



# System managementu **BEZPEČNOSTI INFORMACÍ**

Martin Drastich

- 
- A photograph of a hard drive with several miniature soldiers in green uniforms standing on its surface. The soldiers are arranged in a circle around the central spindle of the drive. The background is a chain-link fence.
- Vývoj a současnost standardů informační bezpečnosti
  - Komentář normy ISO/IEC 27001:2005
  - Implementace systému managementu bezpečnosti informací
  - Audit, auditor, fáze auditu
  - Akreditace a certifikace ISMS



# System managementu **BEZPEČNOSTI INFORMACÍ**

Martin Drastich



**Upozornění pro čtenáře a uživatele této knihy**

Všechna práva vyhrazena. Žádná část této tištěné či elektronické knihy nesmí být reprodukována a šířena v papírové, elektronické či jiné podobě bez předchozího písemného souhlasu nakladatele. Neoprávněné užití této knihy bude **trestně stíháno**.

# Systém managementu bezpečnosti informací

**Martin Drastich**

Vydala Grada Publishing, a.s.  
U Průhonu 22, Praha 7  
jako svou 4654. publikaci

Recenzoval Doc. Mgr. Roman Jašek, Ph.D.  
Odpovědný redaktor Ing. Pavel Němeček  
Sazba Tomáš Brejcha  
Počet stran 128  
První vydání, Praha 2011

© Grada Publishing, a.s., 2011

V knize použité názvy programových produktů, firem apod. mohou být ochrannými známkami nebo registrovanými ochrannými známkami příslušných vlastníků.

Vytiskla Tiskárna PROTISKA, s.r.o., České Budějovice

ISBN 978-80-247-4251-9 (tištěná verze)  
ISBN 978-80-247-7616-3 (elektronická verze ve formátu PDF)  
ISBN 978-80-247-7617-0 (elektronická verze ve formátu EPUB)

Úvod .....	13
------------	----

## ČÁST I.: Geneze vývoje a současnost standardů informační bezpečnosti ..... 15

# 1.

### Vývoj informační bezpečnosti

1.1 Historie v souvislostech .....	16
1.1.1 Období do konce 80. let .....	16
1.1.2 Období 90. let .....	16
1.1.3 Hodnocení úrovně bezpečnosti informačních systémů .....	17
1.1.4 Globalizace a úrovně bezpečnosti .....	18
1.2 Současný stav informační bezpečnosti .....	18
1.2.1 Standardizace informační bezpečnosti .....	19
1.2.2 Průzkum stavu informační bezpečnosti v České republice .....	20
1.3 Důvody zavedení systému managementu bezpečnosti informací .....	21

# 2.

### Normy řady ČSN ISO/IEC 2700x

2.1 Struktura norem řady ISO 2700x .....	23
2.1.1 ISO 27001 – Specifikace pro systémy řízení bezpečnosti informací .....	23
2.1.2 ISO 27002 – Návod na implementaci opatření .....	23
2.1.3 ISO 27003 – Návod na zavedení ISMS v souladu s ISO/IEC 27001:2005 ...	24
2.1.4 ISO 27004 – Metriky ISMS .....	24
2.1.5 ISO 27005 – Management rizik bezpečnosti informací .....	24
2.1.6 ISO 27006 – Návod na implementaci opatření .....	24
2.1.7 ISO 27008 – Doporučení pro auditování ISMS tzv. „technický audit“ ...	24
2.1.8 ISO 27799 – Informační bezpečnost ve zdravotnictví .....	25
2.2 Připravované normy .....	25

## ČÁST II.: ISO/IEC 27001:2005 ..... 27

# 3.

### Obsah normy ISO/IEC 27001:2005

3.1 Cíle normy .....	28
3.2 Procesní model ISMS .....	28
3.2.1 Plánuj .....	29
3.2.2 Dělej .....	29
3.2.3 Kontroluj .....	30
3.2.4 Jednej .....	30
3.3 Povinná dokumentace .....	30

