Załącznik do Zarządzenia nr 112
Rektora Uniwersytetu Przyrodniczego w Lublinie
z dnia 8 października 2020 r.
w sprawie wprowadzenia Regulaminu
korzystania z poczty elektronicznej

Regulamin korzystania z poczty elektronicznej

1. Przeznaczenie dokumentu 2
2. Zasady korzystania z poczty elektronicznej 2
2.1. Wprowadzenie 2
2.2. Główne zasady 2
2.3. Konfigurowanie wiadomości 3
2.4. Zmiana i odzyskiwanie hasła 3
2.5. Przesyłanie danych osobowych 3
2.6. Adresowanie wiadomości 4
2.7. Działania zakazane 5

1. Przeznaczenie dokumentu.

1.1. Regulamin określa zasady używania służbowej poczty elektronicznej (e-mail). Celem dokumentu jest ustanowienie obowiązujących wymagań w zakresie dozwolonego i poprawnego korzystania z poczty e-mail, a także zminimalizowanie ryzyka dla ochrony danych osobowych przekazywanych drogą elektroniczną. Zasady określone w regulaminie obowiązują wszystkich użytkowników poczty służbowej.

1.2. Regulamin korzystania z poczty elektronicznej obowiązuje każdego pracownika Uniwersytetu Przyrodniczego w Lublinie.

2. Zasady korzystania z poczty elektronicznej.

2.1. Wprowadzenie

Poczta elektroniczna jest obecnie jednym z najważniejszych środków komunikacji. Wiadomości mogą być szybko i pewnie transportowane wewnątrz sieci wewnętrznej oraz globalnie w Internecie. Użycie poczty elektronicznej wiąże się jednak z pewnym ryzykiem. Wiadomości mogą być przechwytywane, zapisywane, odczytywane i przekazywane przez nieuprawnionego odbiorcę. Nieformalne komentarze zawarte w treści wiadomości lub załącznikach mogą być źle zinterpretowane przez odbiorcę i prowadzić do problemów m.in. natury prawnej. Wysyłanie wiadomości do wielu odbiorców w sposób ujawniający ich prywatne adresy e-mail stanowi obecnie jedno z najczęstszych naruszeń ochrony danych osobowych. Zapewnienie właściwego korzystania z poczty elektronicznej stanowi obecnie jeden z priorytetów w zakresie odpowiedniej ochrony danych osobowych.

2.2. Główne zasady.

2.2.1. Korzystanie ze służbowej poczty elektronicznej jest jednym ze sposobów realizowania obowiązków powierzonych użytkownikowi poczty i powinno być realizowane tylko i wyłącznie w celach służbowych, związanych z realizowaniem tych zadań.

2.2.2. Użytkownicy poczty elektronicznej są odpowiedzialni za korzystanie z poczty w taki sposób, aby minimalizować ryzyka naruszenia bezpieczeństwa informacji.

2.2.3. Użytkownik jest uprawniony do korzystania tylko i wyłącznie z przydzielonego lub przydzielonych mu adresów e-mail. Zakazane jest korzystanie z adresu e-mail innego użytkownika, a także logowanie się do skrzynki pocztowej innego użytkownika. Niedopuszczalne jest przekazywanie dostępu do swojej poczty osobom trzecim.

2.2.4. Wszystkie nieprawidłowości w działaniu poczty elektronicznej, a także wątpliwości związane ze sposobem korzystania z poczty elektronicznej, w tym związane z jej bezpieczeństwem, należy niezwłocznie konsultować z pracownikiem Centrum Informatyki.

2.2.5. Dane osobowe przekazywane drogą elektroniczną powinny być przekazywane w załączniku zabezpieczonym hasłem, zgodnie z opisaną w regulaminie procedurą.

2.3. Konfigurowanie wiadomości.

2.3.1. Przed wysłaniem pierwszej wiadomości użytkownik jest zobligowany do skonfigurowania zasad wysyłania wiadomości, w tym nazwy użytkownika i podpisu pod wiadomością zgodnie z obowiązującymi standardami.

