DZIENNIK URZĘDOWY
MINISTRA SPRAWIEDLIWOŚCI

Warszawa, dnia 28 czerwca 2012 r.

Poz. 93

ZARZĄDZENIE MINISTRA SPRAWIEDLIWOŚCI

z dnia 27 czerwca 2012 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości i sądów powszechnych

Na podstawie art. 34 ust. 1 i ust. 2 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2012 r. poz. 392) w związku z art. 9 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. Nr 98, poz. 1070, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. W Ministerstwie Sprawiedliwości i sądach powszechnych wprowadza się Politykę Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości i sądów powszechnych, stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Ministerstwo Sprawiedliwości i sądy powszechne wdrożą Politykę Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości i sądów powszechnych w terminie 6 miesięcy od dnia wejścia w życie niniejszego zarządzenia.

§ 3. Realizację zadań określonych w Polityce Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości i sądów powszechnych nadzoruje podsekretarz stanu odpowiedzialny za informatyzację.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Minister Sprawiedliwości: *Jarosław Gowin*

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 154, poz. 1787, z 2002 r. Nr 153, poz. 1271, Nr 213, poz. 1802 i Nr 240, poz. 2052, z 2003 r. Nr 188, poz. 1838 i Nr 228, poz. 2256, z 2004 r. Nr 34, poz. 304, Nr 130, poz. 1376, Nr 185, poz. 1907 i Nr 273, poz. 2702 i 2703, z 2005 r. Nr 13, poz. 98, Nr 131, poz. 1102, Nr 167, poz. 1398, Nr 169, poz. 1410, 1413 i 1417, Nr 178, poz. 1479 i Nr 249, poz. 2104, z 2006 r. Nr 144, poz. 1044 i Nr 218, poz. 1592, z 2007 r. Nr 25, poz. 162, Nr 64, poz. 433, Nr 73, poz. 484, Nr 99, poz. 664, Nr 112, poz. 766, Nr 136, poz. 959, Nr 138, poz. 976, Nr 204, poz. 1482 i Nr 230, poz. 1698, z 2008 r. Nr 41, poz. 251, Nr 223, poz. 1457, Nr 228, poz. 1507 i Nr 234, poz. 1571, z 2009 r. Nr 1, poz. 4, Nr 9, poz. 57, Nr 26, poz. 156 i 157, Nr 56, poz. 459, Nr 157, poz. 1241, Nr 178, poz. 1375, Nr 219, poz. 1706 i Nr 223, poz. 1777, z 2010 r. Nr 182, poz. 1228 i Nr 205, poz. 1364 oraz z 2011 r. Nr 109, poz. 627, Nr 126, poz. 714 i Nr 203, poz. 1192.

Załącznik do zarządzenia Ministra
Sprawiedliwości z dnia 27 czerwca 2012 r.
(poz. 93)

Polityka Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości i sądów powszechnych*

Spis treści

* Dokument powstał w ramach projektu współfinansowanego przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

1. Wstęp

Bezpieczeństwo informacji oraz systemów, w których są one przetwarzane jest jednym z kluczowych elementów zapewniających realizacje zadań statutowych Ministerstwa Sprawiedliwości i sądów powszechnych (MS i SP).

W celu zapewnienia bezpieczeństwa informacji Ministerstwo Sprawiedliwości i sądy powszechne wprowadzają spójny system zarządzania bezpieczeństwem informacji.

Polityka Bezpieczeństwa Informacji jest zestawem powiązanych ze sobą dokumentów (polityk, regulaminów, instrukcji, standardów, szablonów umów) określających zasady i sposób zarządzania bezpieczeństwem aktywów informacyjnych i zasobów materialnych Ministerstwa Sprawiedliwości i sądów powszechnych. Zarządzanie to służy ochronie oraz udostępnianiu aktywów w taki sposób, aby utrzymać poufność, dostępność oraz integralność przetwarzanych informacji na odpowiednim poziomie.

2. Cel polityki bezpieczeństwa informacji

Celem Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości i sądów powszechnych jest:

1. Zapewnienie właściwej ochrony zasobów informacyjnych.
2. Stworzenie podstaw do wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji.

3. Zakres obowiązywania polityki bezpieczeństwa informacji

Polityka Bezpieczeństwa Informacji jest zbiorem zasad, które obowiązane są stosować osoby posiadające dostęp do zasobów informacyjnych. Określa również zasady ochrony infrastruktury, zasobów informatycznych i ludzkich.