# 4.

## Odpovědnost, audit, přezkoumání a zlepšování

<b>4.1 Odpovědnost managementu</b>	32
4.1.1 Osobní závazek vedení	32
4.1.2 Řízení zdrojů	32
4.1.3 Školení, informovanost a odborná způsobilost	32
<b>4.2 Interní audit ISMS</b>	33
<b>4.3 Přezkoumání systému managementu ISMS</b>	33
4.3.1 Všeobecně	33
4.3.2 Vstupy pro přezkoumání	33
4.3.3 Výstupy pro přezkoumání	33
<b>4.4 Zlepšování ISMS</b>	34
4.4.1 Neustále zlepšování	34
4.4.2 Opatření k nápravě	34
4.4.3 Preventivní opatření	34

# 5.

## Bezpečnostní politika

<b>5.1 Politika bezpečnosti informací</b>	35
5.1.1 Dokument bezpečnostní politiky informací	35
5.1.2 Přezkoumání bezpečnostní politiky informací	35

# 6.

## Organizace bezpečnosti informací

<b>6.1 Vnitřní organizace</b>	37
6.1.1 Závazek vedení organizace směrem ISMS	37
6.1.2 Koordinace bezpečnosti informací	37
6.1.3 Přidělení odpovědnosti v oblasti bezpečnosti informací	37
6.1.4 Schvalovací proces pro prostředky zpracování informací	38
6.1.5 Ujednání o ochraně důvěrných informací	38
6.1.6 Kontakt s orgány veřejné správy	38
6.1.7 Kontakty se speciálními zájmovými skupinami	38
6.1.8 Nezávislé přezkoumání bezpečnosti informací	39
<b>6.2 Externí subjekty, partneři</b>	39
6.2.1 Identifikace rizik vyplývajících z přístupu externích subjektů	39
6.2.2 Bezpečnostní požadavky pro přístup klientů	39
6.2.3 Zohlednění bezpečnostních požadavků v dohodách s třetí stranou	40

# 7.

## Řízení aktiv

<b>7.1 Odpovědnost za aktiva</b>	41
7.1.1 Evidence aktiv	41
7.1.2 Vlastnictví aktiv	41
7.1.3 Přijatelné využívání aktiv	41
<b>7.2 Klasifikace informací</b>	42
7.2.1 Doporučení pro klasifikaci	42
7.2.2 Označování a zpracování informací	42

# 8.

## Bezpečnost z hlediska lidských zdrojů

<b>8.1 Před vznikem pracovního vztahu</b>	43
8.1.1 Role a odpovědnosti	43
8.1.2 Prověřování osob	43
8.1.3 Podmínky a požadavky při výkonu pracovní činnosti	43
<b>8.2 Během pracovního procesu</b>	44
8.2.1 Odpovědnosti vedoucích pracovníků	44
8.2.2 Bezpečnostní povědomí, vzdělání a výcvik	44
8.2.3 Disciplinární řízení	44
<b>8.3 Ukončení nebo změna pracovního vztahu</b>	45
8.3.1 Odpovědnost při ukončování pracovního vztahu	45
8.3.2 Navrácení zapůjčených aktiv	45
8.3.3 Odebrání přístupových práv	45

# 9.

## Fyzická bezpečnost a bezpečnost prostředí

<b>9.1 Zabezpečení prostoru</b>	46
9.1.1 Fyzický bezpečnostní perimetr	46
9.1.2 Fyzické kontroly vstupu osob	46
9.1.3 Zabezpečení kanceláří, místnosti a prostředků	46
9.1.4 Ochrana před hrozbami vnějšku a prostředí	47
9.1.5 Práce v zabezpečených oblastech	47
9.1.6 Veřejný přístup, prostory pro nakládku a vykládku	47
<b>9.2 Bezpečnost zařízení</b>	47
9.2.1 Umístění zařízení a jeho ochrana	47
9.2.2 Podpůrná zařízení, dodávky energie	48
9.2.3 Bezpečnost kabelových rozvodů	48
9.2.4 Údržba zařízení	48
9.2.5 Bezpečnost zařízení používané mimo prostory organizace	48
9.2.6 Bezpečná likvidace nebo opakované použití zařízení	48
9.2.7 Odstranění a přemístění majetku	49

