Załącznik nr 1 do Zarządzenia nr 40/2024 Starosty Tureckiego

w sprawie wprowadzenia w Starostwie Powiatowym w Turku

procedur dotyczących bezpieczeństwa udostępnianych danych osobowych

Procedura Korzystania ze Służbowej Poczty Elektronicznej

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 ryzyka 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.

1. 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 firmowego systemu poczty e-mail oraz określa standardy postępowania, mające na celu minimalizację zagrożeń związanych z ochroną i przetwarzaniem danych osobowych i firmowych.

2. 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.

3. Zakres Obowiązujących Zasad

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

1) Ustanowienie jasnych wytycznych dotyczących dozwolonego użytku służbowej poczty elektronicznej.
2) Definiowanie procedur zabezpieczeń, takich jak stosowanie haseł, szyfrowanie wiadomości oraz regularne aktualizacje oprogramowania antywirusowego.
3) Określenie zasad dotyczących archiwizacji korespondencji elektronicznej i zarządzania cyklem życia informacji.
4) Wskazanie odpowiednich działań w przypadku wykrycia podejrzanych lub nieautoryzowanych działań związanych z pocztą elektroniczną.
5) Podkreślenie znaczenia prywatności i poufności w komunikacji elektronicznej, wskazując na odpowiedzialność każdego użytkownika za ochronę przekazywanych danych.

4. 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 jednostki.
2) **Własność Korespondencji:** Wszystkie e-maile generowane, odbierane lub wysyłane przez pracowników są uznawane za własność organizacji. Jednostka zastrzega sobie prawo do dostępu do wszystkich wiadomości e-mail w ramach prowadzonej działalności, zgodnie z obowiązującym prawem.
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 kont pocztowych przypisanych do innych pracowników, jak również udostępnianie swojej skrzynki pocztowej innym, nieupoważnionym osobom, 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 kierownikowi jednostki, administratorom serwerów pocztowych oraz inspektorowi ochrony danych.

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

5. Ustawienia i Zarządzanie Konfiguracją Wiadomości E-mail

1) **Inicjalne Ustawienia:** Przed rozpoczęciem użytkowania służbowej skrzynki e-mail, każdy pracownik zobowiązany jest do skonfigurowania podstawowych ustawień swojego konta, utworzenia profesjonalnego podpisu e-mail, który powinien być zgodny ze standardami przyjętymi w jednostce.
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) **Podpisywanie Wiadomości z Ogólnego Adresu:** W przypadku korzystania przez kilku pracowników z jednego, ogólnego adresu e-mail (np. kontakt@urząd.pl), konieczne jest indywidualne podpisywanie się imieniem i nazwiskiem w treści każdej wysyłanej wiadomości, aby zapewnić jasność komunikacji.
5) **Autoodpowiedź po Zakończeniu Współpracy:** W sytuacji ustania stosunku pracy na koncie e-mailowym pracownika zostanie ustawiona autoodpowiedź informująca o zakończeniu zatrudnienia oraz wskazująca kontakt do osoby, która przejmuje obowiązki.
6) **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. W przypadku wysłania informacji do osoby nieupoważnionej należy bezzwłocznie poinformować o zaistniałej sytuacji Kierownika jednostki i inspektora ochrony danych osobowych.
7) **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. Przetwarzanie danych osobowych na kontach pocztowych musi odbywać się zgodnie z przepisami i instrukcją kancelaryjną. Dane osobowe, których przetwarzanie nie jest uzasadnione wykonywanymi zadaniami lub przepisami archiwizacji należy niezwłocznie usunąć.

6. 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 szyfrowane i

przekazywane w formie załączników zabezpieczonych hasłem. Takie podejście zapobiega nieautoryzowanemu dostępowi do informacji, nawet w przypadku przechwycenia wiadomości.

2) **Zabezpieczanie Plików przez Kompresję:** Powszechną 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. Muszą się składać z co najmniej 8 znaków, 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.
5) **Stałe Hasła dla Zaufanych Odbiorców:** Możliwe jest uzgodnienie stałego hasła dla ciągłej korespondencji z określonym odbiorcą, co ułatwia proces szyfrowania i dekodowania informacji. Jako alternatywę, można użyć informacji znanej tylko wybranemu odbiorcy jako hasła, które nie będzie wymagało oddzielnej komunikacji. Takie hasło należy okresowo zmieniać, nie rzadziej niż raz na miesiąc.

7. 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) **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.

8. Zakazane Praktyki w Użytkowaniu Służbowej Poczty Elektronicznej

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

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 jednostki jest zabronione.
2) **Nieautoryzowany Dostęp i Manipulacja:** Zabrania się przechwytywania, podglądania, zapisywania, modyfikowania lub ujawniania treści wiadomości e-mail należących do innych osób, chyba że jest to uzasadniona konieczność i odbywa się z odpowiednim upoważnieniem.
3) **Użycie Zewnętrznych Kont Pocztowych:** Używanie prywatnych kont pocztowych do celów służbowych jest zakazane.
4) **Przekierowywanie Wiadomości:** Aby zapobiec wyciekom informacji, zabrania się automatycznego przekierowywania wiadomości e-mail do zewnętrznych systemów pocztowych.

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.