

**ZARZĄDZENIE NR 44/2022**  
**WÓJTA GMINY GRUTA**

z dnia 29 czerwca 2022 r.

**w sprawie zasad organizacji i korzystania z poczty elektronicznej w Urzędzie Gminy Gruta.**

Na podstawie art. 33 ust. 1, ust. 3 i ust. 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jednolity Dz. U. z 2022 poz. 559), ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jednolity Dz. U.2020 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 (tekst jednolity Dz. U.2017.2247), w związku z Zarządzeniem nr 71/2018 Wójta Gminy Gruta z dnia 31 grudnia 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych, zarządzam, co następuje:

§ 1. Wprowadzam do stosowania w Urzędzie Gminy Gruta Zasady organizacji i korzystania z poczty elektronicznej, które stanowią załącznik do niniejszego zarządzenia.

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

§ 3. Wykonanie zarządzenia powierzam Kierownikom komórek organizacyjnych Urzędu Gminy Gruta.

§ 4. Nadzór nad zarządzeniem powierzam Sekretarzowi Urzędu Gminy Gruta.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Zastępca Wójta Gminy Gruta

**Tomasz Groszewski**

## Zasady organizacji i korzystania z poczty elektronicznej w Urzędzie Gminy Gruta

### Rozdział 1.

#### Postanowienia ogólne

§ 1. W celu zapewnienia efektywnej, skutecznej i bezpiecznej wymiany informacji w postaci elektronicznej, zarówno wewnątrz Urzędu Miasta i Gminy Gruta 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 Gminy Gruta, Gruta 244, 86-330 Mełno;
2. **Wójcie** - należy przez to rozumieć Wójta Gminy Gruta;
3. **komórkach organizacyjnych** - należy przez to rozumieć referaty, 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 Wójta Gminy Gruta odpowiedzialną za bezpieczeństwo informacji w tym danych osobowych w systemach informatycznych;
5. **Pracownikach** - należy przez to rozumieć pracowników Urzędu bez względu na rodzaj zawartej umowy o pracę;
6. **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;
7. **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;
8. **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;
9. **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 Gminy Gruta oraz inne przepisy prawa lub procedury wewnętrzne.

§ 5. 1. Poczta elektroniczna może być wykorzystywana tylko do celów służbowych. Pracownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego do wszelkiej korespondencji z innymi Pracownikami Urzędu oraz klientami zewnętrznymi. Przy korespondencji zewnętrznej Pracownik musi pamiętać, iż kieruje korespondencją 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 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 zabezpieczonego hasłem;
- 6) korespondencję w danej sprawie odkładać do akt sprawy.
- 7) Pracownik zobowiązany jest do okresowej archiwizacji wiadomości (skrzynki pocztowe posiadają ograniczoną wielkość).

### **2. 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.

### **3. Niedopuszczalne są próby włamań na konta innych użytkowników.**

§ 6. 1. Wiadomości wysyłane z służbowej skrzynki pocztowej stanowią własność pracodawcy i Wójt Gminy Gruta może je kontrolować.

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

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

Wójt ma również prawo kontroli przestrzegania przez Pracowników zasad korzystania z służbowej poczty elektronicznej określonych w procedurach wewnętrznych.

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

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

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.

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.

Nadanie, unieważnienie, przywrócenie dostępu do konta pocztowego następuje na wniosek, którego wzór określa załącznik nr 2 do Zarządzenia Wójta Gminy Gruta nr 44/2022 z dnia 29 czerwca 2022 r. w sprawie zasad organizacji i korzystania z poczty elektronicznej w Urzędzie Gminy Gruta.

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.

Adres konta pocztowego zostanie utworzony wedle następującego wzorca:

pierwsza litera imienia i po kropce nazwisko; i.nazwisko@gruta.pl lub

nazwa komórki organizacyjnej: komorkaorganizacyjna@gruta.pl lub

stanowisko służbowe: stanowisko@gruta.pl lub

nazwa jednostki organizacyjnej: nazwajednostkiorganizacyjnej@gruta.pl.

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

Zaleca się stosowanie haseł na poziomie WYSOKIM, składających się z minimum 8 znaków długości, czterech rodzajów znaków (mała litera, duża litera, cyfra, znak specjalny).

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

W przypadku ustania zatrudnienia danego Pracownika Kierownicy niezwłocznie wnioskuje o unieważnienie dostępu do jego konta pocztowego.

Konto użytkownika może być także zablokowane w przypadkach związanych z naruszeniem bezpieczeństwa lub z innych ważnych powodów, decyzję podejmuje Wójt lub ASI.

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

Zasady postępowania określone w Polityce Ochrony Danych Osobowych w Urzędzie Gminy Gruta, stanowiącej załącznik do Zarządzenia nr 71/2018 Wójta Gminy Gruta z dnia 31 grudnia 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych stosuje się odpowiednio.

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 przełożonemu i ASI.

**§ 9. 1.** Pracownicy, aby dowiedzieć się, czy można bezpiecznie otworzyć daną stronę, powinni sprawdzić informacje o jej zabezpieczeniach.

Jeśli nie można wejść na stronę bezpiecznie lub z zachowaniem prywatności, przeglądarka wyświetla ostrzeżenie. Aby sprawdzić zabezpieczenia strony, należy zobaczyć symbol stanu bezpieczeństwa na lewo od adresu internetowego.

**§ 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:

- 1) wiadomość zawiera szczegółowe instrukcje dalszego postępowania, np.: „otwórz załącznik”.
- 2) 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.
- 3) 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.
- 4) 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:

- 1) wyłączyć autopodgląd otrzymywanych informacji, co uniemożliwi automatyczny ich odczyt i wykonanie złośliwego kodu, w sytuacji kiedy email takowy zawiera,
- 2) 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:

- 1) nie odpowiadaj nigdy na spam przesłany do Ciebie – taka odpowiedź to najlepsze potwierdzenie poprawności Twojego adresu email;
- 2) 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:

*"Ten adres e-mail oraz wszelkie załączone pliki są poufne i mogą zawierać informacje, które są chronione prawami własności intelektualnej. Jeżeli nie jest Pan/Pani zamierzonym adresatem powyższej wiadomości, nie może jej Pan/Pani ujawniać, kopiować, dystrybuować, ani też w żaden inny sposób udostępniać lub wykorzystywać. O błędnym zaadresowaniu wiadomości prosimy niezwłocznie poinformować nadawcę i usunąć wiadomość.,,*

9. Należy zgłaszać ASI przypadki podejrzanych wiadomości email.

#### **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 oraz procedury wewnętrzne.

Załącznik nr 2 do Zarządzenia Wójta Gminy Gruta  
nr 44/2022 z dnia 29 czerwca 2022 r.  
w sprawie zasad organizacji i korzystania z poczty  
elektronicznej  
w Urzędzie Gminy Gruta

Wzór

**Wniosek o nadanie/unieważnienie/przywrócenie\*  
dostępu do konta pocztowego**

Gruta dnia.....

.....

(imię i nazwisko Pracownika)

.....

(komórka organizacyjna)

**Administrator Systemów Informatycznych**

w Urzędzie Gminy Gruta

Zwracam się z prośbą o nadanie/unieważnienie/przywrócenie\* dostępu do konta  
pocztowego

o nazwie... ..

w domenie **gruta.pl**.

\* niepotrzebne skreślić

.....

(podpis wnioskodawcy)

**II. Obsługa wniosku**

Akceptuję / Nie akceptuję\*

**Nadano/unieważniono/przywrócono\* dostęp do konta pocztowego .....**  
**@gruta.pl**

\* niepotrzebne skreślić

.....

(data, podpis ASI)