Niniejszy dokument dotyczy wszystkich pracowników w rozumieniu w szczególności ustawy o służbie cywilnej oraz przepisów Kodeksu Pracy, a także innych osób mających dostęp do informacji chronionych (np. pracowników firm zewnętrznych realizujących prace) Ministerstwa Sprawiedliwości i sądów powszechnych.

Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej).

4. Wprowadzenie systemu zarządzania bezpieczeństwem w Ministerstwie Sprawiedliwości i sądach powszechnych

Ministerstwo Sprawiedliwości i sądy powszechne powinny ustanowić, wdrożyć, eksploatować, monitorować, przeglądać, utrzymywać i doskonalić System Zarządzania Bezpieczeństwem Informacji (SZBI).

Wprowadzenie Systemu Zarządzania Bezpieczeństwem Informacji powinno być decyzją strategiczną kierownictwa umocowaną w akcie prawa wewnętrznego. Na projektowanie i wdrażanie Systemu Zarządzania Bezpieczeństwem Informacji powinny mieć wpływ potrzeby i cele działania jednostki organizacyjnej, wymagania bezpieczeństwa, realizowane procesy oraz wielkość i struktura jednostki organizacyjnej.

W Ministerstwie Sprawiedliwości za ustanowienie wdrożenie, eksploatowanie, monitorowanie, przeglądanie, utrzymywanie i doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji odpowiada Minister Sprawiedliwości, natomiast w sądach powszechnych prezesi tych sądów.

Zadaniem Ministra Sprawiedliwości i prezesów sądów jest zapewnienie warunków niezbędnych do ustanowienia wdrożenia, eksploatowania, monitorowania, przeglądania, utrzymywania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.

Polityka Bezpieczeństwa Informacji jest jednym z elementów Systemu Zarządzania Bezpieczeństwem Informacji.

5. Organizacja Systemu Zarządzania Bezpieczeństwem Informacji

Przy wprowadzeniu Systemu Zarządzania Bezpieczeństwem Informacji powinno uwzględniać się postanowienia Polskich Norm z zakresu bezpieczeństwa informacji takich jak PN-ISO/IEC 27001:2007 i PN-ISO/IEC 27005:2010.

6. Utrzymanie odpowiedniego poziomu bezpieczeństwa informacji

Wprowadzony System Zarządzania Bezpieczeństwem Informacji powinien uwzględniać procesy utrzymania odpowiedniego poziomu bezpieczeństwa w tym:

1. Zarządzanie ryzykiem.
2. Zarządzania dostępem do zasobów.
3. Monitorowania poziomu bezpieczeństwa.
4. Zarządzania incydentem.
5. Nadzoru nad dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji.

Nakłady ponoszone na zabezpieczenia powinny być poprzedzone analizą ryzyka i kosztów, adekwatnie do potencjalnych strat spowodowanych naruszeniem bezpieczeństwa.

Dla utrzymania odpowiedniego poziomu bezpieczeństwa informacji istotne jest systematyczne szkolenie oraz podnoszenie kwalifikacji zawodowych pracowników.

7. Struktura dokumentacji Polityki Bezpieczeństwa Informacji

Dokumentacja **Polityk Bezpieczeństwa Informacji** ma strukturę hierarchiczną. Poszczególne poziomy dokumentacji opisują system zarządzania bezpieczeństwem informacji na różnych poziomach szczegółowości.

Dokumentacja Polityk Bezpieczeństwa Informacji składa się z następujących poziomów:

1. Poziom Ministerstwa Sprawiedliwości i sądów powszechnych.
2. Poziom jednostki organizacyjnej.
3. Poziom systemu teleinformatycznego.

4. Poziom systemu informatycznego.
5. Poziom procedur, instrukcji i regulaminów.

Niniejszy dokument główny ***Polityki Bezpieczeństwa Informacji*** Ministerstwa Sprawiedliwości i sądów powszechnych, określa podstawowe założenia Polityki Bezpieczeństwa Informacji obowiązujące w Ministerstwie Sprawiedliwości i sądach powszechnych.

