZTA ELEKTRONICZNA

- 8.1. W przypadku jednostek publicznych, zaleca się korzystanie wyłącznie z Elektronicznej Platformy Usług Administracji Publicznej (e-PUAP), dopuszczalne jest wykorzystywanie poczty do zastosowań biznesowych.
- 8.2. Nie zaleca się korzystania z darmowych kont pocztowych.
- 8.3. Nie zaleca się zapisywania haseł do poczty elektronicznej przez przeglądarkę internetową.
- 8.4. Podczas wysyłania wiadomości należy zweryfikować poprawność adresów e-mail odbiorcy.
- 8.5. Bezpieczne logowanie do poczty elektronicznej:
- 8.5.1. Jeśli logujesz się do swojego konta poprzez interfejs webmail, korzystając z przeglądarki internetowej, sprawdź jaki adres pojawia się w pasku adresu. Powinien rozpoczynać się <https://>.
- 8.5.2. Sprawdź certyfikat bezpieczeństwa (należy kliknąć kłódkę tuż obok paska adresu – wtedy wyświetla się informacja czy połączenie jest szyfrowane).
- 8.5.3. Jeżeli zarządzasz swoją pocztą elektroniczną włącz filtr antyspamowy.
- 8.5.4. Nie otwieraj załącznika, jeśli nie jesteś pewien, kto wysłał do Ciebie wiadomość.
- 8.5.5. Unikaj otwierania plików, które zawierają końcówkę: exe, .bat, .com, .lnk, .scr, .vbs.
- 8.5.6. Nie klikaj w linki od nieznanymi nadawców, mogą zawierać przekierowanie do zainfekowanych stron.
- 8.5.7. Nie odpowiadaj na wiadomości od podejrzanych nadawców.
- 8.5.8. Korzystaj z dwuetapowego systemu uwierzytelniania, jeśli jest taka możliwość.
- 8.5.9. Jeśli uznasz wiadomość za niechcianą i podejrzaną, oznacz ją jako SPAM. Możesz to zrobić poprzez wciśnięcie przycisku „zgłoś SPAM”. Umożliwia Ci to filtr antyspamowy. Możesz również dodać nadawcę do tzw. Listy zablokowanych nadawców. W ten sposób uczysz swój filtr antyspamowy właściwej oceny swoich maili.
- 8.5.10. Do każdego konta podawaj zawsze inne hasło.
- 8.6. Korespondencja elektroniczna:
- 8.6.1. Pracownik przesyłając informacje za pośrednictwem poczty elektronicznej ponosi odpowiedzialność za prawidłowe zaadresowanie wiadomości elektronicznej i przesłanie jej do uprawnionego odbiorcy.
- 8.6.2. Zabrania się przesyłania za pośrednictwem poczty elektronicznej treści niezgodnych z obowiązującymi przepisami prawa, naruszających zasady współżycia społecznego oraz naruszających prawa własności intelektualnej innych osób.
- 8.6.3. Zabrania się przesyłania do innych pracowników, wiadomości o treści niezwiązanej z jej działalnością, a w szczególności wiadomości elektronicznych zawierających m.in.: informacje o charakterze komercyjnym, niechcianych lub niepotrzebnych wiadomości.
- 8.6.4. Zabrania się rozsyłania za pośrednictwem poczty elektronicznej załączników zawierających pliki zagrażające lub mogące zagrażać bezpieczeństwu systemu teleinformatycznego pracodawcy.
- 8.6.5. Zabrania się wykorzystywania przydzielonego pracownikowi służbowego konta pocztowego do celów prywatnych (np. Prowadzenie korespondencji nie związanej z



Instrukcja Bezpieczeństwa Danych Osobowych – Urząd Miasta w Radymnie

Strona 5 z 9

Wydanie 1

Data wydania 11.07.2023

działalnością służbową, rejestrowania się przy użyciu konta służbowego na forach, portalach społecznościowych, newsletterach, itp.).

