ZARZĄDZENIE NR 33/08

Rektora-Komendanta Szkoły Głównej Służby Pożarniczej

z dnia 9 lipca 2008 r.

w sprawie ustalenia Polityki Bezpieczeństwa Informacji w SGSP

Na podstawie § 16 Regulaminu organizacyjnego SGSP, stanowiącego załącznik do zarządzenia nr 1/08 Rektora-Komendanta SGSP z dnia 14 stycznia 2008 r., zarządza się co następuje:

§ 1

Wprowadza się Politykę Bezpieczeństwa Informacji w SGSP, stanowiącą załącznik do zarządzenia.

§ 2

Zobowiązuje się kierowników komórek organizacyjnych SGSP do zapoznania strażaków i pracowników z Polityką Bezpieczeństwa Informacji w SGSP.

§ 3

Traci moc zarządzenie nr 34/07 Rektora-Komendanta SGSP z dnia 26 czerwca 2007r.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik
do zarządzenia nr 33/08
Rektora-Komendanta SGSP
z dnia 9 lipca 2008 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Cel wprowadzenia Polityki Bezpieczeństwa Informacji

1. Polityka Bezpieczeństwa Informacji stanowi zapewnienie, że Rektor-Komendant SGSP wspiera i kieruje bezpieczeństwem informacji zgodnie z wymaganiami właściwych przepisów prawa oraz regulacji wewnętrznych.

Znaczenie bezpieczeństwa informacji dla SGSP

2. Informacja oraz wspierające ją procesy i systemy są ważnymi aktywami SGSP.
3. SGSP i jej systemy informacyjne są narażone na zagrożenia bezpieczeństwa z wielu różnych źródeł, łącznie z przestępstwami z użyciem komputera, szpiegostwem, sabotażem, wandalizmem, pożarem czy powodzią.
4. Ochrona informacji przed szerokim spektrum zagrożeń ma zapewnić ciągłość działania SGSP.

Zakres stosowania dokumentu Polityki Bezpieczeństwa Informacji

5. Polityka Bezpieczeństwa Informacji ma zastosowanie w stosunku do wszystkich postaci informacji: dokumentów papierowych, zapisów elektronicznych i innych, będących własnością SGSP lub administrowanych przez SGSP i przetwarzanych w systemach informatycznych, tradycyjnych (papierowych) i komunikacyjnych SGSP.
6. Polityka Bezpieczeństwa Informacji, w zakresie bezpieczeństwa informacji w SGSP, jest aktem nadrzędnym w stosunku do wszystkich innych obowiązujących w SGSP regulacji.
7. Polityka Bezpieczeństwa Informacji ma zastosowanie w stosunku do wszystkich pracowników SGSP (za pracownika SGSP, w rozumieniu niniejszego dokumentu, uważa się także strażaka pełniącego służbę w SGSP), innych osób zatrudnionych w SGSP, jak również osób trzecich mających dostęp do informacji w SGSP.
8. Ochrona informacji wynikająca z Polityki Bezpieczeństwa Informacji jest realizowana na każdym etapie przetwarzania informacji.

Realizacja Polityki Bezpieczeństwa Informacji

9. Bezpieczeństwo informacji będzie osiągane poprzez wdrażanie odpowiednich zabezpieczeń, o których mowa w ust. 21.
10. Zabezpieczenia będą ustanawiane, wdrażane, monitorowane, przeglądane, a w razie potrzeby zmieniane tak, aby spełnić poszczególne cele związane z bezpieczeństwem oraz prowadzoną działalnością statutową SGSP.
11. Działania będą powiązane z pozostałymi procesami zarządzania funkcjonującymi w SGSP.