# 10.

## Řízení komunikací a řízení provozu

<b>10.1 Provozní postupy a odpovědnost</b>	50
10.1.1 Dokumentace provozních postupů	50
10.1.2 Řízení změn	50
10.1.3 Oddělení povinností	50
10.1.4 Oddělení vývoje, testování a provozu	51
<b>10.2 Řízení dodávek služeb třetích stran</b>	51
10.2.1 Dodávky služeb	51
10.2.2 Monitorování a přezkoumávání služeb zabezpečovaných třetí stranou	51
10.2.3 Řízení změn ve službách zabezpečovaných třetími stranami	51
<b>10.3 Plánování a přejímání informačních systémů</b>	52
10.3.1 Řízení kapacit a kapacitní plánování	52



10.3.2	Přejímání systémů .....	52
<b>10.4</b>	<b>Ochrana proti škodlivým programům a mobilním kódům .....</b>	<b>52</b>
10.4.1	Opatření na ochranu proti škodlivým programům .....	52
10.4.2	Opatření na ochranu proti mobilním kódům .....	53
<b>10.5</b>	<b>Zálohování .....</b>	<b>53</b>
10.5.1	Zálohování informací .....	53
<b>10.6</b>	<b>Správa bezpečnosti sítě .....</b>	<b>53</b>
10.6.1	Síťová opatření .....	53
10.6.2	Bezpečnost síťových služeb .....	54
<b>10.7</b>	<b>Bezpečnost při zacházení s médii .....</b>	<b>54</b>
10.7.1	Správa výměnných počítačových médií .....	54
10.7.2	Likvidace médií .....	54
10.7.3	Postupy pro manipulaci s informacemi .....	54
10.7.4	Bezpečnost systémové dokumentace .....	55
<b>10.8</b>	<b>Výměna informací .....</b>	<b>55</b>
10.8.1	Postupy a politiky při výměně informací a programů .....	55
10.8.2	Dohody o výměně informací a programů .....	55
10.8.3	Bezpečnost médií při přepravě .....	56
10.8.4	Elektronické zasílání zpráv .....	56
10.8.5	Informační systémy organizace .....	56
<b>10.9</b>	<b>Služby elektronického obchodu .....</b>	<b>56</b>
10.9.1	Elektronický obchod .....	56
10.9.2	On-line transakce .....	57
10.9.3	Veřejně přístupné informace .....	57
<b>10.10</b>	<b>Monitorování .....</b>	<b>57</b>
10.10.1	Pořizování auditních záznamů .....	57
10.10.2	Monitorování používání systému .....	57
10.10.3	Ochrana vytvořených záznamů .....	58
10.10.4	Administrátorský a operátorský deník .....	58
10.10.5	Záznam o selhání .....	58
10.10.6	Synchronizace hodin .....	58

# 11.

## Řízení přístupu

<b>11.1</b>	<b>Požadavky na řízení přístupu .....</b>	<b>59</b>
11.1.1	Politika řízení přístupu .....	59
<b>11.2</b>	<b>Řízení přístupu uživatelů .....</b>	<b>59</b>
11.2.1	Registrace uživatele .....	59
11.2.2	Řízení privilegovaného přístupu .....	60
11.2.3	Správa uživatelských hesel .....	60
11.2.4	Přezkoumání přístupových práv uživatelů .....	60
<b>11.3</b>	<b>Odpovědnosti uživatelů .....</b>	<b>60</b>
11.3.1	Používání hesel .....	60
11.3.2	Neobsluhovaná zařízení uživatelů .....	61
11.3.3	Zásada prázdného stolu a prázdné obrazovky .....	61