- 8.6.6. Zabrania się przekierowywania poczty służbowej na prywatną skrzynkę (np. W celu pracy w domu).
- 8.6.7. Wiadomości przesyłane pocztą elektroniczną poza sieć służbową, zawierające informacje chronione należy zabezpieczyć.
- 8.6.8. W ramach użytkowania poczty elektronicznej zabrania się wysyłania plików multimedialnych (np. .mp3, .wav, .mov, .avi) oraz wykonywalnych (np. Exe, .bat, .com, .cmd), chyba że wynika to wprost z obowiązków służbowych wykonywanych przez pracownika.

9. ZASADA CZYSTEGO EKРАНU

- 9.1. Należy zadbać, aby ustawienia monitorów stacji roboczych nie pozwalały na przeglądanie wyświetlonych informacji osobom postronnym (np. ułożenie monitora komputera „plecami” do wejścia do pomieszczenia lub wydzielonego miejsca na przyjęcie klienta/osoby trzeciej).
- 9.2. Pracownik zobowiązany jest do utrzymywania porządku na pulpicie komputera, w tym w szczególności przechowywania dokumentów w dedykowanych folderach, ograniczając jednocześnie liczbę folderów. Zaleca się, aby na pulpicie komputera znajdowały się jedynie ikony standardowego oprogramowania i aplikacji oraz skróty folderów pod warunkiem, że ich nazwy nie zawierają informacji o ich zawartości lub treści

10. ZASADY STOSOWANIA HASEŁ

- 10.1. Obowiązkiem pracownika jest zmiana hasła:
 - 10.1.1. dla systemów dziedzicznych raz na 90 dni.
 - 10.1.2. dla systemu operacyjnego indywidualnych stacji roboczych raz na 90 dni.
 - 10.1.3. dla systemów zewnętrznych zgodnie z instrukcjami właściciela zasobu.
- 10.2. Hasło powinno być złożone z minimum 12 znaków, dużych i małych liter, cyfr i znaków specjalnych.
- 10.3. Nie dopuszcza się stosowania haseł zawierających: imiona, nazw pracownika, daty, nazwy miast czy państw oraz wyrazów posiadających skojarzenie z osobą.
- 10.4. Udostępnianie własnego hasła jest rażącym naruszeniem obowiązków pracowniczych.
- 10.5. Hasło nie powinno być zapisywane.
- 10.6. W przypadku podejrzenia, iż nasze hasło zostało ujawnione/skompromitowane (zostało zagubione, poznały je niepowołane osoby) należy bezzwłocznie powiadomić o tym fakcie informatyka telefonicznie lub za pośrednictwem poczty elektronicznej na adres: informatyk@radymno.pl (przy czym dotyczy to wyłącznie osób posiadających służbowe konta pocztowe).
- 10.7. Niedopuszczalne jest stosowanie tych samych haseł prywatnie oraz w pracy.
- 10.8. W przypadku zablokowania konta należy zwrócić się do informatyka telefonicznie oraz na za pośrednictwem poczty elektronicznej w celu jego odblokowania w celu jego odblokowania.

11. ZASADY UŻYTKOWANIA SYSTEMÓW INFORMATYCZNYCH



Instrukcja Bezpieczeństwa Danych Osobowych – Urząd Miasta w Radymnie

Strona 6 z 9

Wydanie 1

Data wydania 11.07.2023

- 11.1. Należy przywiązywać szczególną uwagę do weryfikacji poprawności danych przed ich wprowadzeniem do systemu. Wprowadzane dane powinny spełniać wymagania odnośnie jakości.
- 11.2. Wszelkie problemy z jakością oraz błędy w danych zauważone podczas przetwarzania danych należy niezwłocznie zgłaszać przełożonym lub rejestrować w systemie zgłoszeń incydentów, których te problemy dotyczą.
- 11.3. Należy postępować zgodnie z instrukcjami informatyka.

