ZARZĄDZENIE Nr 12 DYREKTORA GENERALNEGO SŁUŻBY ZAGRANICZNEJ

z dnia 17 maja 2011 r.

w sprawie wdrożenia i eksploatacji systemu poczty elektronicznej w domenie spin.msz

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 domenie spin.msz, 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 domenie spin.msz wprowadza się do eksploatacji system służący komunikacji służbowej użytkowników w ramach sieci spin.msz.

2. Służbowa komunikacja realizowana w ramach systemu, odbywa się wyłącznie przy wykorzystaniu adresów zarejestrowanych w domenie spin.msz.

3. Dyrektor komórki organizacyjnej MSZ właściwej w sprawach teleinformatyki upoważniony jest do wydania i aktualizowania instrukcji określającej:

   1) szczegółowe zasady użytkowania niejawnej służbowej poczty elektronicznej w tym szczegółowe prawa i obowiązki administratorów i użytkowników systemu;

   2) szczegółowe zasady budowy, eksploatacji i zarządzania systemem.

4. Zasady przydziału kont określa dokumentacja bezpieczeństwa teleinformatycznego, właściwa dla systemu.

5. Dyrektor komórki organizacyjnej właściwej w sprawach zarządzania informacją w porozumieniu z dyrektorem komórki organizacyjnej właściwej w sprawach teleinformatyki jest upoważniony do wydania i aktualizowania instrukcji określającej zasady tworzenia systemowych nazw kont, a także adresów indywidualnych oraz instytucjonalnych w domenie spin.msz.

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

System

§ 4

1. System służy wymianie:

   1) informacji niejawnych oznaczonych klauzulą „zastrzeżone";

   2) informacji niejawnych, oznaczonych klauzulami „Restreint UE", „NATO Restricted", „WEU Restricted";

   3) informacji niejawnych innych organizacji międzynarodowych oraz państw, jeśli na podstawie przyjętych przez Rzeczpospolitą Polską zobowiązań wymagają ochrony na poziomie określonym dla klauzuli „zastrzeżone";

   4) informacji jawnych zawierających treści wrażliwe;z wykorzystaniem komunikacji tekstowej i graficznej.

2. Zabrania się przetwarzania w systemie informacji niejawnych o klauzuli wyższej niż klauzula, do której system został akredytowany.

3. Dostęp do domeny spin.msz zapewnia użytkownikowi system teleinformatyczny dopuszczony, w rozumieniu przepisów o ochronie informacji niejawnych do przetwarzania informacji niejawnych o klauzuli „zastrzeżone".

Komponenty systemu

§ 5

W skład systemu wchodzą następujące komponenty zlokalizowane w Centrali MSZ:

1) kontrolery domeny usługi Active Directory — zbudowane na platformie Windows Serwer 2008 R2;

2) serwery poczty elektronicznej — zbudowane na platformie Linux w oparciu o oprogramowanie serwerowe RedHat oraz Qmail;

3) systemy pamięci masowych — zbudowane w oparciu o platformę NetApp;

4) dedykowana infrastruktura PKI — zbudowana w oparciu o oprogramowanie Centaur CCK, serwery usług CA — Windows Serwer 2008 R2, serwery usług bazodanowych MS SQL;

5) system kopii bezpieczeństwa i archiwizacji poczty — zbudowany w oparciu o oprogramowanie Symantec Netbackup, serwer usługi Kryptomail-Arch; serwer PosgreSQL;

6) urządzenia sieciowe — przełączniki, routery oraz urządzenia dostępowe Cisco.

Zadania komórek organizacyjnych

§ 6

1. Dyrektor komórki organizacyjnej właściwej w sprawach teleinformatyki:

   1) pełni funkcje organizatora systemu w MSZ;

   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;

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 bezpośredniemu 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, 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;

10) stosować się do zaleceń i wskazówek w zakresie bezpieczeństwa zawartych w biuletynach wydawanych przez producentów komponentów składowych systemu;

11) powiadamiać, w trybie opisanym we właściwej dokumentacji bezpieczeństwa teleinformatycznego, inspektora bezpieczeństwa teleinformatycznego w Ministerstwie Spraw Zagranicznych w przypadku stwierdzenia prób nieuprawnionego dostępu do systemu, jego nieuprawnionej modyfikacji oraz innych zdarzeniach zagrażających bezpieczeństwu systemu.