<b>11.4 Řízení přístupu k síti</b>	61
11.4.1 Politika užívání síťových služeb	61
11.4.2 Autentizace uživatele pro externí připojení	61
11.4.3 Identifikace zařízení v sítích	62
11.4.4 Ochrana portů pro vzdálenou diagnostiku a konfiguraci	62
11.4.5 Princip oddělení skupin v sítích	62
11.4.6 Řízení síťových spojení	62
11.4.7 Řízení směrování sítí	62
<b>11.5 Řízení přístupu k operačnímu systému</b>	62
11.5.1 Bezpečné postupy připojení	63
11.5.2 Identifikace a autentizace uživatelů	63
11.5.3 Systém správ hesel	63
11.5.4 Použití systémových nástrojů	63
11.5.5 Časové omezení relace	63
11.5.6 Časové omezení spojení	64
<b>11.6 Řízení přístupu k aplikacím a informacím</b>	64
11.6.1 Omezení přístupu k informacím	64
11.6.2 Oddělení citlivých systémů	64
<b>11.7 Mobilní výpočetní zařízení a práce na dálku</b>	64
11.7.1 Mobilní výpočetní zařízení a sdělovací technika	64
11.7.2 Práce na dálku	65

# 12.

## **Sběr dat, vývoj a údržba informačních systémů**

<b>12.1 Požadavky na bezpečnost informačních systémů</b>	66
12.1.1 Analýza a specifikace požadavků na bezpečnost	66
<b>12.2 Správný postup zpracování v aplikacích</b>	66
12.2.1 Validace vstupních dat	66
12.2.2 Kontrola a řízení vnitřního zpracování	66
12.2.3 Celistvost zpráv	67
12.2.4 Validace výstupních dat	67
<b>12.3 Kryptografické prostředky a opatření</b>	67
12.3.1 Politika pro použití kryptografických prostředků a opatření	67
12.3.2 Správa klíčů	67
<b>12.4 Bezpečnost systémových souborů</b>	68
12.4.1 Správa provozního programového vybavení	68
12.4.2 Ochrana dat pro testování systému	68
12.4.3 Řízení přístupu do knihovny zdrojových kódů	68
<b>12.5 Bezpečnost procesů vývoje a podpory</b>	69
12.5.1 Postupy řízení změn	69
12.5.2 Technické přezkoumání změn operačního systému	69
12.5.3 Omezení změn programových balíků	69
12.5.4 Únik informací	69
12.5.5 Programové vybavení vyvíjené externím dodavatelem	70

<b>12.6 Řízení technických zranitelností</b>	70
12.6.1 Řízení, správa a kontrola technických zranitelností	70

# 13.

## **Zvládání bezpečnostních incidentů**

<b>13.1 Hlášení bezpečnostních incidentů</b>	71
13.1.1 Hlášení bezpečnostních událostí	71
13.1.2 Hlášení bezpečnostních slabín	71
<b>13.2 Zvládání bezpečnostních incidentů a kroky k nápravě</b>	72
13.2.1 Odpovědnosti a postupy	72
13.2.2 Ponaučení z bezpečnostních incidentů	72
13.2.3 Shromažďování důkazů	72

# 14.

## **Řízení kontinuity organizace**

<b>14.1 Aspekty bezpečnosti informací při řízení kontinuity činnosti organizace</b>	73
14.1.1 Zahrnutí bezpečnosti informací do procesu řízení kontinuity činnosti organizace	73
14.1.2 Kontinuita činností organizace a hodnocení rizik	73
14.1.3 Vytváření a implementace plánu kontinuity	73
14.1.4 Systém plánování kontinuity činností organizace	74
14.1.5 Testování, udržování a přezkoumávání plánu kontinuity	74