Oświadczenie Rektora-Komendanta

12. Ochrona i bezpieczeństwo aktywów informacyjnych jest ważnym obszarem zarządzania SGSP.
13. Rektor-Komendant SGSP przywiązuje dużą wagę do kwestii związanych z bezpieczeństwem informacji oraz do wdrażania odpowiednich programów i mechanizmów jej ochrony.
14. Dokumenty Polityki Bezpieczeństwa Informacji stanowią kluczowy element strategii bezpieczeństwa SGSP.
15. Rektor-Komendant SGSP dąży do zredukowania ryzyka związanego z bezpieczeństwem aktywów informacyjnych do akceptowanego poziomu zachowując równowagę pomiędzy ryzykiem utraty bezpieczeństwa aktywów informacyjnych, a środkami przeznaczanymi na ich zabezpieczenia.
16. Każdy pracownik SGSP jest zobowiązany zapoznać się z dokumentami Polityki Bezpieczeństwa Informacji, w zakresie go dotyczącym i przestrzegać postanowień zawartych w tych dokumentach i innych aktach z niego wynikających.
17. Do organizacji zasad ochrony informacji Rektor-Komendant wyznaczył Administratora Bezpieczeństwa Informacji (ABI).
18. Rektor-Komendant zobowiązuje ABI do merytorycznego przeglądu dokumentów Polityki Bezpieczeństwa Informacji oraz zabezpieczeń z niej wynikających nie rzadziej niż raz w roku oraz wykonania aktualizacji wynikającej z przeglądu.

Zgodność z prawem, regulacjami wewnętrznymi i innymi wymaganiami.

19. Punktem wyjścia do wdrożenia bezpieczeństwa informacji są zabezpieczenia wynikające z podstawowych wymogów prawa oraz praktyka uznana za powszechną w bezpieczeństwie informacji.

20. Najważniejszymi zabezpieczeniami dla SGSP z prawnego punktu widzenia są:
    1) ochrona i poufność danych osobowych wynikające z ustawy o ochronie danych osobowych
    2) ochrona zapisów SGSP wynikających z ustawy o rachunkowości, innych przepisów prawa i regulacji wewnętrznych,
    3) ochrona prawa do własności intelektualnej wynikająca z ustawy o prawie autorskim i prawach pokrewnych.
    4) ochrona informacji niejawnych zgodnie z ustawą o ochronie informacji niejawnych
21. Zabezpieczeniami uznawanymi za powszechną praktykę w zakresie bezpieczeństwa informacji będzie:
    1) zbiór dokumentów Polityki Bezpieczeństwa Informacji, w szczególności: Polityka Bezpieczeństwa Danych Osobowych, Polityka Rachunkowości, Instrukcje Bezpieczeństwa Systemów Przetwarzania,
    2) przypisanie odpowiedzialności w zakresie bezpieczeństwa informacji,
    3) uświadamianie, kształcenie i szkolenie z zakresu bezpieczeństwa informacji,
    4) poprawne przetwarzanie w aplikacjach,
    5) zarządzanie podatnościami technicznymi,
    6) zarządzanie ciągłością działania,
    7) reagowanie na incydenty związane z bezpieczeństwem informacji oraz minimalizacja ich skutków.

Zarządzanie ryzykiem utraty bezpieczeństwa aktywów informacyjnych SGSP

22. Celem określenia i wdrożenia wymagań bezpieczeństwa aktywów informacyjnych w SGSP wprowadza się okresowy powtarzalny proces szacowania ryzyka utraty bezpieczeństwa uwzględniający wszelkie zmiany mające wpływ na jego wynik.
23. SGSP przyjmuje zasadę akceptowalnej równowagi, tj. nakłady na zabezpieczenia będą odpowiadać potencjalnym stratom, wynikającym z naruszenia bezpieczeństwa informacji.
24. Inicjatorem i koordynatorem procesu szacowania ryzyka jest ABI, z którym współpracują Właściciele Zbiorów Informacji.
25. Wyniki szacowania ryzyka będą wskazywać i określać adekwatne działanie zarządcze, priorytety dla zarządzania ryzykiem bezpieczeństwa informacji oraz wdrożenie wybranych mechanizmów zabezpieczających.

Wykaz aktywów i systemów przetwarzania informacji w SGSP

26. Podział informacji przetwarzanej w SGSP przedstawia załącznik nr 1.
27. Wykaz zbiorów informacji chronionej zawiera załącznik nr 2.

