WÓJT GMINY KWILCZ
UL. KARDYNAŁA STEFANA WYSZYŃSKIEGO 23
64-420 KWILCZ

Zarządzenie nr 58/2024
Wójta Gminy Kwilcz
z dnia 23.04.2023 r.

w sprawie wprowadzenia do użytku służbowego Procedury korzystania ze służbowej poczty elektronicznej w Urzędzie Gminy w Kwilczu.

Na podstawie art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L z 2016r. Nr 119, str 1 z póź. zm.)

Wójt Gminy Kwilcz
zarządza co następuje:

§ 1

Wprowadza się do użytku: „Procedurę korzystania ze służbowej poczty elektronicznej w Urzędzie Gminy w Kwilczu", stanowiącej załącznik nr 1 do zarządzenia.

§ 2

Zobowiązuje się wszystkich pracowników przetwarzających dane osobowe w Urzędzie Gminy w Kwilczu do stosowania i przestrzegania „Procedury korzystania ze służbowej poczty elektronicznej w Urzędzie Gminy w Kwilczu", o której mowa w § 1.

§ 3

1. Wykonanie zarządzenia powierza się Inspektorowi Ochrony Danych Osobowych.
2. Nadzór nad wykonaniem zarządzenia powierza się Sekretarzowi Gminy.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Stanisław Mannek

sprawdzono pod względem
formalno-prawnym
Małgorzata Jagodzińska
Radca Prawny

WÓJT GMINY KWILCZ
UL. KARDYNAŁA STEFANA WYSZYŃSKIEGO 23
64-420 KWILCZ

ZAŁĄCZNIK NR 1 DO ZARZĄDZENIA
NR 58/2024 WÓJTA GMINY KWILCZ
Z DNIA 23.04.2024 R.

PROCEDURA KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ W URZĘDZIE GMINY W KWILCZU

WSTĘP

Poczta elektroniczna stanowi kluczowy element współczesnej komunikacji w ramach organizacji jak i w sferze osobistej oferując możliwość szybkiego i skutecznego przesyłania wiadomości zarówno w obrębie organizacji, jak i na skalę globalną.

Niemniej jednak, użytkowanie e-maila nie jest wolne od ryzyka. Istnieje możliwość, że wiadomości mogą zostać przechwycone, nieautoryzowanie zapisane, odczytane lub nawet przekazane dalej przez osoby trzecie. Dodatkowo, nieoficjalne uwagi lub komentarze zamieszczone w treści e-maili lub w załącznikach mogą być błędnie zrozumiane przez adresatów, co potencjalnie prowadzi do konfliktów lub komplikacji prawnych. Jednym z głównych ryzyk jest również masowe wysyłanie wiadomości, które ujawniają prywatne adresy e-mail odbiorców, co stanowi naruszenie prywatności i ochrony danych osobowych. Z tego powodu, kluczowe jest ścisłe przestrzeganie zasad bezpiecznego korzystania z poczty elektronicznej, aby zminimalizować ryzyko i zapewnić odpowiednią ochronę przesyłanych danych. W obecnych czasach, odpowiednie zarządzanie i bezpieczne użytkowanie poczty elektronicznej są niezbędne do ochrony danych osobowych, bezpieczeństwa informacji i zapewnienia prywatności komunikacji.

PRZEDMIOT PROCEDURY

Niniejsza procedura ma na celu określenie jednolitych zasad korzystania z systemu służbowej poczty elektronicznej. Dokument ten został opracowany w celu zapewnienia, że wszystkie działania związane z używaniem poczty elektronicznej w ramach organizacji są realizowane w sposób bezpieczny, efektywny oraz zgodny z obowiązującymi przepisami o ochronie danych. Procedura ta dotyczy każdego pracownika mającego dostęp do systemu poczty e-mail oraz określa standardy postępowania, mające na celu minimalizację zagrożeń związanych z ochroną i przetwarzaniem danych osobowych i urzędowych.

CELE PROCEDURY

Głównym celem niniejszej procedury jest:

1. Zapewnienie spójności i zgodności w korzystaniu z służbowej poczty elektronicznej wśród wszystkich pracowników.

2. Ochrona poufności i integralności informacji przekazywanych drogą elektroniczną.

3. Zminimalizowanie ryzyka wystąpienia incydentów bezpieczeństwa, w tym nieautoryzowanego dostępu do informacji, ich utraty lub uszkodzenia.

