

Zarządzenie Nr 65/2023
Burmistrza Miasta Pionki
z dnia 25 maja 2023 roku

w sprawie zasad organizacji i korzystania z poczty elektronicznej w Urzędzie Miasta Pionki

Na podstawie art. 33 ust. 1, ust. 3 i ust. 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. 2023 r. poz. 40 ze zm.), ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), zarządzam, co następuje:

§ 1. Wprowadzam do stosowania w Urzędzie Miasta Pionki Zasady organizacji i korzystania z poczty elektronicznej, które stanowią Załącznik nr 1 do niniejszego zarządzenia.

§ 2. Zobowiązuję pracowników Urzędu Miasta Pionki do przestrzegania zasad organizacji i korzystania z poczty elektronicznej określonych niniejszym zarządzeniem.

§ 3. Wykonanie zarządzenia powierzam Kierownikom komórek organizacyjnych Urzędu Miasta Pionki.

§ 4. Nadzór nad zarządzeniem powierzam Sekretarzowi Miasta Pionki.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.



BURMISTRZ MIASTA

(-) Robert Kowalczyk

**Zasady organizacji i korzystania z poczty elektronicznej
w Urzędzie Miasta Pionki**

**Rozdział 1
Postanowienia ogólne**

§ 1. W celu zapewnienia efektywnej, skutecznej i bezpiecznej wymiany informacji w postaci elektronicznej, zarówno wewnątrz Urzędu Miasta Pionki, jak i z klientami zewnętrznymi, wprowadza się niniejsze zasady organizacji i korzystania z poczty elektronicznej.

§ 2. Ilekroć w niniejszej instrukcji jest mowa o:

1. Urzędzie - należy przez to rozumieć Urząd Miasta Pionki, ul. Aleja Jana Pawła II 15, 26-670 Pionki;
2. Burmistrzu - należy przez to rozumieć Burmistrza Miasta Pionki;
3. komórkach organizacyjnych - należy przez to rozumieć wydziały, Urząd Stanu Cywilnego, samodzielne stanowiska pracy oraz powołane w Urzędzie doraźne lub stałe zespoły;
4. Kierownikach – należy przez to rozumieć kierowników komórek organizacyjnych;
5. Administratorze Systemów Informatycznych (ASI) - należy przez to rozumieć osobę wyznaczoną przez Burmistrza odpowiedzialną za bezpieczeństwo informacji w tym danych osobowych w systemach informatycznych;
6. Koordynatorze Bezpieczeństwa Informacji (KBI) - należy przez to rozumieć osobę wyznaczoną przez Burmistrza odpowiedzialną za bieżący nadzór nad przestrzeganiem zasad zarządzania bezpieczeństwem informacji w Urzędzie;
7. Pracownikach - należy przez to rozumieć pracowników Urzędu bez względu na rodzaj zawartej umowy o pracę;
8. świadczeniu usługi drogą elektroniczną - należy przez to rozumieć wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;
9. środkach komunikacji elektronicznej - należy przez to rozumieć rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztę elektroniczną;
10. usługodawcy - należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową świadczy usługi drogą elektroniczną;
11. usługobiorcy - należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która korzysta z usługi świadczonej drogą elektroniczną.

§ 3. 1. Urząd używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności.

2. Urząd organizując przetwarzanie danych w systemie teleinformatycznym, zapewnia możliwość przekazywania danych również w postaci elektronicznej przez wymianę dokumentów elektronicznych związanych z załatwianiem spraw należących do jego zakresu działania, wykorzystując informatyczne nośniki danych lub środki komunikacji elektronicznej.

3. Urząd udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.

4. Urząd realizując zadania publiczne przy wykorzystaniu systemu teleinformatycznego albo z użyciem środków komunikacji elektronicznej do przekazywania danych pomiędzy nim a podmiotem niebędącym organem administracji rządowej:

1) zapewnia, aby system teleinformatyczny służący do wymiany danych pomiędzy nim a podmiotami niebędącymi organami administracji rządowej, poza minimalnymi wymaganiami, o których mowa w ust. 1, spełniał wymóg równego traktowania rozwiązań informatycznych;

2) publikuje w Biuletynie Informacji Publicznej lub udostępnia w inny sposób zestawienie stosowanych w oprogramowaniu interfejsowym systemu teleinformatycznego, używanego przez niego do realizacji zadań publicznych, struktur dokumentów elektronicznych, formatów danych oraz protokołów komunikacyjnych i szyfrujących.