Na poziomie jednostki organizacyjnej – Ministerstwo Sprawiedliwości i sądy powszechne opracowują i wdrażają następujące dokumenty Polityki Bezpieczeństwa Informacji:

1. **P*olitykę Bezpieczeństwa Informacji jednostki organizacyjnej***, która określa zasady bezpieczeństwa informacji obowiązujące w danej jednostce organizacyjnej wynikające z aktów prawnych oraz z realizowanych zadań statutowych jednostki.
2. ***Politykę Bezpieczeństwa Systemów Teleinformatycznych jednostki organizacyjnej***, która określa zasady bezpieczeństwa dla systemów teleinformatycznych obowiązujące w danej jednostce organizacyjnej wynikające z aktów prawnych oraz z realizowanych zadań statutowych jednostki.
3. ***Polityki Bezpieczeństwa dla poszczególnych systemów teleinformatycznych***, która opisuje w jaki sposób zasady bezpieczeństwa zawarte w ***Polityce Bezpieczeństwa Informacji jednostki organizacyjnej i Polityce Bezpieczeństwa Systemów Teleinformatycznych jednostki organizacyjnej*** są realizowane dla danych systemów teleinformatycznych.
4. ***Procedury, standardy, instrukcje, regulaminy*** oraz inne dokumenty, które regulują szczegółowe zasady korzystania z zasobów informacyjnych jednostek organizacyjnych, a także użytkowania systemów informatycznych.

Opracowane w jednostkach organizacyjnych dokumenty muszą być zgodne z aktami prawnymi wymienionymi w rozdziale 14 niniejszego dokumentu oraz innymi przepisami szczegółowo definiującymi i wprowadzającymi ochronę informacji.

8. Odpowiedzialność za ochronę informacji

W Ministerstwie Sprawiedliwości za bezpieczeństwo informacji odpowiada Minister Sprawiedliwości, natomiast w sądach prezesi tych sądów.

Wszyscy pracownicy są obowiązani, odpowiednio do swoich obowiązków służbowych i zajmowanych stanowisk, do ochrony informacji i przestrzegania **Polityki Bezpieczeństwa Informacji**, a zwłaszcza zasad zawartych w procedurach, regulaminach oraz innych dokumentach Polityki Bezpieczeństwa Informacji. Pracownicy w szczególności obowiązani są do przestrzegania procedur opisujących zasady korzystania z haseł, procedur ochrony antywirusowej oraz procedur eksploatacji systemów informatycznych. **Wszyscy pracownicy** są obowiązani do przestrzegania zasad ochrony informacji prawnie chronionej.

Kierownictwo każdej jednostki organizacyjnej powinno wyznaczyć role i odpowiedzialności w obszarze zarządzania bezpieczeństwem informacji, w tym role i odpowiedzialności dla reagowania w przypadkach naruszenia bezpieczeństwa informacji.

9. Podstawowe zasady bezpieczeństwa informacji

Poniższe uniwersalne zasady są podstawą dla skutecznego zarządzania bezpieczeństwem informacji i powinny być brane pod uwagę przy wprowadzaniu Systemu Zarządzania Bezpieczeństwem Informacji w Ministerstwie Sprawiedliwości i sądach powszechnych:

1. **Zasada uprawnionego dostępu.** Każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufności.
2. **Zasada przywilejów koniecznych.** Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
3. **Zasada wiedzy koniecznej.** Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
4. **Zasada usług koniecznych.** Udostępniane powinny być tylko takie usługi jakie są konieczne do realizacji zadań statutowych.
5. **Zasada asekuracji.** Każdy mechanizm zabezpieczający musi być ubezpieczony drugim, innym (podobnym). W przypadkach szczególnych może być stosowane dodatkowe (trzecie) niezależne zabezpieczenie.
6. **Zasada świadomości zbiorowej.** Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie.
7. **Zasada indywidualnej odpowiedzialności.** Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
8. **Zasada obecności koniecznej.** Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
9. **Zasada stałej gotowości.** System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
10. **Zasada najsłabszego ogniwa.** Poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element.
11. **Zasada kompletności.** Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
12. **Zasada ewolucji.** Każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
13. **Zasada odpowiedniości.** Używane środki techniczne i organizacyjne muszą być adekwatne do sytuacji.
14. **Zasada świadomej konwersacji.** Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.
15. **Zasada segregacji zadań.** Zadania i uprawnienia powinny być tak podzielone, aby jedna osoba nie mogła zdobyć pełni władzy nad całym systemem.

10. Dobór zabezpieczeń

Ministerstwo Sprawiedliwości i sądy powszechne powinny dobierać cele stosowania zabezpieczeń i zabezpieczenia adekwatne do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa informacji.

Zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie zapewniając wspólnie wymagany poziom bezpieczeństwa informacji. W doborze celów stosowania zabezpieczeń i zabezpieczeń należy kierować się zaleceniami Polskiej Normy PN-ISO/IEC 17799.