4. Promowanie odpowiedzialnego i świadomego korzystania z narzędzi komunikacji elektronicznej.

5. Zapewnienie zgodności z obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych i tajemnicy przedsiębiorstwa.

ZAKRES OBOWIĄZUJĄCYCH ZASAD

Procedura dotyczy wszystkich aspektów związanych z korzystaniem z poczty elektronicznej, w tym, ale nie ograniczając się do:

a. Ustanowienie jasnych wytycznych dotyczących dozwolonego użytku służbowej poczty elektronicznej.

b. Definiowanie procedur zabezpieczeń, takich jak stosowanie haseł, szyfrowanie wiadomości oraz regularne aktualizacje oprogramowania antywirusowego.

c. Określenie zasad dotyczących archiwizacji korespondencji elektronicznej i zarządzania cyklem życia informacji.

d. Wskazanie odpowiednich działań w przypadku wykrycia podejrzanych lub nieautoryzowanych działań związanych z pocztą elektroniczną.

e. Podkreślenie znaczenia prywatności i poufności w komunikacji elektronicznej, wskazując na odpowiedzialność każdego użytkownika za ochronę przekazywanych danych.

ZASADY KORZYSTANIA Z SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ – SZCZEGÓŁOWE WYTYCZNE

1. Przeznaczenie Służbowe: Użycie służbowej poczty elektronicznej jest wyłącznie zarezerwowane dla celów zawodowych, co oznacza, że każdy pracownik jest zobowiązany do wykorzystywania tego narzędzia ściśle w zakresie wykonywania powierzonych mu zadań. Jakiekolwiek wykorzystanie poczty do celów prywatnych jest niezgodne z polityką urzędu.

2. Własność Korespondencji: Wszystkie e-maile generowane, odbierane lub wysyłane przez pracowników są uznawane za własność organizacji. Urząd zastrzega sobie prawo do dostępu do wszystkich wiadomości e-mail w ramach prowadzonej działalności, zgodnie z obowiązującym prawem i wewnętrznymi regulacjami.

3. Odpowiedzialność za Bezpieczeństwo Informacji: Oczekuje się, że użytkownicy służbowej poczty elektronicznej będą postępować z najwyższą ostrożnością, aby zabezpieczyć wszelkie przekazywane informacje przed nieautoryzowanym dostępem, zmianą, utratą lub zniszczeniem. Wszelkie działania, które mogą zwiększyć ryzyko naruszenia bezpieczeństwa danych, powinny być unikane.

4. Wyłączność Użycia Przydzielonych Adresów: Każdy pracownik ma prawo korzystać wyłącznie z adresu e-mail, który został mu przydzielony przez organizację. Używanie adresów e-mail przypisanych do innych pracowników, jak również dostęp do ich skrzynek pocztowych, jest surowo zabronione.

5. Raportowanie Nieprawidłowości: W przypadku wystąpienia jakichkolwiek nieprawidłowości w funkcjonowaniu systemu poczty elektronicznej lub pojawienia się wątpliwości dotyczących bezpieczeństwa używania e-maila, pracownik jest zobowiązany do niezwłocznego zgłoszenia tego faktu działowi IT lub odpowiedniej jednostce w organizacji.

6. Ochrona Danych Osobowych: Wszystkie dane osobowe przesyłane za pośrednictwem poczty elektronicznej muszą być odpowiednio zabezpieczone, najlepiej poprzez wysyłanie ich w załącznikach chronionych hasłem.

USTAWIENIA I ZARZĄDZANIE KONFIGURACJĄ WIADOMOŚCI E-MAIL

1. Inicjalne Ustawienia: Przed rozpoczęciem użytkowania służbowej skrzynki e-mail, informatyk zobowiązany jest do skonfigurowania podstawowych ustawień kont, w tym personalizacji nazwy konta i sygnatury podpisu. Podpis powinien zawierać podstawowe informacje kontaktowe oraz stanowisko zawodowe pracownika oraz klauzule informacyjne.