12. OPROGRAMOWANIE

- 12.1. Pracownik może korzystać jedynie z oprogramowania, na które pracodawca posiada aktualne licencje lub posiada prawo do używania.
- 12.2. Pracownik nie może za pomocą komputerów służbowych pobierać z Internetu lub przysyłać nielicencjonowanego oprogramowania oraz innych utworów chronionych prawem autorskim (w tym w szczególności utworów muzycznych, filmów, grafiki, gier komputerowych i tym podobnych).
- 12.3. Pracownik nie może instalować na komputerach pracodawcy prywatnych kopii oprogramowania, plików muzycznych i video, z żadnego nośnika i z żadnego innego urządzenia.

13. ZASADY DOTYCZĄCE DOSTĘPU DO SIECI INTERNET

- 13.1. Dostęp do sieci Internet może odbywać się wyłącznie na podstawie nadanych uprawnień w zakresie realizowania zadań służbowych. Korzystając z usług sieciowych należy przestrzegać następujących zasad:
 - 13.1.1. Użytkować Internet wyłącznie do celów służbowych,
 - 13.1.2. Korzystać wyłącznie z witryn internetowych niezbędnych do realizacji zadań służbowych,
 - 13.1.3. Zweryfikować certyfikaty udostępniane na witrynie,
 - 13.1.4. Pliki zawierające dane chronione należy przed wysłaniem zabezpieczyć (stosując szyfrowanie wiadomości z hasłem do otwarcia pliku).
- 13.2. Korzystaj z antywirusa i konta z ograniczonymi uprawnieniami (nie admina).
- 13.3. W przypadku oznak zainfekowania komputera złośliwym oprogramowaniem należy:
 - 13.3.1. Powiadomić Informatyka - osoba odpowiedzialna za nadzór i konserwację systemów informatycznych (zadanie pracownika).
 - 13.3.2. Odłączyć komputer od sieci lokalnej oraz sieci Internet (zadanie osoby odpowiedzialnej za nadzór i konserwację systemów informatycznych).
 - 13.3.3. Jeśli nie można uruchomić komputera z dysku twardego (błąd przy starcie), należy spróbować uruchomić system w trybie awaryjnym lub przy użyciu dysku startowego systemu Windows (zadanie osoby odpowiedzialnej za nadzór i konserwację systemów informatycznych).
 - 13.3.4. Wykonać pełne skanowanie systemu operacyjnego (zadanie osoby odpowiedzialnej za nadzór i konserwację systemów informatycznych).
- 13.4. Korzystanie z sieci Internet.
 - 13.4.1. Pracownik ma prawo korzystać z sieci Internet wyłącznie: w celach związanych z realizacją zadań służbowych, zgodnie z obowiązującymi regulaminami i przepisami prawa, w zakresie przyznanym uprawnieniom.
 - 13.4.2. Pracownikowi zabronione jest korzystanie z sieci Internet w celu: uzyskania nieuprawnionego dostępu do zasobów będących własnością pracodawcy lub



Instrukcja Bezpieczeństwa Danych Osobowych – Urząd Miasta w Radymnie

Strona 7 z 9

Wydanie 1

Data wydania 11.07.2023

zasobów podmiotów zewnętrznych, pobierania, udostępniania i rozpowszechniania jakichkolwiek materiałów (informacji, danych, tekstów, programów komputerowych, dźwięków, fotografii, grafik, filmów) naruszających prawa własności intelektualnej, pobierania, udostępniania i rozpowszechniania jakichkolwiek materiałów zakazanych przepisami prawa, w tym m.in. Zawierających groźby, treści obraźliwe, zniesławiające, pornograficzne lub naruszających w jakikolwiek inny sposób prawa innych osób.

- 13.4.3. Zabronione jest podejmowanie przez pracowników działań powodujących istotne ograniczenia w korzystaniu z sieci Internet przez innych pracowników, a w szczególności: pobieranie dużej ilości danych, w sytuacji, gdy nie jest to uzasadnione wykonywanymi obowiązkami służbowymi, podejmowanie działań skutkujących ograniczeniami w funkcjonowaniu jakichkolwiek usług sieciowych.
- 13.4.4. Zabronione jest umożliwianie dostępu z Internetu do zasobów zlokalizowanych na urządzeniu komputerowym lub w sieci służbowej (np. Przy wykorzystaniu serwerów WWW, ftp, programów tunelujących, P2P).