2.3.2. W przypadku nieobecności należy ustawić "autoodpowiedź" zawierającą informację o osobie, która zastępuje w czasie nieobecności, do której nadawca może przekazać wiadomość.

2.3.3. Ustawienie przekazywania wiadomości na inny adres e-mail, tzn. innego pracownika, wymaga uprzedniej zgody bezpośredniego przełożonego. Zgoda powinna być udokumentowana (na piśmie lub elektronicznie, jako wiadomość e-mail).

2.3.4. Jeżeli kilku pracowników korzysta z ogólnego adresu e-mail, np. kontakt@, to każda wiadomość powinna zostać podpisana imieniem i nazwiskiem osoby, która udziela odpowiedzi.

2.3.5. Każda wiadomość powinna być wysyłana z zachowaniem należytej staranności w zakresie sprawdzenia poprawności treści, załączników, a także adresatów wiadomości. W korespondencji mailowej należy zachować kulturę informacji i treści.

2.3.6. Zalecane jest okresowe czyszczenie skrzynki pocztowej poprzez usuwanie starych wiadomości, które nie będą już potrzebne oraz przechowywanie wiadomości w strukturze folderów. W pierwszej kolejności powinny być usuwane wiadomości z załącznikami.

2.4. Zmiana i odzyskiwanie hasła.

2.4.1. Użytkownik zobligowany jest do zmiany hasła do swojego konta co 180 dni.

2.4.2. System pocztowy na 21 dni przed upływem terminu wysyła wiadomość przypominającą o zmianie hasła.

2.4.3. W przypadku zapomnienia hasła lub zablokowania konta użytkownik powinien osobiście zwrócić się do Centrum Informatyki celem uzyskania nowego hasła do konta.

2.4.4. Pracownik Centrum Informatyki może zweryfikować tożsamość pracownika na podstawie informacji uzyskanych z Biura Kadr lub po wglądzie do dokumentu potwierdzającego tożsamość.

2.4.5. W przypadku zapomnienia hasła bądź zablokowania konta dopuszcza się możliwość wysłania nowego hasła na adres mailowy podany przez pracownika.

2.4.6. W sytuacji gdy pracownik pracuje wykonuje pracę zdalnie, dopuszcza się możliwość zmiany hasła na wniosek pracownika, wysłany z adresu mailowego sekretariatu jednostki w której jest zatrudniony, w takim przypadku hasło również zostanie wysłane na adres mailowy jednostki.

2.5. Przesyłanie danych osobowych.

2.5.1. Użytkownik może zastosować szyfrowanie wiadomości wewnętrznych w przypadku przesyłania treści objętych szczególną ochroną, z uwzględnieniem wcześniejszej wymiany certyfikatów pomiędzy nadawcą i odbiorcą (np. przez przesłanie

wiadomości podpisanych cyfrowo). Zasady szyfrowania korespondencji zewnętrznej powinny być uzgadniane z poszczególnymi odbiorcami.

2.5.2. Dane osobowe (nawet imiona, nazwiska, czy adresy e-mail) powinny być przekazywane w zabezpieczonym hasłem załączniku do wiadomości e-mail.

2.5.3. Ochrona przesyłanych plików powinna być realizowana w powiązaniu z klasyfikacją informacji poprzez opatrzenie dokumentu hasłem wymaganym do otwarcia i/lub modyfikacji.

2.5.4. Użytkownik może także zabezpieczyć plik lub pliki poprzez kompresję z zabezpieczeniem archiwum wynikowego hasłem.

2.5.5. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.

2.5.6. Hasło powinno zostać przekazane odbiorcy inną drogą korespondencji.

2.5.7. Dopuszczalne jest uzgodnienie stałego hasła na korespondencję z jednym odbiorcą.

2.5.8. Dopuszczalne jest zastosowanie jako hasła informacji, która jest znana tylko odbiorcy, której nie trzeba będzie przekazywać mu odrębną drogą komunikacji, np. znany mu numer ewidencyjny.