28. Informacje uznane za chronione podlegają ochronie przed nieautoryzowanym: dostępem, powielaniem, ujawnieniem, modyfikacją, wykorzystaniem, zniszczeniem, jak również utratą, kradzieżą oraz zatajeniem.
29. Informacje jawne podlegają ochronie przed modyfikacją i utratą (zniszczeniem).
30. Wykaz zidentyfikowanych w SGSP systemów przetwarzania zbiorów danych przedstawia załącznik nr 3.
31. Zależności pomiędzy zbiorami danych, a systemami przetwarzania przedstawia załącznik nr 4.
32. Załączniki nr 2-4, o których mowa w ust. 27, 30 i 31 są dostępne stosując zasadę wiedzy koniecznej tylko dla osób upoważnionych. Wzór wykazu osób upoważnionych stanowi załącznik nr 5.
33. Dla informacji uznanej, jako chroniona oraz systemów przetwarzania zostaną opracowane polityki i instrukcje bezpieczeństwa oraz wynikające z nich regulaminy i procedury.

Zastosowanie zasad bezpieczeństwa informacji

34. Zasady zarządzania bezpieczeństwem informacji określone w dokumentach Polityki Bezpieczeństwa Informacji mają zastosowanie w stosunku do:
    1) wszystkich pracowników, innych osób zatrudnionych, konsultantów, stażystów i innych osób mających dostęp do informacji podlegającej ochronie,
    2) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są i lub będą informacje podlegające ochronie,
    3) wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się informacje podlegające ochronie,
    4) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

Dostęp do informacji chronionych

35. Każdy, kto ma uzyska
36. dostęp do informacji chronionej SGSP, wynikający z zasady wiedzy koniecznej jest zobowiązany do:
    1) zapoznania się z przepisami wewnętrznymi SGSP dotyczącymi zasad ochrony informacji,
    2) uczestniczenia w szkoleniu dotyczącym zasad ochrony informacji w SGSP i z zasad korzystania z systemów informatycznych,
    3) podpisania oświadczenia dotyczącego ochrony informacji w SGSP,
    4) uzyskania upoważnienia do przetwarzania.

37. Zakres nadanych uprawnień uzależniony jest od zakresu zadań realizowanych na danym stanowisku (lub wynika z realizacji umowy).
38. Wykaz osób upoważnionych do przetwarzania informacji chronionych prowadzi ABI wg wewnętrznych procedur.

Wymagania dotyczące kształcenia, szkoleń i uświadamiania
w dziedzinie bezpieczeństwa informacji

39. Wszyscy pracownicy SGSP, inne osoby zatrudnione w SGSP oraz, gdzie to jest wskazane, wykonawcy i użytkownicy reprezentujący stronę trzecią, będą odpowiednio przeszkoleni oraz regularnie informowani o uaktualnieniach obowiązujących w SGSP polityk
i procedur które są związane z realizowanymi zadaniami.
40. Szkolenia będą przeprowadzane przed przyznaniem dostępu do informacji lub usług i rozpoczynać się będą od formalnego procesu zapoznania się z polityką oraz wymaganiami bezpieczeństwa SGSP.
41. Uświadamianie, kształcenie i szkolenie będzie dostosowane do zakresu realizowanych zadań i umiejętności osoby oraz będzie zawierało informacje na temat znanych zagrożeń, procedur postępowania przy przetwarzaniu informacji oraz w przypadku zaistnienia incydentu związanego z bezpieczeństwem informacji.

Zarządzanie ciągłością

42. Celem przeciwdziałania przerwom w działalności statutowej SGSP oraz ochronie krytycznych procesów przed rozległymi awariami systemów informatycznych lub katastrofami, oraz celem zapewnienia wznowienia działalności w wymaganym czasie w SGSP, zostanie opracowany i wdrożony proces zarządzania ciągłością działania.
43. Za organizację i utrzymanie procesu zapewnienia ciągłości działania odpowiedzialny będzie ABI.
44. Zadania w tym zakresie ABI będzie realizował we współpracy z kierownictwem SGSP.