# 15.

## **Soulad a požadavky**

<b>15.1 Soulad s právními normami</b>	75
15.1.1 Identifikace odpovídajících předpisů	75
15.1.2 Ochrana duševního vlastnictví	75
15.1.3 Ochrana záznamů organizace	75
15.1.4 Ochrana dat a soukromí osobních údajů	76
15.1.5 Prevence zneužití prostředků pro zpracování informací	76
15.1.6 Registrace kryptografických opatření	76
<b>15.2 Soulad s bezpečnostními politikami, normami a technická shoda</b>	76
15.2.1 Shoda s bezpečnostními politikami a normami	76
15.2.2 Kontrola technické shody	76
<b>15.3 Hlediska auditu informačních systémů</b>	77
15.3.1 Opatření pro audit informačního systému	77
15.3.2 Ochrana nástrojů pro audit systému	77

## **ČÁST III.: Implementace** 79

# 16.

## **Implementace**

<b>16.1 Rozhodnutí managementu o zavedení ISMS</b>	80
<b>16.2 Ustanovení rozsahu a hranice ISMS</b>	80
<b>16.3 Vstupní analýza</b>	80

<b>16.4 Stanovení bezpečnostní politiky (politika ISMS)</b>	82
<b>16.5 Analýza rizik</b>	82
<b>16.6 Příklad harmonogramu implementace</b>	84
<b>16.7 Vypracování povinných dokumentů</b>	86
16.7.1 Bezpečnostní příručka	87
16.7.2 Prohlášení o aplikovatelnosti POA	87
16.7.3 Směrnice řízení dokumentů a záznamů	87
16.7.4 Směrnice interní auditu	88
16.7.5 Směrnice nápravných a preventivních opatření	88
<b>16.8 Implementace, zavádění do praxe, školení zaměstnanců</b>	89
<b>16.9 Systémový audit</b>	89
<b>16.10 Integrované systémy řízení</b>	90

## **ČÁST IV.: Audit** 93

### **Audit**

<b>17.1 Úvod do problematiky průběhu auditu</b>	94
<b>17.2 Důvody, cíle a odpovědnosti auditu</b>	95
<b>17.3 Rozsah činností auditu</b>	95

### **Auditor**

<b>18.1 Charakteristika auditora</b>	97
<b>18.2 Etický kodex auditora</b>	97
<b>18.3 Příslušný výcvik auditora</b>	98
<b>18.4 Techniky řízení týmu</b>	98
18.4.1 Styly řízení auditu	99
18.4.2 Řízení auditorského skupiny	99

### **Fáze auditu**

<b>19.1 Fáze přípravy auditu</b>	101
19.1.1 Etapa vstupního plánování	101
19.1.2 Předběžná prohlídka	101
19.1.3 Podrobné plánování	102
<b>19.2 Fáze auditování</b>	102
19.2.1 Systémy dokumentace auditu	102
19.2.2 Taktika a technika auditu	102
19.2.3 Technika dotazů	103
19.2.4 Kontrolní (check) listy	103
19.2.5 Hledání objektivních důkazů	104
19.2.6 Hledání kořenových příčin	104
19.2.7 Neshody v systému	105
19.2.8 Registrace neshod	105

19.2.9	Hlášení neshod .....	105
19.2.10	Pozorování z auditu .....	106
<b>19.3</b>	<b>Fáze následných opatření .....</b>	<b>106</b>
19.3.1	Zpráva z auditu .....	106
19.3.2	Příprava souhrnné zprávy .....	106
19.3.3	Závěrečná schůzka a prezentace souhrnné zprávy .....	107
19.3.4	Dohoda a následná nápravná opatření .....	107