2.6. Adresowanie wiadomości.

2.6.1. Przesłanie wiadomości do konkretnej osoby powinno wynikać z celu komunikacji.

2.6.2. Adresatów, których zaangażowanie jest konieczne dla osiągnięcia zamierzonego celu (np. uzyskania odpowiedzi) należy wskazywać w polu Do / To.

2.6.3. Wskazanie adresata w polu DW (Do Wiadomości) / CC (Carbon Copy) powoduje jawne przesłanie do niego kopii wiadomości.

2.6.4. Przekazywanie wiadomości w sposób ujawniający dane adresatów (Do / Do wiadomości) jest dozwolone tylko wówczas, gdy adresy e-mail odbiorców są adresami służbowymi, a adresaci znają wzajemnie swoje adresy e-mail i są zaangażowani w sprawę, której dotyczy wysyłana wiadomość.

2.6.5. W przypadku wysyłania wiadomości do osoby, o której wiadomo, że jest nieobecna lub rzadko odbiera pocztę, zalecane jest przesyłanie korespondencji do wiadomości osoby odpowiedzialnej za dany temat i/lub podejmującej w tym temacie decyzje. Zmniejsza to ryzyko powstania strat lub zagrożeń wynikających z nieterminowego obsługiwania korespondencji przez adresata.

2.6.6. Pole UDW (Ukryte Do Wiadomości) / BCC (Blind Carbon Copy) służy do wysyłania wiadomości z dodatkowym ukryciem przed adresatem faktu istnienia (i tożsamości) trzeciej strony wskazanej w tym polu.

2.6.7. W przypadku wysyłania wiadomości do kilku odbiorców, którzy nie znają się wzajemnie i/lub korzystają z prywatnych adresów e-mail, należy ich adresy wskazać w polu Ukrytej kopii. W takim wypadku wiadomość należy zaadresować do siebie, wskazując swój adres e-mail w polu Do.

2.6.8. Jeżeli niezbędne jest wysłanie masowej korespondencji, należy powiadomić o tym pracownika Centrum Informatyki, w celu zastosowania odpowiedniego programu.

2.7.Działania zakazane.

- Zabrania się używania poczty elektronicznej:
- do tworzenia, wysyłania lub przechowywania wiadomości e-mail lub załączników, które mogą być uznane za nielegalne lub są powszechnie uznawane za obraźliwe, nieetyczne, nielegalne lub w inny sposób niestosowne, w tym: obraźliwe komentarze dotyczące rasy, płci, koloru skóry, niepełnosprawności, wieku, orientacji seksualnej, pornografii, terroryzmu, przekonań i praktyk religijnych, przekonań politycznych, narodowości, odnośniki do lub ewidentnie obraźliwych stron WWW i podobnych materiałów; żarty, wiadomości - łańcuszki, ostrzeżenia o wirusach, prośby o pomoc charytatywną, wirusy i inne oprogramowanie złośliwe;
- do oficjalnego reprezentowania pracodawcy bez odpowiedniego upoważnienia;
- do korespondencji prywatnej lub pracy charytatywnej niepowiązanej z działalnością pracodawcy;
- do wysyłania wiadomości e-mail z cudzego konta lub w cudzym imieniu (włączając w to użycie zmienionego pola From:/Od:);do każdego innego niezgodnego z prawem, nieetycznego celu;
- Zabronione jest uczestniczenie w przechwytywaniu, podglądaniu, zapisywaniu, zmienianiu lub ujawnianiu wiadomości e-mail należącej do innej osoby (nie dotyczy osób odpowiednio upoważnionych lub wtedy, gdy niezbędne jest to do zarządzania systemem poczty elektronicznej).
- Dopuszcza się do korzystania w celach służbowych z innej, w tym prywatnej poczty e-mail.