Konsekwencje naruszenia Polityki Bezpieczeństwa Informacji

45. Osoby naruszające zasady Polityki Bezpieczeństwa Informacji zostaną pociągnięte do odpowiedzialności służbowej (porządkowej, dyscyplinarnej) i karnej.

Załącznik nr 1
do Polityki Bezpieczeństwa Informacji w SGSP

Podział informacji przetwarzanych w SGSP

Informacja jawna	Informacja chroniona
1. Informacja jawna wymagana przepisami prawa. *(Ustawa o dostępie do informacji publicznej, Ustawa o rachunkowości)* 2. Informacja jawna związana z działalnością SGSP 3. Informacja reklamowa i marketingowa.	1. Dane osobowe (*Ustawa o ochronie danych osobowych*) 2. Informacja niejawna (*Ustawa o ochronie informacji niejawnej*) 3. Zapisy SGSP (*Ustawa o rachunkowości, inne przepisy prawa, przepisy wewnętrzne SGSP*) 4. Informacja stanowiąca własność intelektualną *(Ustawa o prawie autorskim i prawach pokrewnych)* 5. Informacja stanowiąca tajemnicę lekarską *(Ustawa o zawodzie lekarza)*

Załącznik nr 2
do Polityki Bezpieczeństwa Informacji w SGSP

Informacja chroniona

A. Dane osobowe

Lp.	Nazwa zbioru	Właściciel	Podstawa prawna
1.	Pracownicy SGSP	Naczelnik Wydziału Kadr i Organizacji	Kodeks pracy Ustawa o PSP
2.	Studenci WIBC	Dziekan WIBC	Ustawa Prawo o szkolnictwie wyższym
3.	Studenci WIBP	Dziekan WIBP	Ustawa Prawo o szkolnictwie wyższym, Ustawa o PSP
4.	Badania psychologiczne	Kierownik Pracowni Psychologicznej	Pismo okólne nr 6 Ministra Spraw Wewnętrznych z dnia 5 grudnia 1991r. Rozporządzenie Ministra Zdrowia z dnia 1 kwietnia 2005r.

B. Do użytku wewnętrznego

Lp.	Nazwa zbioru	Właściciel	Podstawa prawna
1.	Dane Finansowe	Kwestor	Ustawa o rachunkowości
2.	Zapisy SGSP	Autor zapisu	Komunikat Nr 16/2006 MF oraz § 7.4 Rozporządzenia MF kolumna 5 Ustawa o prawie autorskim i prawach pokrewnych,
3.	Dokumentacja/Korespondencja kancelaryjna	Autor	Przepisy i regulacje wewnętrzne

Załącznik nr 3
do Polityki Bezpieczeństwa Informacji w SGSP

Systemy przetwarzania informacji

A. Systemy informatyczne

Lp	Nazwa systemu	Administrator
1.	Simple System V	Dział Administrowania Sieciami Komputerowymi
2.	Multicache	Dział Administrowania Sieciami Komputerowymi
3.	Płatnik	Właściciel stanowiska roboczego
4.	Merak (poczta)	Dział Administrowania Sieciami Komputerowymi
5.	System wspomagania decyzji	Właściciel stanowiska roboczego
6.	Sowa	Autor oprogramowania
7.	Mapi	Autor oprogramowania
8.	Azak 2000	Właściciel stanowiska roboczego
9.	Dziekanat	Właściciel stanowiska roboczego
10.	Oprogramowanie na samodzielnym stanowisku roboczym	Właściciel stanowiska roboczego

B. System tradycyjny (papierowy)

Załącznik nr 4
do Polityki Bezpieczeństwa Informacji w SGSP

Zależności pomiędzy zbiorami danych, a systemami przetwarzania

Zbiory danych	**Systemy przetwarzania**

Załącznik nr 5
do Polityki Bezpieczeństwa Informacji w SGSP

Wzór wykazu osób upoważnionych do wglądu
do załączników do Polityki Bezpieczeństwa Informacji

Warszawa dnia ……..

ZATWIERDZAM:

……
(Rektor Komendant SGSP)

Wykaz osób upoważnionych do wglądu do załączników 2-4
do Polityki Bezpieczeństwa Informacji: