

ZARZĄDZENIE Nr 11 DYREKTORA GENERALNEGO SŁUŻBY ZAGRANICZNEJ

z dnia 17 maja 2011 r.

w sprawie wdrożenia i eksploatacji systemu poczty elektronicznej w domenę msz.gov.pl

Na podstawie art. 25 ust. 4 pkt 1 i ust. 10 ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. Nr 227, poz. 1505 oraz z 2009 r. Nr 157, poz. 1241 i Nr 219, poz. 1706) zarządza się, co następuje:

Przepisy ogólne**§ 1****1. Zarządzenie określa:**

- 1) zasady korzystania z systemu poczty elektronicznej w domenę msz.gov.pl, zwanego dalej „systemem” funkcjonującego w Ministerstwie Spraw Zagranicznych oraz placówkach zagranicznych;
 - 2) zadania komórek organizacyjnych Ministerstwa Spraw Zagranicznych zwanym dalej MSZ;
 - 3) obowiązki administratora oraz użytkowników systemu.
2. Najważniejsze zasady kulturalnego i efektywnego korzystania ze środków telekomunikacji w środowisku teleinformatycznym służby zagranicznej oraz w Internecie określa netykieta służby zagranicznej zatwierdzana przez dyrektora generalnego służby zagranicznej w odrębnym trybie.

§ 2

Pojęcia używane w zarządzeniu są zgodne z definicjami zawartymi w słowniku obowiązujących pojęć dla potrzeb Księgi Norm Teleinformatycznych i Teletechnicznych, ustalonym w odrębnym trybie.

§ 3

1. W domenę msz.gov.pl wprowadza się do eksploatacji system poczty elektronicznej służący komunikacji służbowej użytkowników.
2. Służbowa komunikacja pocztą elektroniczną z dostępem do Internetu odbywa się wyłącznie przy wykorzystaniu adresów zarejestrowanych w domenę msz.gov.pl., z wyjątkiem komunikacji instytucji polskich.
3. Dyrektor komórki organizacyjnej MSZ właściwej w sprawach teleinformatyki upoważniony jest do wydania i aktualizowania instrukcji określającej:
 - 1) szczegółowe zasady użytkowania służbowej poczty elektronicznej, w tym szczegółowe prawa i obowiązki administratorów i użytkowników systemu;
 - 2) szczegółowe zasady budowy, eksploatacji i zarządzania systemem.
4. Dyrektor komórki organizacyjnej właściwej w sprawach zarządzania informacją w porozumieniu z dyrektorem komórki organizacyjnej właściwej w spra-

wach teleinformatyki jest upoważniony do wydania i aktualizowania instrukcji określającej zasady przydziału kont, tworzenia ich nazw i adresów indywidualnych oraz instytucjonalnych służbowej poczty elektronicznej.

5. Użytkownicy, a także inne osoby wykonujące obowiązki związane z administrowaniem systemem ponoszą odpowiedzialność służbową za przestrzeganie obowiązków określonych w zarządzeniu oraz w instrukcjach, o których mowa w ust. 3 i 4.

System**§ 4**

1. System służy wymianie informacji z wykorzystaniem komunikacji tekstowej i graficznej.
2. Zabrania się przetwarzania w systemie informacji niejawnych oraz stanowiących tajemnice prawnie chronione.
3. Dostęp do systemu zapewnia użytkownikowi:
 - 1) konto w domenę Active Directory;
 - 2) skrzynka pocztowa na serwerze pocztowym;
 - 3) klient pocztowy Microsoft Outlook;
 - 4) terminal BlackBerry.
4. W uzasadnionych przypadkach dyrektor komórki organizacyjnej właściwej w sprawach teleinformatyki może udostępnić użytkownikowi dostęp do systemu poprzez aplikację Outlook Web Access.

Komponenty systemu**§ 5**

W skład systemu wchodzi następujące komponenty zlokalizowane w Centrali MSZ oraz kontynentalnych węzłach systemu:

- 1) kontrolery domeny Active Directory — zbudowane w oparciu o platformę Windows 2008 R2;
- 2) serwery poczty elektronicznej — zbudowane w oparciu o oprogramowanie Microsoft Exchange Server 2010 SP1 systemy pamięci masowych — zbudowane w oparciu o platformę firmy NetApp;
- 3) system kopii bezpieczeństwa i archiwizacji poczty — zbudowany w oparciu o platformę Symantec Enterprise Vault;
- 4) urządzenia sieciowe — routery oraz przełączniki Cisco zlokalizowane w sieci LAN oraz urządzenia dostępowe CheckPoint.

Zadania komórek organizacyjnych

§ 6

1. Dyrektor komórki organizacyjnej właściwej w sprawach teleinformatyki:
 - 1) pełni funkcje organizatora systemu w MSZ i placówkach zagranicznych pełniących rolę regionalnych węzłów teleinformatycznych systemu;
 - 2) wyznacza administratora systemu oraz administratorów systemów wspierających z uwzględnieniem podziału obowiązków dotyczących administrowania poszczególnymi komponentami systemu, pełniących nadzór nad realizacją zadań związanych z funkcjonowaniem systemu;
 - 3) sprawuje nadzór nad wykonywaniem obowiązków administratorów systemu oraz ściśle z nim współpracującego administratora systemu BlackBerry;
 - 4) planuje środki finansowe na funkcjonowanie i rozwój systemu w szczególności środki przeznaczone na zakup niezbędnego sprzętu i licencji oprogramowania;
 - 5) wydaje niezbędne decyzje, wytyczne i instrukcje.
2. Dyrektor komórki organizacyjnej właściwej do spraw finansów zapewnia środki na finansowanie utrzymania i rozwoju systemu.
3. Dyrektor komórki organizacyjnej właściwej do spraw szkolenia organizuje szkolenia dla administratorów i użytkowników systemu.

Obowiązki administratora systemu

§ 7

Administrator systemu jest obowiązany:

- 1) zapewnić nieprzerwaną pracę systemu;
- 2) nadzorować prawidłowe funkcjonowanie komponentów systemu;
- 3) w przypadku wykrycia nieprawidłowości w pracy systemu niezwłocznie przystąpić do działań mających na celu przywrócenie poprawnej pracy systemu;
- 4) utrzymywać niezbędne zasoby systemowe na poziomie wymaganym dla prawidłowej pracy systemu;
- 5) analizować logi systemowe pod kątem nieprawidłowej pracy systemu oraz prób dostępu ze strony osób niepowołanych;
- 6) raportować bezpośrednio przełożonemu wszystkie dostrzeżone nieprawidłowości w pracy systemu;
- 7) chronić przed niepowołanym dostępem i zniszczeniem danych przechowywanych w skrzynkach pocztowych;

- 8) ściśle współpracować z administratorem systemu kopii bezpieczeństwa i archiwizacji poczty elektronicznej, w szczególności w celu określania polityk wykonywania kopii bezpieczeństwa oraz odzyskiwania danych po awarii;
- 9) ściśle współpracować administratorami systemów wspierających oraz administratorami innych systemów teleinformatycznych, w szczególności z administratorem systemu BlackBerry;
- 10) stosować się do zaleceń zawartych w biuletynach dotyczących bezpieczeństwa wydawanych przez producenta systemu pocztowego;
- 11) powiadamiać dyrektora komórki organizacyjnej właściwej w sprawach teleinformatyki w przypadku stwierdzenia prób nieuprawnionego dostępu do systemu, jego nieuprawnionej modyfikacji oraz innych zdarzeniach zagrażających bezpieczeństwu systemu.

Obowiązki administratorów systemów wspierających

§ 8

Administratorzy systemów wspierających obowiązani są do:

- 1) ścisłej współpracy z administratorem systemu;
- 2) przedstawiania do konsultacji i akceptacji wszelkich zmian w konfiguracji serwerów, usług oraz systemów mających wpływ na funkcjonowanie systemu;
- 3) powiadamiania administratora systemu o wystąpieniu zdarzeń zagrażającym bezpieczeństwu systemu lub utracie ciągłości działania;
- 4) instalowania i konfigurowania sprzętu oraz oprogramowania niezbędnego do niezawodnej pracy systemów wspierających;
- 5) aktualizowania platformy sprzętowo-programowej systemów wspierających;
- 6) zapewnienia ciągłości działania systemów wspierających;
- 7) podejmowania czynności w celu wyjaśnienia wszelkich zaobserwowanych nieprawidłowości w działaniu systemu.