14. ZASADY KORZYSTANIA Z KOMPUTERÓW PRZENOŚNYCH

- 14.1. Pracownik może wnosić sprzęt komputerowy wyłącznie za zgodą przełożonego, po uprzednim upewnieniu się, że urządzenie zostało zaszyfrowane - np. Poprzez ustanowienie hasła dostępu.
- 14.2. Komputer nie może być udostępniany osobom nieuprawnionym.
- 14.3. Instalacja oprogramowania może być dokonywana wyłącznie przez informatyka.
- 14.4. W przypadku kradzieży komputera należy o tym fakcie poinformować przełożonego oraz informatyka.
- 14.5. W razie utracenia urządzenia mobilnego – bez względu na to, czy był on szyfrowany, czy też nie – pracownik jest zobowiązany do poinformowania o tym Informatyka oraz swojego bezpośredniego przełożonego.
- 14.6. Obowiązuje zakaz wykorzystywania prywatnych nośników informacji (płyty CD, DVD, kart SD, kart SSD, dysków zewnętrznych, pendrive, laptopów i im podobnych) do celów służbowych.
- 14.7. Komputery przenośne po zakończonej pracy winny być przechowywane w warunkach zapewniających ich bezpieczeństwo (np. szafy zamykane na klucz).

15. ZASADY DOTYCZĄCE POLITYKI ANTYWIRUSOWEJ

- 15.1. W przypadku, gdy program antywirusowy zgłasza nieaktualną bazę sygnatur wirusów należy o tym fakcie poinformować informatyka telefonicznie lub za pośrednictwem poczty elektronicznej.
- 15.2. W przypadku identyfikacji wirusa na komputerze należy zawiesić pracę i niezwłocznie o tym fakcie poinformować informatyka.
- 15.3. Wszystkie nośniki zewnętrzne podłączane do stacji roboczej należy przed użyciem sprawdzić programem antywirusowym.

16. ZGŁASZANIE ZDARZEŃ MOGĄCYCH ŚWIADCZYĆ O NARUSZENIU BEZPIECZEŃSTWA



Instrukcja Bezpieczeństwa Danych Osobowych – Urząd Miasta w Radymnie

Strona 8 z 9

Wydanie 1

Data wydania 11.07.2023

16.1. Wszystkie niestandardowe działania systemu informatycznego oraz zdarzenia mogące wskazywać na utratę bezpieczeństwa powinny być niezwłocznie zgłoszone informatykowi telefonicznie lub za pośrednictwem poczty elektronicznej.

16.2. Symptomy wskazujące, na możliwość naruszenia bezpieczeństwa teleinformatycznego:

- obcy identyfikator w oknie logowania,
- nietypowe obciążenie (spowolnienie pracy) stacji roboczej,
- nowe oprogramowanie nieznanego typu,
- wyłączony program antywirusowy,
- zwiększona ilość niechcianej poczty (spamu),
- brak możliwości zalogowania się na własny identyfikator i hasło,
- nazwy plików w historii, które nie były otwierane,
- widoczne ślady przebywania osób trzecich w czasie nieobecności.

17. ZASADY NAPRAWY SPRZĘTU KOMPUTEROWEGO

- 17.1. W przypadku, gdy na nośnikach stanowiących integralną część sprzętu przekazywanego do naprawy, znajdują się informacje podlegające ochronie, pracownik ma obowiązek zgłosić ten fakt przy przekazywaniu urządzenia do serwisu. Sprzęt taki naprawiany jest pod nadzorem informatyka lub innego właściwego pracownika. Jeżeli zaś taki nadzór nie jest możliwy, to informacje muszą być uprzednio skutecznie usunięte, przy zapewnieniu możliwości ich późniejszego odtworzenia, bądź jeśli istnienie możliwość wymontowania nośnika danych (np. Dysku twardego z komputera przenośnego), urządzenie należy przekazać do naprawy po uprzednim wymontowaniu nośnika. Fakt oddania urządzenia do naprawy stwierdza się poprzez spisanie protokołu zdawczo-odbiorczego.
- 17.2. Niedopuszczalny jest samodzielny serwis urządzenia komputerowego lub jego rozmontowywanie przez pracownika.
- 17.3. Pamiętaj, że takie same zagrożenia jakie generuje laptop, w większości przypadków dotyczą również telefonów komórkowych.