11. Sankcje za naruszenie zasad bezpieczeństwa informacji

Nieprzestrzeganie zasad zawartych w dokumentach polityki bezpieczeństwa, jest naruszeniem obowiązków pracowniczych wynikających w szczególności z ustaw o służbie cywilnej, o pracownikach urzędów państwowych, pracownikach sądów i prokuratury oraz Kodeksu Pracy i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie sprawcy do odpowiedzialności wynikającej z przepisów prawa i Regulaminu Pracy.

12. Zasady rozpowszechniania dokumentu oraz tryb wprowadzania zmian

Z ***Polityką Bezpieczeństwa Informacji*** Ministerstwa Sprawiedliwości i sądów powszechnych i dokumentami związanymi powinna się zapoznać kadra kierownicza oraz wszyscy pracownicy.

Niniejszy dokument może być udostępniony uprawnionym podmiotom zewnętrznym w celu zapoznania się i postępowania w zgodzie z postanowieniami niniejszego dokumentu.

13. Słownik pojęć

Dokument – dokumentem jest każdy przedmiot (np. pismo, plik tekstowy itp.), który ze względu na zawartą w nim treść, może stanowić wartość dla pracodawcy,

Dostępność – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu (na podstawie PN-ISO/IEC 27001),

Incydent – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji (na podstawie PN-ISO/IEC 17799),

Informacja – to taki czynnik, któremu można przypisać określone znaczenie, aby móc go wykorzystywać do różnych celów,

Integralność – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów (na podstawie PN-ISO/IEC 27001),

Jednostka organizacyjna – Ministerstwo Sprawiedliwości, Sąd Apelacyjny, Sąd Okręgowy, Sąd Rejonowy,

Komórka organizacyjna – Departament, Biuro, Wydział, Oddział, Wieloosobowe stanowisko, wydzielone stanowisko,

PBI – Polityka Bezpieczeństwa Informacji,

PBST – Polityka Bezpieczeństwa Systemów Teleinformatycznych,

Poufność – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom (na podstawie PN-ISO/IEC 27001),

Pracodawca – jednostka organizacyjna dla której użytkownik świadczy pracę bez względu na jakiej podstawie (umowa o pracę, umowa zlecenia, staż, praktyki, itp.),

Pracownik – osoba, która świadczy pracę na rzecz Pracodawcy bez względu na jakiej podstawie (umowa o pracę, umowa zlecenia, staż, praktyki, itp.),

Ryzyko – kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji (na podstawie PN-ISO/IEC,

SZBI – System Zarządzania Bezpieczeństwem Informacji,

Użytkownik – osoba która posiada konto w systemie Pracodawcy,

14. Przepisy prawne i polskie normy

W Ministerstwie Sprawiedliwości i sądach powszechnych informacje podlegają ochronie zgodnie z następującymi wymogami prawa:

1. Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. Nr 16, poz. 93, z późn. zm.).
2. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.).
3. Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94, z późn. zm.).
4. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.).
5. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228, z późn. zm.,).
6. Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503, z późn. zm.).
7. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2005 r. Nr 145, poz. 1221, z późn. zm.).
8. Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2009 r. Nr 152, poz. 1223, z późn. zm.).
9. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r. Nr 90, poz. 631, z późn. zm.).
10. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198, z późn. zm.).
11. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.).
12. Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub podlegających na dostępie warunkowym (Dz. U. Nr 126, poz. 1068, z późn. zm.).
13. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.).
14. Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665, z późn. zm.).
15. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. Nr 128, poz. 1402, z późn. zm.).
16. Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2008 r., nr 50 poz. 292).
17. Ustawa z dnia 6 lipca 1982 r. o Księgach Wieczystych i hipotece (Dz. U. z 2001, Nr 124, poz. 1361).
18. Rozporządzenie Ministra Finansów z dnia 1 lutego 2010 r. w sprawie przeprowadzania i dokumentowania audytu wewnętrznego (Dz. U. Nr 21, poz. 108).

19. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
20. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie określenia podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. Nr 159, poz. 948).
21. Rozporządzenie Rady Ministrów z dnia z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r., poz. 526).
22. Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz. U. Nr 148, poz. 973, z późn. zm.).

Podstawą normalizacyjną dokumentu Polityki Bezpieczeństwa Informacji są niżej wymienione polskie normy:

1. PN ISO/IEC 27001:2007 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.
2. PN ISO/IEC 27005 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.
3. PN-ISO/IEC 17799:2007 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.
4. PN-I-13335-1:1999 Technika Informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych.
5. PN ISO/IEC 20000-1:2007 Technika Informatyczna – Zarządzanie usługami część 1: Specyfikacja.
6. PN ISO/IEC 20000-2:2007 Technika Informatyczna – Zarządzanie usługami część 2: Reguły postępowania.