2. Autoodpowiedź podczas Nieobecności: W przypadku planowanej nieobecności (np. urlopu), pracownik jest zobowiązany do aktywacji funkcji autoodpowiedzi, informującej o czasowej niedostępności oraz wskazującej alternatywny kontakt do osoby zastępującej w tym czasie.
3. Delegowanie Dostępu do Skrzynki: Ustawienie przekierowania otrzymywanych wiadomości na adres e-mail innego pracownika wymaga uzyskania wcześniejszej zgody bezpośredniego przełożonego. Zgoda ta powinna być udokumentowana pisemnie lub za pomocą e-maila.
4. Staranność w Przygotowaniu Wiadomości: Przy tworzeniu i wysyłaniu każdej wiadomości e-mail, należy zachować szczególną staranność w zakresie dokładności treści, prawidłowego doboru załączników oraz precyzyjnego adresowania do odbiorców.
5. Zarządzanie Skrzynką Odbiorczą: Zaleca się regularne przeglądanie i porządkowanie zawartości skrzynki odbiorczej, w tym usuwanie nieaktualnych wiadomości oraz organizowanie pozostałych w odpowiednich folderach w celu ułatwienia zarządzania korespondencją i optymalizacji pracy. Okres retencji danych ustalony jest w Rejestrze Czynności Przetwarzania Danych Osobowych.

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI W KOMUNIKACJI E-MAILOWEJ

1. Zabezpieczanie Danych Osobowych: Wszelkie przesyłane dane osobowe, takie jak imiona, nazwiska czy adresy e-mail, a także inne dane muszą być przekazywane w formie załączników zabezpieczonych hasłem. Takie podejście zapobiega nieautoryzowanemu dostępowi do informacji, nawet w przypadku przechwycenia wiadomości.
2. Zabezpieczanie Plików przez Kompresję: Alternatywną metodą ochrony przesyłanych plików jest ich kompresja do formatu archiwum, które następnie zabezpiecza się silnym hasłem. Taki sposób zabezpieczenia dodatkowo minimalizuje ryzyko dostępu do zawartości przez osoby nieuprawnione.
3. Wymogi dotyczące Haseł: Hasła stosowane do zabezpieczania dokumentów i archiwów powinny być skomplikowane, unikatowe i nieoparte na słownikowych kombinacjach. Zaleca się, aby zawierały one mieszaninę liter, cyfr oraz znaków specjalnych.
4. Komunikacja Haseł: Hasło do zabezpieczonego dokumentu lub archiwum powinno być przekazywane odbiorcy za pomocą alternatywnego kanału komunikacji, np. poprzez rozmowę telefoniczną lub za pomocą innej platformy komunikacyjnej, smsem, co zapobiega jego przechwyceniu.

ZASADY ADRESOWANIA WIADOMOŚCI E-MAIL

1. Cel Komunikacji: Każda wysyłana wiadomość powinna być skierowana do określonego odbiorcy lub odbiorców z konkretnym celem. Należy upewnić się, że treść e-maila jest adekwatna do kontekstu komunikacji z daną osobą.
2. Selekcja Adresatów: W polu "Do/To" powinni znaleźć się wyłącznie ci adresaci, od których oczekuje się bezpośredniego zaangażowania lub odpowiedzi na treść wiadomości. Jest to kluczowe dla zapewnienia skuteczności komunikacji oraz uniknięcia niepotrzebnego przeciążenia informacyjnego.
3. Użycie Pola DW/CC: Dodanie adresata w polu "DW (Do Wiadomości)/CC (Carbon Copy)" oznacza, że otrzymuje on kopię wiadomości w celach informacyjnych. Należy jednak pamiętać, aby używać tego pola z rozwagą, by nie przekazywać informacji osobom, dla których nie jest ona przeznaczona.

4. Ochrona Prywatności Adresatów: Wszelkie wiadomości, które ujawniają adresy e-mail wielu odbiorców, powinny być wysyłane z zachowaniem szczególnej ostrożności. Jeśli adresy e-mail odbiorców są służbowe i istnieje świadomość wspólnego zaangażowania w daną sprawę, dopuszczalne jest ich ujawnienie. W przeciwnym razie zaleca się stosowanie pola BCC/UDW, aby chronić prywatność adresatów.
5. Komunikacja z Nieobecnymi: W przypadku wysyłania wiadomości do osoby nieobecnej lub rzadko sprawdzającej pocztę, zaleca się skierowanie korespondencji również do osoby odpowiedzialnej za dany obszar lub podejmującej decyzje. Dzięki temu minimalizowane jest ryzyko opóźnień lub braku reakcji na ważne wiadomości.
6. Używanie Pola BCC/UDW: Pole "Ukryte Do Wiadomości/BCC (Blind Carbon Copy)" powinno być stosowane w sytuacjach, gdy nie chcemy ujawniać listy wszystkich adresatów lub gdy adresaci nie powinni być świadomi obecności innych odbiorców wiadomości.
7. Masowa Korespondencja: W przypadku planowania wysyłki masowej korespondencji, należy skonsultować się z działem IT w celu wyboru najbardziej odpowiedniego narzędzia lub oprogramowania, które ułatwi zarządzanie taką komunikacją, zapewniając jej efektywność i zgodność z polityką ochrony danych.