18. ZASADY MONITOROWANIA USŁUG I ZASOBÓW

- 18.1. Wszelkie usługi (np.: poczta elektroniczna, serwer plików, Internet), do których pracownik posiada dostęp, nie mogą być wykorzystywane do celów prywatnych ani działań, które stanowią naruszenie obowiązującego w Polsce prawa np. Sabotaż, przestępstwa informatyczne, oszustwa, przemoc, rasizm, terroryzm itp.
- 18.2. Pracownik zobowiązany jest przechowywać kopie dokumentów istotnych dla funkcjonowania Jednostki w folderach sieciowych w celu zapewnienia możliwości objęcia ich procesem tworzenia kopii zapasowych. Dostęp do takich katalogów powinny mieć jedynie osoby uprawnione.
- 18.3. Informacje wrażliwe (np. Dane osobowe, tajemnica przedsiębiorstwa) przesyłane pocztą elektroniczną poza siecią służbową winny być przesyłane w postaci zaszyfrowanej lub przesyłane w skompresowanym załączniku z użyciem hasła. Hasło powinno być przekazywane przy wykorzystaniu innego kanału komunikacji np. Telefonicznie, przy pomocy wiadomości sms.
- 18.4. Komputery, konta pocztowe, nośniki danych – pamięci flash (pendrive) i inne urządzenia przekazane w ramach obowiązków służbowych, stanowią własność Jednostki i mogą być wykorzystywane wyłącznie w ramach realizacji powierzonych zadań związanych z wykonywaną pracą.



**Instrukcja Bezpieczeństwa Danych
Osobowych – Urząd Miasta w
Radymnie**

Strona 9 z 9

Wydanie 1

Data wydania 11.07.2023

18.5. Wszelkie dane wytworzone przez pracowników na urządzeniach komputerowych należących do pracodawcy są jego własnością.

18.6. Przełożeni pracowników, mają prawo i obowiązek kontrolować, czy pracownicy korzystający z urządzeń komputerowych stosują się do regulacji określonych w niniejszym dokumencie.

**19. ZASADY ODPOWIEDZIALNOŚCI PRACOWNIKÓW ZA SZKODY ZWIĄZANE
Z NIEPRAWIDŁOWYM UŻYTKOWANIEM URZĄDZEŃ SŁUŻBOWYCH**

19.1. W przypadku uszkodzenia urządzenia komputerowego wynikającego z rażącego zaniedbania pracownika w zakresie sprawowania opieki nad powierzonym urządzeniem, pracownik ten może zostać obciążony kosztami jego naprawy bądź wymiany. Decyzję o obciążeniu kosztami naprawy, bądź odtworzenia sprzętu podejmuje bezpośredni przełożony pracownika.

19.2. Pracownicy naruszający zasady korzystania ze sprzętu komputerowego określone w niniejszym dokumencie, mogą podlegać odpowiedzialności na zasadach określonych w obowiązujących przepisach prawa.

19.3. Pracownicy ponoszą pełną odpowiedzialność za:

- powierzony sprzęt;
- naruszenie prywatności innego pracownika;
- dopuszczenie do infrastruktury teleinformatycznej osób nieuprawnionych;
- udostępnienie swojego komputera lub konta innej osobie oraz wykorzystanie przez nią dostępu do infrastruktury;
- podszywanie się pod innych pracowników;
- wszelkie dane przechowywane w ramach kont pocztowych;
- wszelkie dane przechowywane na komputerze służbowym podłączonym do sieci LAN oraz poczynania dokonywane za pomocą swojego komputera lub z wykorzystaniem swojego konta.