5. Obowiązki usługodawcy i usługobiorcy, zasady ochrony danych osobowych oraz jego odpowiedzialność w związku ze świadczeniem usług drogą elektroniczną określa ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

Rozdział 2

Odpowiedzialność i uprawnienia

§ 4. 1. Odpowiedzialność za przestrzeganie niniejszych zasad ponoszą wszyscy Pracownicy realizujący zadania przy wykorzystaniu systemu teleinformatycznego albo z użyciem środków

komunikacji elektronicznej zgodnie z posiadanymi zakresami obowiązków.

2. W sprawach nieuregulowanych zastosowanie mają odpowiednio zasady zarządzania bezpieczeństwem informacji w Urzędzie Miasta Pionki oraz inne przepisy prawa lub procedury wewnętrzne.

§ 5. 1. Poczta elektroniczna może być wykorzystywana tylko do celów służbowych.

2. Pracownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego do wszelkiej korespondencji z innymi Pracownikami Urzędu oraz klientami zewnętrznymi.

3. Przy korespondencji zewnętrznej Pracownik musi pamiętać, iż kieruje korespondencję w imieniu Urzędu, wobec czego jest zobowiązany do stosowania między innymi następujących reguł:

1) sprawdzać skrzynkę pocztową codziennie, minimum dwukrotnie, do godz. 9.00 oraz drugi raz po godz. 13.00;

2) bezzwłocznie (z zachowaniem terminu ustawowego) odpowiadać na każde pismo od podmiotu zewnętrznego;

3) odpowiadając na pismo zawsze określać jego temat;

4) umieszczać swój podpis;

5) pliki zawierające zbiory danych osobowych przysyłać w formie pliku zaszyfrowanego, zabezpieczonego hasłem;

6) korespondencję e-mailową w danej sprawie odkładać do akt sprawy.

4. Pracownik zobowiązany jest do okresowej archiwizacji wiadomości (skrzynki pocztowe posiadają ograniczoną wielkość).

5. Użytkownikom poczty zabrania się:

- 1) otwierania linków oraz załączników poczty elektronicznej ze źródeł niewiadomego pochodzenia;
- 2) przesyłania i udostępniania danych naruszających prawo, powszechnie uznanych za obsceniczne lub obraźliwe oraz oszczerstw i treści obrażającej uczucia innych;
- 3) rozpowszechniania materiałów o treści pornograficznej, propagujących przemoc, nawołujących do nietolerancji i nienawiści itp., lub naruszających obowiązujące prawo;
- 4) uprawiania hazardu;
- 5) rozpowszechniania niechcianych wiadomości e-mail (spamu);
- 6) prowadzenia działalności komercyjnej nie związanej z działalnością Urzędu;
- 7) rozsyłania listów, które wykorzystując elementy socjotechniki generują niepożądany ruch na serwerach poczty elektronicznej oraz treści prawem chronionych bez odpowiedniego zabezpieczenia np. szyfrowania;
- 8) przesyłania i udostępniania treści niezgodnych z prawem lub będących przedmiotem ochrony własności intelektualnej lub mogących naruszyć czyjekolwiek prawa osobiste;
- 9) rozpowszechniania wirusów komputerowych i innych programów mogących uszkodzić komputery innych użytkowników Internetu.

6. Niedopuszczalne są próby włamań na konta innych użytkowników.

§ 6. 1. Wiadomości wysyłane ze służbowej skrzynki pocztowej stanowią własność pracodawcy

i Burmistrz może je kontrolować.

2. Z uwagi na konieczność zapewnienia ochrony interesu i bezpieczeństwa Urzędu Burmistrz zastrzega sobie prawo do wglądu we wszystkie wiadomości Pracownika o charakterze służbowym (zarówno w skrzynce odbiorczej, jak i w wiadomości wysłane).

3. Kontrola służbowej korespondencji Pracowników oraz ich poczty elektronicznej może nastąpić po wcześniejszym uprzedzeniu pracownika.

4. Burmistrz ma również prawo kontroli przestrzegania przez Pracowników zasad korzystania ze służbowej poczty elektronicznej określonych w innych procedurach wewnętrznych.

§ 7. 1. Nadzór i opiekę techniczną nad systemem poczty elektronicznej Urzędu sprawuje ASI.

2. Zobowiązuje się ASI do monitorowania połączeń i natężenia ruchu w sieci Urzędu i rejestrowanie oraz zgłaszania Burmistrzowi rażących przypadków naruszeń niniejszych zasad.

3. Działania ASI zmierzające 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 nielegalnej treści oraz kontroli antywirusowej nie wymagają zgody Pracownika.