ZAKAZANE PRAKTYKI W UŻYTKOWANIU W SŁUŻBOWEJ POCZTY ELEKTORNICZNEJ

W celu zapewnienia profesjonalnej, etycznej i bezpiecznej komunikacji elektronicznej, użytkownikom służbowej poczty elektronicznej wyraźnie zabrania się następujących działań:

8.1 Nieodpowiednia Zawartość i Reprezentacja:

a. Nielegalne i Nieodpowiednie Treści: Zakazane jest tworzenie, wysyłanie lub przechowywanie treści, które mogą być uznane za nielegalne, obraźliwe, dyskryminacyjne lub nieetyczne a także treści o charakterze rasistowskim, seksistowskim, pornograficznym, propagującym terroryzm, oraz wszelkie inne materiały uznawane powszechnie za nieodpowiednie.

b. Nieautoryzowana Reprezentacja: Używanie poczty elektronicznej do reprezentowania pracodawcy bez wyraźnego upoważnienia jest zabronione.

c. Prywatna Korespondencja: Wykorzystywanie służbowej poczty elektronicznej do celów prywatnych, osobistych lub niezwiązanych z działalnością pracodawcy jest niedozwolone.

d. Podszywanie się: Wysyłanie wiadomości e-mail z cudzego konta lub w cudzym imieniu, włączając w to manipulację nagłówkiem "From" / "Od", jest surowo zakazane.

e. Masowa Korespondencja: Ręczne rozsyłanie masowej korespondencji jest niedozwolone. W przypadku konieczności wysłania masowych wiadomości należy skorzystać z narzędzi do mailingu, po uprzedniej konsultacji z działem IT.

f. Działania Niezgodne z Prawem: Wykorzystywanie poczty elektronicznej do jakichkolwiek działań niezgodnych z prawem, nieetycznych lub szkodliwych dla urzędu jest zabronione.

8.2 Nieautoryzowany Dostęp i Manipulacja:

a. Zabrania się przechwytywania, podglądania, zapisywania, modyfikowania lub ujawniania treści wiadomości e-mail należących do innych osób, chyba że jest to niezbędne do zarządzania systemem poczty elektronicznej i odbywa się z odpowiednim upoważnieniem.

8.3 Użycie Zewnętrznych Kont Pocztowych:

a. Używanie prywatnych kont pocztowych do celów służbowych jest zakazane.

8. 4 Przekierowywanie Wiadomości:

a. Zabrania się automatycznego przekierowywania wiadomości e-mail do zewnętrznych systemów pocztowych, aby zapobiec wyciekom informacji.

Procedura ta stanowi kompleksowy zestaw wytycznych mających na celu zapewnienie, że komunikacja e-mailowa w organizacji jest prowadzona w sposób bezpieczny, profesjonalny i zgodny z najlepszymi praktykami ochrony danych. Jej naruszenie traktowane jest jako naruszenie obowiązków pracowniczych i wiązać będzie się z nałożeniem stosownych kar dyscyplinarnych na pracownika.

WÓJT
Stanisław Mannek

WÓJT GMINY KWILCZ
UL. KARDYNAŁA STEFANA WYSZYŃSKIEGO 23
64-420 KWILCZ

Załącznik nr 1
do Procedury Korzystania z Poczty Elektronicznej
w Urzędzie Gminy w Kwilczu

PROCEDURA RETENCJI DANYCH W SYSTEMIE POCZTY ELEKTRONICZNEJ W URZĘDZIE GMINY W KWILCZU

CEL PROCEDURY

Celem niniejszej procedury jest określenie zasad zarządzania czasem przechowywania danych osobowych oraz innych informacji w systemie poczty elektronicznej, w celu zapewnienia zgodności z wymogami prawnymi dotyczącymi ochrony danych osobowych oraz ograniczenia czasu przechowywania do okresu niezbędnego dla celów przetwarzania.