## **ČÁST V.: Akreditace a certifikace .....** 109

# 20.

### **Akreditace a certifikace**

<b>20.1</b>	<b>Akreditace .....</b>	<b>110</b>
<b>20.2</b>	<b>Certifikace .....</b>	<b>110</b>
20.2.1	Certifikační orgán .....	110
20.2.2	Pracovníci certifikačního orgánu .....	111
20.2.3	Provádění dozoru .....	111
20.2.4	Certifikace procesů .....	111
20.2.5	Certifikační dokument .....	111
<b>20.3</b>	<b>Certifikační audit .....</b>	<b>112</b>
20.3.1	První etapa certifikačního auditu .....	112
20.3.2	Druhá etapa certifikačního auditu .....	113
20.3.3	Zprávy a závěry z certifikačního auditu .....	113
<b>20.4</b>	<b>Pravidla a postupy certifikačního orgánu .....</b>	<b>113</b>
20.4.1	Žádost o prvotní audit a certifikace .....	113
20.4.2	Přezkoumání žádosti k provedení auditu .....	114
<b>20.5</b>	<b>Certifikační stupně auditu .....</b>	<b>114</b>
20.5.1	První stupeň auditu .....	114
20.5.2	Druhý stupeň auditu .....	115
20.5.3	Závěry z prvotního certifikačního auditu .....	115
20.5.4	Informace pro udělení prvotní certifikace .....	116
20.5.5	Dozorové činnosti .....	116
<b>20.6</b>	<b>Udržování certifikace .....</b>	<b>116</b>
<b>20.7</b>	<b>Plánování, opakování, udělení certifikace .....</b>	<b>117</b>
<b>20.8</b>	<b>Změny v certifikačním řízení .....</b>	<b>117</b>

<b>Závěr .....</b>	<b>120</b>
<b>Bibliografie .....</b>	<b>121</b>
<b>Pojmy .....</b>	<b>122</b>
<b>Zkratky .....</b>	<b>124</b>
<b>Summary .....</b>	<b>125</b>
<b>Rejstřík .....</b>	<b>126</b>

# Úvod

Objev principů zemědělství přinesl lidstvu metodu přetváření přírodních zdrojů v bohatství, jež vyvolala první vlnu civilizačních změn. Druhá civilizační vlna přinesla tovární systém tvorby bohatství, vedla k hromadné výrobě, koncentraci průmyslu, ke snaze o vytvoření stále větších trhů a masovou spotřebu.

Po zemědělské a průmyslové revoluci jsme v současné době v období nástupu třetí revoluční vlny<sup>1</sup> tzv. informační revoluce. Na vlastní kůži dnes prožíváme příchod třetí velké vlny změn v dějinách. Ocitáme se tak uprostřed procesu vytváření nové společnosti tzv. informační společnosti, která s sebou přináší odlišné způsoby práce a myšlení, digitální ekonomiku, internetové bankovníctví, e-government, firemní informační systémy, technologie B2B a B2C atp.

Třetí vlna civilizačních změn je charakteristická tím, že primárním faktorem jsou informace. Mění se celá struktura společnosti. Homogenita druhé vlny je nahrazována heterogenitou třetí vlny, která si žádá stále více výměny informací mezi jejími uživateli – firmami, státními správou, finančními úřady, soudy, dalšími institucemi a v neposlední řadě mezi jednotlivci. To vyvolává znalost informačních a komunikačních technologií.

V souvislosti s používáním informačních a komunikačních technologií vyvstává otázka nejen pro management firem, státní organizace, ale i pro jednotlivce ohledně bezpečnosti a ochrany dat a informací. Na firemní účet (resp. u přepážky na pobočce banky), vlastní peněženku, občanský průkaz nebo cestovní pas jsme se naučili si dávat pozor, vkladní knížky bývají pečlivě uchovány, ale se zabezpečením nebo ochranou dat při využívání informačních a komunikačních technologií si již rady nevíme. Zejména firmy by si měly uvědomit, že vlastní spoustu citlivých informací o vlastní výrobě, dodavatelích, odběratelích, plánech, investicích, zaměstnancích atp.

---

<sup>1</sup> TOFFLER, A., TOFFLEROVÁ, H. *Nová civilizace. Třetí vlna a její důsledky*. Praha: Nakladatelství Dokořán, 2001; s. 15.