4. ASI przeprowadza raz w roku – kontrole ogólne oraz doraźnie - na wybranych stanowiskach.

Rozdział 3

Przebieg realizacji/opis czynności

§ 8. 1. Wniosek do ASI o nadanie adresu służbowej skrzynki poczty elektronicznej (dalej konta

pocztowego) dla nowozatrudnionego Pracownika składają Kierownicy niezwłocznie po uzyskaniu przez niego stosownych upoważnień.

2. Nadanie, unieważnienie, przywrócenie dostępu do konta pocztowego następuje na wniosek, którego wzór określa załącznik do niniejszych zasad.
3. Nadanie lub zmiana adresu konta pocztowego może również nastąpić w wyniku zmian dostawcy usług, wówczas wniosek, o którym mowa w ust. 1 nie jest wymagany.
4. Adres konta pocztowego zostanie utworzony wedle następującego wzorca:

pierwsza mała litera imienia.z małej litery nazwisko@pionki.pl

lub

nazwa komórki organizacyjnej (skrót wynikający z regulaminu organizacyjnego)@pionki.pl

lub

nazwa zadania.@pionki.pl

lub

nazwa jednostki organizacyjnej.@pionki.pl .

5. ASI przekaze pracownikowi szczegóły dotyczące pierwszego logowania oraz hasło do konta pocztowego.

6. Zaleca się stosowanie haseł na poziomie WYSOKIM, składających się z minimum 8 znaków

długości, czterech rodzajów znaków (mała litera, duża litera, cyfra, znak specjalny).

7. Pracownik jest zobowiązany do zachowania hasła w poufności i nieujawniania go osobom trzecim.

8. W przypadku ustania zatrudnienia danego Pracownika Kierownicy niezwłocznie wnioskują do ASI o usunięcie dostępu do jego konta pocztowego.

9. Konto użytkownika może być także zablokowane w przypadkach związanych z naruszeniem

bezpieczeństwa lub z innych ważnych powodów, decyzję podejmuje KBI w porozumieniu z Burmistrzem.

10. Odblokowanie konta użytkownika po incydencie wymaga nadania nowego hasła tymczasowego dostępu do systemu informatycznego.

12. Kończąc świadczenie pracy dla Urzędu, Pracownik jest zobowiązany przekazać wszystkie dane zapisane w komputerze (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje) związane z wykonywanymi zadaniami służbowymi kierownikowi, a w przypadku samodzielnych stanowisk sekretarzowi i ASI.

§ 9. 1. Pracownicy, aby dowiedzieć się, czy można bezpiecznie otworzyć daną stronę, powinni

sprawdzić informacje o jej zabezpieczeniach.

2. Jeśli nie można wejść na stronę bezpiecznie lub z zachowaniem prywatności, przeglądarka wyświetla ostrzeżenie.

3. Aby sprawdzić zabezpieczenia strony, należy zobaczyć symbol stanu bezpieczeństwa na lewo od adresu internetowego i ewentualnie kliknąć ikonę, np.:

1) Bezpieczna

2) Informacje lub Niezabezpieczona

3) Niezabezpieczona lub Niebezpieczna

- § 10.** 1. Bardzo częstym atakiem na internautów jest tzw. atak socjotechniczny, intruz najczęściej namawia do otwarcia załącznika poczty elektronicznej, taki załącznik zawiera w sobie złośliwe oprogramowanie, które jest uruchamiane wraz z jego otwarciem.
2. Najskuteczniejszą metodą obrony przed tymi atakami jest nie otwieranie załączników, których wiadomość jest spersonalizowana – jest skierowana bezpośrednio do nadawcy określonego z imienia lub nazwiska, choć może być i tak, że skierowana jest po prostu

„do Ciebie” korzystając z powszechnie przyjętych form grzecznościowych, np.: „Szanowna Pani”, „Szanowny Panie”, ponadto:

a) wiadomość zawiera szczegółowe instrukcje dalszego postępowania, np.: „otwórz załącznik”.

b) wiadomość w swej treści, lub poprzez wyraźne wskazanie, zawiera zachętę do szybkiego działania, gdyż zwłoka może spowodować problemy, np.: może nastąpić blokada konta, egzekucja długu, wstrzymanie świadczenia usługi, itp., działanie pod presją ma zmusić do popełnienia błędu.

c) wiadomość bardzo często zawiera błędy ortograficzne lub gramatyczne, jest napisana nieskładnie i niechlujnie, w wyjątkowych sytuacjach jest napisana z wykorzystaniem automatycznego tłumaczenia treści na język polski, co akurat czyni ją na tyle niewiarygodną, że w praktyce odsuwa groźbę skutecznego ataku.

d) atakujący w swoim mailu prosi o dane, do których nie powinien mieć dostępu, klasycznym przykładem jest próba wymuszenia podania hasła lub niektórych danych osobowych.