ZAKRES I OBOWIĄZKI

Procedura obejmuje wszystkich użytkowników systemu poczty elektronicznej w organizacji i nakłada na nich obowiązek przestrzegania zasad retencji danych. Każdy użytkownik jest zobowiązany do aktywnego udziału w procesie zarządzania danymi i odpowiedzialny za eliminację danych niepotrzebnych lub przestarzałych zgodnie z ustalonymi okresami retencji.

ZASADY OGÓLNE

Poczta elektroniczna stanowi narzędzie służbowe, przeznaczone wyłącznie do komunikacji służbowej. Zakazuje się wykorzystywania poczty do celów prywatnych.

Użytkownicy zobowiązani są do niezwłocznego usuwania wiadomości e-mail, których okres przechowywania upłynął, zgodnie z określonymi w procedurze okresami retencji.

OKRESY RETENCJI

Okresy retencji są ustalane indywidualnie dla różnych typów korespondencji, w zależności od ich znaczenia i wymogów prawnych, w tym między innymi:

a. Korespondencja związana z udzielaniem odpowiedzi na pytania klientów: przechowywana przez rok od zakończenia korespondecji.
b. Korespondencja z kontrahentami: przechowywana przez rok od zakończenia współpracy.
c. Zapytania ofertowe – rok od momentu otrzymania oferty.
d. CV - rok od momentu otrzymania CV, o ile jest prowadzona rekrutacja lub kandydat wyraził zgodę na przechowywanie CV do kolejnych procesów rekrutacji.
e. Zapytania w trybie dostępu do informacji publicznej – rok od momentu udzielenia odpowiedzi.
f. Żądania związane z przetwarzaniem danych – rok od momentu zakończenia korespondencji.
g. Korespondencja dotycząca postępowań administarycjnych - rok od momentu zakończenia korespondencji
h. Korespondencja wewnętrzna, dotycząca spraw administracyjnych – rok od momentu zakończenia korespondencji.

PRAKTYKI ZARZĄDZANIA DANYCH

Użytkownicy powinni:

a. Regularnie przeglądać swoją skrzynkę pocztową w celu identyfikacji i usuwania wiadomości, których okres przechowywania upłynął.
b. Usuwać kopie robocze, spam, prywatne wiadomości oraz nieistotne powiadomienia niezwłocznie po ich zidentyfikowaniu.

c. Pobierać ważne załączniki na dysk zewnętrzny lub wewnetrzny system zarządzania dokumnetami przed usunięciem wiadomości e-mail.

MONITOROWANIE I KONTROLA

Administrator systemu poczty elektronicznej jest odpowiedzialny za monitorowanie przestrzegania procedury retencji danych przez użytkowników i za wysyłanie okresowych przypomnieć o konieczności przeprowadzania retencji danych.

PRZECHOWYWANIE DANYCH PO ZAKOŃCZENIU WSPÓŁPRACY

Dane z poczty elektronicznej użytkownika są przechowywane przez okres roku po zakończeniu współpracy, pod warunkiem, że były wykorzystywane wyłącznie do celów służbowych.
Aby zapewnić efektywną retencję informacji zawartych w systemie poczty elektronicznej, użytkownik powinien stosować się do następujących praktyk:

1. **Grupowanie Wiadomości:**
Wykorzystywanie funkcji grupowania wiadomości według wątków umożliwia lepszą organizację i łatwiejsze zarządzanie korespondencją.

2. **Oznaczanie Wiadomości dla Retencji:**
Klasyfikowanie wiadomości lub wątków poprzez nadawanie im odpowiednich etykiet lub przenoszenie do dedykowanych folderów, zgodnie z typem korespondencji, ułatwia identyfikację termiów retencji.

3. **Regularny Przegląd Korespondencji:**
Systematyczne, miesięczne przeglądanie korespondencji w celu usunięcia wiadomości, których okres przechowywania wygasł, zgodnie z ustalonymi terminami retencji.