Obowiązki Wydziału Technicznego Wsparcia Użytkowników

§ 9

Wydział Technicznego Wsparcia Użytkowników komórki organizacyjnej właściwej w sprawach teleinformatyki odpowiada za:

- 1) instruowanie użytkowników systemu w zakresie eksploatacji i przestrzegania zasad bezpieczeństwa;
- 2) udzielanie pomocy w rozwiązywaniu problemów użytkowników systemu, wynikających z jego codziennej eksploatacji;

- 3) przekazywanie administratorowi systemu wszelkich informacji o stwierdzonych nieprawidłowościach i błędach w funkcjonowaniu systemu;
- 4) przekazywanie zgłoszeń serwisowych wykraczających poza kompetencje Wydziału Technicznego Wsparcia Użytkowników do administratora systemu.

Obowiązki użytkownika systemu

§ 10

Użytkownik jest obowiązany:

- 1) korzystać z systemu wyłącznie w celach służbowych;
- 2) przestrzegać przekazanych mu instrukcji eksploatacji oraz bieżących poleceń administratora systemu;
- 3) przestrzegać zakazu logowania się do systemu poprzez konta systemowe innych użytkowników indywidualnych i instytucjonalnych, wykorzystując ich uprawnienia;
- 4) przestrzegać zakazu tworzenia reguł transportowych automatycznie przekazujących służbową korespondencję pocztową na adresy pocztowe tworzone poza domeną msz.gov.pl.

§ 11

1. Służbowa korespondencja elektroniczna przechowywana w systemie, w tym korespondencja wytworzona przez użytkownika stanowi własność pracodawcy. W celu wykonywania obowiązków służbowych użytkownik jest upoważniony do wytwarzania, wysyłania, przesyłania do dalszych adresatów oraz udostępniania służbowej korespondencji elektronicznej innym użytkownikom.
2. Poza przypadkami określonymi w ust. 3–5 zabroniony jest dostęp do treści służbowej korespondencji znajdującej się na koncie pocztowym użytkownika, przez inne osoby niż użytkownik.
3. Użytkownik jest obowiązany udostępnić wytworzoną przez siebie oraz otrzymaną służbową korespondencję elektroniczną na wezwanie:
 - 1) bezpośredniego przełożonego;
 - 2) pracownika przeprowadzającego, na podstawie odrębnych przepisów, czynności kontrolne;
 - 3) rzecznika dyscypliny finansów publicznych oraz jego zastępcy;
 - 4) przewodniczącego składu orzekającego resortowej komisji orzekającej przy Ministrze Spraw Zagranicznych w sprawach o naruszenie dyscypliny finansów publicznych;
 - 5) rzecznika dyscyplinarnego służby zagranicznej oraz członka personelu dyplomatyczno-konsularnego wyznaczonego w trybie określonym w art. 37 ust. 4 ustawy z dnia 27 lipca 2001 r. o służbie zagranicznej;

- 6) przewodniczącego składu orzekającego komisji dyscyplinarnej Ministerstwa Spraw Zagranicznych;
- 7) innych organów i działających na ich polecenie osób, jeżeli taki obowiązek wynika z przepisów prawa.

4. Osoby wymienione w ust. 3 pkt 1–6 obowiązane są wskazać użytkownikowi powody, dla których żądają udostępnienia służbowej korespondencji elektronicznej.
5. W przypadku, w którym zachodzi pilna potrzeba uzyskania służbowej korespondencji elektronicznej znajdującej się na koncie pocztowym użytkownika, a nie można w tym celu porozumieć się z użytkownikiem, administrator udostępnia jej treść w zakresie określonym we wniosku bezpośredniego przełożonego użytkownika.

Bezpieczeństwo systemu

§ 12

1. Administrator odpowiada za bezpieczeństwo systemu, w tym proponuje reguły bezpieczeństwa oraz wdraża je w systemie po zatwierdzeniu ich przez dyrektora komórki organizacyjnej właściwej do spraw teleinformatyki.
2. Dyrektor komórki organizacyjnej właściwej do spraw teleinformatyki uzgadnia reguły, o których mowa w ust. 1 z dyrektorem komórki organizacyjnej właściwej do spraw kontroli polityki bezpieczeństwa teleinformatycznego, który odpowiada za tworzenie i nadzór nad wdrożeniem polityki bezpieczeństwa teleinformatycznego urzędu.