§ 8

Obowiązki administratorów systemów wspierających

Administratorzy systemów wspierających obowiązani są do:

1) ścisłej współpracy z administratorem systemu;

2) przedstawiania do konsultacji i akceptacji wszelkich zmian w konfiguracji nadzorowanych serwerów oraz usług teleinformatycznych mających wpływ na funkcjonowanie systemu;

3) powiadamiania administratora systemu oraz w trybie opisanym w właściwej dokumentacji bezpieczeństwa teleinformatycznego powiadamiać inspektora bezpieczeństwa teleinformatycznego w Ministerstwie Spraw Zagranicznych o wystąpieniu zdarzeń wpływających zarówno na bezpieczeństwo jak i utratę ciągłości działania systemu;

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) sprawdzić zawartość przydzielonej mu skrzynki pocztowej niezwłocznie po przystąpieniu do pracy oraz systematycznie w zależności od charakteru wykonywanych przez niego obowiązków.

§ 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 zabroniony jest dostęp do treści służbowej korespondencji znajdującej się na koncie pocztowym użytkownika, przez inne osoby niż użytkownik.

3. Z zastrzeżeniem zasad i procedur określonych w przepisach o ochronie informacji niejawnych użytkownik jest obowiązany udostępnić wytworzoną przez siebie oraz otrzymaną służbową korespondencje elektroniczną na wezwanie:
   1) 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.

Bezpieczeństwo systemu

§ 12

Administrator odpowiada za bezpieczeństwo systemu, w tym wdraża reguły bezpieczeństwa w trybie i na zasadach określonych w dokumentacji bezpieczeństwa teleinformatycznego właściwej dla systemu oraz przepisach o ochronie informacji niejawnych.

Szyfrowanie korespondencji

§ 13

1. System wykorzystuje klucze publicznej korporacyjnej infrastruktury PKI (infrastruktury klucza publicznego) zapewniając automatyczne szyfrowanie całości korespondencji w sposób zapewniający poufność jej treści.

2. System zapewnia możliwość odszyfrowania korespondencji, o której mowa w ust. 1 osobom, o których mowa w § 4 ust. 1 zarządzania Nr 26 Dyrektora Generalnego Służby Zagranicznej z dnia 21 grudnia 2010 r. w sprawie zasad i trybu monitorowania treści przetwarzanych w środowisku teleinformatycznym resortu spraw zagranicznych, zwanych dalej „monitorującymi", z zastrzeżeniem ust. 3.

3. Odszyfrowanie korespondencji możliwe jest pod warunkiem zapewnienia kompletnej rozliczalności wszystkich czynności monitorujących ze szczególnym uwzględnieniem przestrzegania zasady ograniczonego dostępu do informacji niejawnych.

4. 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 pracownikom monitorującym.

Podpisywanie korespondencji resortowym podpisem elektronicznym

§ 14

1. Wszystkie wiadomości generowane w systemie są automatycznie opatrzone resortowym podpisem elektronicznym.

2. W ramach domeny spin.msz 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. Poza domeną spin.msz resortowy podpis elektroniczny, o którym mowa w ust. 1 nie wywołuje takiego skutku, chyba, że wynika to z zawartej umowy, bądź odbiorca wiadomości tak uzgodni z nadawcą.

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. W ramach domeny spin.msz odbiorca wiadomości opatrzonej resortowym podpisem elektronicznym nie jest uprawniony do żądania ponownego przesłania tej wiadomości w formie dokumentu papierowego opatrzonego własnoręcznym podpisem nadawcy.

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. Dyrektor komórki organizacyjnej właściwej w sprawach zarządzania informacją wyda instrukcję, o której mowa w § 3 w terminie do 30 dni od dnia wejścia zarządzenia w życie.
3. 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