4. **Usuwanie Niepotrzebnych Wiadomości:**
Natychmiastowe usuwanie kopii roboczych, wiadomości uznanych za spam, prywatnych oraz innych nieistotnych komunikatów, jak automatyczne powiadomienia.

5. **Wykorzystanie Automatyzacji:**
Korzystanie z funkcji automatycznego archiwizowania i usuwania wiadomości, zgodnie z ustalonymi okresami retencji, aby usprawnić proces zarządzania danymi.

6. **Zapisywanie Ważnych Załączników:**
Pobieranie istotnych dokumentów załączonych do wiadomości e-mail, takich jak umowy czy wnioski, na dysk. Wiadomości, które nie są już potrzebne, powinny być usuwane po zapisaniu ważnych załączników.

7. **Opróżnianie Kosza:**
Regularne, co najmniej raz w miesiącu, opróżnianie folderu z usuniętymi wiadomościami, aby zwolnić miejsce i utrzymywać porządek w systemie poczty.

Po zakończeniu współpracy dane z poczty e-mail użytkownika są przechowywane przez ustalony okres, wymagający od użytownika korzystania z poczty wyłącznie w celach służbowych i niezwłocznego usuwania korespondencji prywatnej.

W związku z utzrymaniem dyscypliny retencji danych, administrator systemu poczty elektronicznej regularnie wysyła przypomnienia do wszystkich użytkowników o konieczności przeglądu i usuwania przestarzałych danych, zgodnie z obowiązującymi procedurami retencji.

Dane zawarte w systemie poczty elektronicznej użytkownika są utrzymywane przez określony czas po zakończeniu współpracy z organizacją, co zobowiązuje użytkownika do odpowiedzialnego zarządzania swoją skrzynką mailową.

WÓJT
Stanisław Mannek

WÓJT GMINY KWILCZ
UL. KARDYNAŁA STEFANA WYSZYŃSKIEGO 23
64-420 KWILCZ

Załącznik nr 2
do Procedury Korzystania z Poczty Elektronicznej
w Urzędzie Gminy w Kwilczu

Wytyczne bezpiecznego korzystania z poczty mailowej

W sprawach służbowych do korespondencji mailowej używaj wyłącznie służbowego adresu mailowego.
Nie prowadź korespondencji mailowej przy użyciu prywatnego adresu mailowego.
Nie wykorzystuj służbowej poczty mailowej do celów prywatnych.
Przed otwarciem maila sprawdź: czy znasz nadawcę, czy oczekiwałeś wiadomości, czy tytuł i załączniki są sensowne, oraz wynik skanowania antywirusowego. W razie wątpliwości konsultuj się z informatykiem.
Bądź bardzo ostrożny, prowadząc korespondencję mailową, i uważaj na ataki phishingowe oraz fałszywe maile.
Nie otwieraj załączników od nieznanych nadawców lub takich, których nie oczekiwałeś.
Traktuj każdy załącznik jako potencjalnie niebezpieczny. Przed otwarciem zapisz go na dysku i przeskanuj antywirusem.
Zwracaj uwagę na linki w mailach; nie klikaj w podejrzane odnośniki.
Bądź świadomy ryzyka phishingu. Analizuj adresy mailowe i treść wiadomości.
Unikaj spamu; niezamawiane wiadomości najlepiej od razu usuwaj.
Przy przesyłaniu danych osobowych przez maila, upewnij się, że nie przekazujesz ich nadmiernie i że adresaci są odpowiednio określeni.
Przed wysłaniem maila upewnij się, że trafia on do odpowiedniego adresata.
Unikaj korespondencji seryjnej; jeśli musisz jej użyć, upewnij się, że wszyscy adresaci faktycznie mają ją otrzymać i użyj opcji 'ukryte do wiadomości'.
Nie przesyłaj w jednym mailu zaszyfrowanej informacji razem z hasłem. Hasło najlepiej przekazać innym kanałem komunikacji.
Proś o potwierdzenie otrzymania ważnych maili od adresata.
Przestrzegaj zasad logowania i udostępniania danych.
Nie rozsyłaj informacji niezwiązanych z pracą, takich jak zdjęcia, filmiki czy łańcuszki szczęścia.
Ogranicz rozmiar załączników; w przypadku potrzeby przesłania dużych plików skonsultuj się z informatykiem.
Okresowo kasuj zbędne maile zgodnie z zasadami archiwizacji.

WÓJT
Stanisław Mannek