Szyfrowanie korespondencji

§ 13

1. System poczty elektronicznej wykorzystuje klucze publicznej korporacyjnej infrastruktury PKI (infrastruktury klucza publicznego) zapewniając w uzasadnionych przypadkach, zwłaszcza przy przesyłaniu informacji zawierających dane osobowe, funkcjonalność umożliwiającą szyfrowanie korespondencji w sposób uniemożliwiający dostęp do jej treści innym osobom, niż nadawca i adresat.
2. W przypadku, w którym nadawca uzna, że ze względu na charakter przesyłanych informacji należy zapewnić, aby dostęp do nich był ograniczony wyłącznie do określonych adresatów jest obowiązany stosować mechanizm szyfrowania korespondencji.
3. System poczty elektronicznej zapewnia możliwość odszyfrowania korespondencji, o której mowa w ust. 1 i 2 za pomocą archiwizowanych kluczy prywatnych użytkowników. Przepisy § 11 stosuje się odpowiednio, z tym, że administrator, na pisemny wniosek bezpośredniego przełożonego użytkownika zatwierdzony przez właściwego członka Kierownictwa MSZ udostępnia zaszyfrowane pliki korespondencji w zakresie określonym we wniosku w celu ich odszyfrowania zastępcy dyrektora do spraw bezpieczeństwa komórki organizacyjnej właściwej w sprawach teleinformatyki.

1. System poczty elektronicznej wykorzystuje niekwalifikowany resortowy podpis elektroniczny umożliwiający identyfikację nadawcy w domenie msz.gov.pl.
2. W ramach domeny msz.gov.pl resortowy podpis elektroniczny, o którym mowa w ust. 1, dzięki certyfikatowi wydawanemu przez komórkę właściwą w sprawach teleinformatyki, identyfikuje osobę, która go złożyła równie skutecznie, jak podpis własnoręczny złożony na dokumencie papierowym. W ramach domeny msz.gov.pl, odbiorca wiadomości opatrzonej resortowym podpisem elektronicznym nie jest uprawniony do żądania ponownego przesłania tej wiadomości w formie dokumentu papierowego opatrzonego własnoręcznym podpisem nadawcy.
3. Instrukcja kancelaryjna określi przypadki, w których ze względu na przepisy prawa oraz bezpieczeństwo obrotu gospodarczego przy sporządzaniu korespondencji niezbędne jest zachowanie formy pisemnej i stosowanie podpisu własnoręcznego.
4. Nadawca obowiązany jest podpisać wiadomość resortowym podpisem elektronicznym w następujących przypadkach:
 - 1) jeżeli wiadomość zawiera wiążące rozstrzygnięcie bądź ostateczne stanowisko w określonej sprawie;
 - 2) jeżeli wiadomość wysyłana jest w ramach procedury prawnej, której nadawca jest uczestnikiem, a jej charakter wskazuje na potrzebę jednoznacznej identyfikacji nadawcy;
 - 3) ilekroć zażąda tego odbiorca wiadomości.
5. Poza przypadkami określonymi w ust. 4 nadawca może uznać, że ze względu na charakter przesyłanej wiadomości należy opatrzyć ją resortowym podpisem elektronicznym.

6. Odbiorca wiadomości może bez podania przyczyny zażądać, aby nadawca wiadomości przesłał ją ponownie podpisaną resortowym podpisem elektronicznym. W takim przypadku nadawca jest obowiązany to żądanie spełnić.

Przepisy przejściowe i końcowe

§ 15

1. Dyrektor komórki organizacyjnej właściwej w sprawach teleinformatyki odpowiada za nadzór nad dostosowaniem systemu poczty elektronicznej funkcjonującego w dniu wejścia zarządzenia w życie do zasad określonych w tym zarządzeniu.
2. Dotychczas używane konta poczty elektronicznej z dostępem do Internetu, funkcjonujące poza domeną msz.gov.pl, z wyłączeniem kont wykorzystywanych przez instytucje polskie, mogą być wykorzystywane nie dłużej niż przez 30 dni od dnia wejścia w życie zarządzenia. Komórka organizacyjna właściwa w sprawach teleinformatyki we współpracy z komórką organizacyjną właściwą w sprawach zarządzania informacją zapewni techniczne warunki przeniesienia zawartości dotychczas używanych kont poczty elektronicznej do domeny msz.gov.pl.
3. Dyrektorzy komórek organizacyjnych właściwych w sprawach teleinformatyki i zarządzania informacją wydadzą instrukcje, o których mowa w § 3 w terminie do 30 dni od dnia wejścia zarządzenia w życie.
4. Zarządzenie wchodzi w życie z dniem podpisania, z wyłączeniem § 13 ust. 3, który wchodzi w życie z dniem 1 czerwca 2011 r.

Dyrektor Generalny Służby Zagranicznej

Jarosław Czubiński