3. Dodatkowo, aby nie dopuścić do automatycznej infekcji poprzez pocztę elektroniczną, warto:

a) wyłączyć autopodgląd otrzymywanych informacji, co uniemożliwi automatyczny ich odczyt

i wykonanie złośliwego kodu, w sytuacji kiedy email takowy zawiera.

b) wyłączyć obsługę Javy i HTML, których wykonanie może również skutkować w infekcji złośliwym kodem.

4. Oprócz podstawowej porady nieotwierania załącznika, aby obronić się przed tego typu atakiem, warto również pamiętać o aktualizacji swojego systemu operacyjnego i aplikacji oraz wyłączeniu niepotrzebnych w systemie opcji, np.: obsługi makr czy języka JavaScript.

5. Zupełnym minimum jest posiadanie oprogramowania antywirusowego, które jest w stanie wykryć jako niebezpieczne większość załączników zawierających wirusy komputerowe.

6. Jedną z powszechniejszych metod inicjacji ataku jest dotarcie do przyszłej ofiary poprzez pocztę elektroniczną, cyberprzestępcy robią to głównie poprzez rozsyłanie spamu, dlatego ważne jest aby korzystać z kilku podstawowych porad:

a) nie odpowiadaj nigdy na spam przesłany do Ciebie – taka odpowiedź to najlepsze potwierdzenie poprawności Twojego adresu email.

b) jeśli do Twojej skrzynki przedostał się spam spróbuj jego próbką „zasilić” swój mechanizm antyspamowy, np.: poprzez dodanie adresu spamera do listy tych, od których nie chcesz dostawać korespondencji.

7. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”, zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”.

8. Podczas wysyłania maili, w szczególności do wielu adresatów jednocześnie, należy załączyć

informację dotyczącą bezpieczeństwa informacji według poniższego wzoru: „Niniejsza wiadomość jest informacją prawnie chronioną. Wiadomość jest przeznaczona wyłącznie dla adresata a dostęp do niej przez osoby trzecie jest niedozwolony. Jeżeli nie jesteś docelowym odbiorcą wiadomości, ujawnianie, kopiowanie oraz rozpowszechnianie, a także wykorzystywanie informacji jest zabronione i może być karalne. Jeżeli przypadkowo otrzymałeś tę wiadomość proszę o natychmiastowe trwałe jej usunięcie oraz powiadomienie o tym nadawcy.”

9. Należy każdorazowo zgłaszać ASI przypadki podejrzanых emaili.

10. Za organizację skrzynek e-mailowych w wydziale odpowiada Kierownik (również podczas zastępstw w razie nieobecności pracownika). Przekierowania e-maili na pisemny wniosek Kierownika dokonuje ASI.

11. Za organizację skrzynek e-mailowych dla samodzielnych stanowisk w Urzędzie odpowiada Sekretarz. Przekierowania e-maili na pisemny wniosek Sekretarza dokonuje ASI.
12. Przed ustaniem stosunku pracy, pracownik przekazuje zawartość skrzynki e-mailowej, tj. wszystkie e-maile ze skrzynki, Kierownikowi lub w przypadku samodzielnych stanowisk Sekretarzowi. Konto do usunięcia przez ASI powinno zostać puste.

Rozdział 4

Postanowienia końcowe

§ 11. Wobec Pracowników, naruszających niniejsze zasady stosowane będą blokady kont pocztowych, oraz konsekwencje służbowe przewidziane Regulaminem Pracy Urzędu.

§ 12. W sprawach nieuregulowanych w niniejszych zasadach stosuje się obowiązujące przepisy prawa.



BURMISTRZ MIASTA

(-) Robert Kowalczyk

Załącznik do zasad organizacji i korzystania
z poczty elektronicznej
w Urzędzie Miasta Pionki

Wzór

Wniosek o nadanie/usunięcie/przywrócenie* dostępu do konta pocztowego

Pionki, dnia

.....
(imię i nazwisko Pracownika)

.....
(komórka organizacyjna)

**Administrator Systemów Informatycznych
w Urzędzie Miasta Pionki**

Zwracam się z wnioskiem o nadanie/usunięcie/przywrócenie* dostępu do konta
pocztowego o nazwie
w domenie @pionki.pl

.....
/pieczętka i podpis wnioskodawcy/

II. Obsługa wniosku

Akceptuję / Nie akceptuję*

Nadano/usunięto/przywrócono* dostęp do konta pocztowego:

.....@pionki.pl

.....
/data, podpis ASI/

* niepotrzebne skreślić