

**2006**

|  |                                     |
|--|-------------------------------------|
| Informační technologie - Bezpečnostní techniky -<br>Soubor postupů pro management bezpečnosti<br>informací | ČSN<br>ISO/IEC 17799<br><br>36 9790 |
|--|-------------------------------------|

Information technology - Security techniques - Code of practice for information security management

Technologies de l'information - Techniques de sécurité - Code de pratique pour la gestion de sécurité d'information

Tato norma je českou verzí mezinárodní normy ISO/IEC 17799:2005. Překlad byl zajištěn Českým normalizačním institutem. Má stejný status jako oficiální verze uvedené mezinárodní normy.

This standard is the Czech version of the International Standard ISO/IEC 17799:2005. It was translated by Czech Standards Institute. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 17799 (36 9790) z dubna 2005.

|  |  |
|--|--|
|  | © Český normalizační institut, 2006<br><b>75901</b><br>Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu. |
|--|--|

Mezi nejvýraznější změny v této aktualizované verzi patří to, že se řízení bezpečnostních incidentů stalo samostatnou oblastí bezpečnosti. Oproti předchozímu vydání normy bylo také odstraněno devět bezpečnostních opatření a sedmáct nových jich přibylo.

Informace o citovaných normativních dokumentech

ISO/IEC 9796-2:2002 zavedena v ČSN ISO/IEC 9796-2:2004 (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy - Část 2: Mechanismy založené na faktorizaci celých čísel

ISO/IEC 9796-3:2000 zavedena v ČSN ISO/IEC 9796-3:2002 (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálních podpisů umožňující obnovu zprávy - Část 3: Mechanismy založené na diskretních logaritmech

ISO 10007:2003 zavedena v ČSN ISO 10007:2004 (01 0334) Systémy managementu jakosti - Směrnice managementu konfigurace

ISO/IEC 11770-1:1996 zavedena v ČSN ISO/IEC 11770-1:1998 (36 9785) Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 1: Struktura

ISO/IEC 12207:1995 zavedena v ČSN ISO/IEC 12207:1997 (36 9784) Informační technologie - Procesy v životním cyklu softwaru

ISO/IEC TR 13335-1:1996 zavedena v ČSN ISO/IEC TR 13335-1:1999 (36 9786) Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT

ISO/IEC TR 13335-3:1998 zavedena v ČSN ISO/IEC TR 13335-3:2000 (36 9786) Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT

ISO/IEC 14888-1:1999 zavedena v ČSN ISO/IEC 14888-1:2001 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 1: Všeobecně

ISO/IEC 14888-2:1999 zavedena v ČSN ISO/IEC 14888-2:2001 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 2: Mechanismy založené na identitě

ISO/IEC 14888-3:1999 zavedena v ČSN ISO/IEC 14888-3:2001 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 3: Mechanismy založené na certifikátu

ISO/IEC 15408-1:1999 zavedena v ČSN ISO/IEC 15408-1:2001 (36 9789) Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a všeobecný model

ISO/IEC 15408-2:1999 zavedena v ČSN ISO/IEC 15408-2:2002 (36 9789) Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční požadavky

ISO/IEC 15408-3:1999 zavedena v ČSN ISO/IEC 15408-3:2002 (36 9789) Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Požadavky na záruky bezpečnosti

EN ISO 19011:2002 zavedena v ČSN EN ISO 19011:2003 (01 0330) Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu

Související ČSN

ČSN ISO/IEC 27001 (36 9790) Informační technologie - Bezpečnostní techniky - Systém řízení bezpečnosti

informací - Požadavky

Vypracování normy

Zpracovatel: Risk Analysis Consultants, s.r.o., IČ 63672774

Technická normalizační komise: TNK 20 Informační technologie

Zaměstnanec Českého normalizačního institutu: Ing. Petr Wallenfels

Strana 3

## MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky -  
Soubor postupů pro management bezpečnosti informací

ISO/IEC 17799  
Druhé vydání  
2005-06-15

ICS 35.040

### Upozornění k manipulaci s PDF souborem

Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe lze tento soubor tisknout nebo prohlížet, ale nesmí být editován, ledaže by typy písma, které jsou vloženy, byly používány na základě licence a instalovány v počítači, na němž se editace provádí. Při stažení tohoto souboru přejímají jeho uživatelé odpovědnost za to, že nebude porušena licenční politika Adobe. Ústřední sekretariát ISO nepřijímá za její porušení žádnou odpovědnost.

Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech použitých k vytváření tohoto souboru PDF, lze najít ve Všeobecných informacích, které jsou k souboru připojeny; parametry, pomocí kterých byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členské organizace ISO mohly používat. V málo pravděpodobném případě, tj. když vznikne problém, který se týká souboru, informujte o tom na níže uvedené adrese Ústřední sekretariát ISO.

© ISO/IEC 2005

Všechna práva vyhrazena. Není-li uvedeno jinak, nesmí být žádná část této publikace reprodukována nebo zpracována jakoukoli jinou formou, jako jsou například elektronické nebo mechanické prostředky, včetně fotokopii a mikrofilmů, bez písemného povolení ISO; povolení lze vyžádat na níže uvedené adrese nebo u členské národní organizace v zemi žadatele.

ISO copyright office

Case postale 56, CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail [copyright@iso.ch](mailto:copyright@iso.ch)

Obsah

|  | Strana |
|--|--------|
| <b>0</b>                                   |        |
| Úvod                                       |        |
| .....                                      |        |
| .....                                      | 10     |
| <b>0.1</b>                                 |        |
| Co je bezpečnost informací?                |        |
| .....                                      |        |
| 10   |        |
| <b>0.2</b>                                 |        |
| Proč je nezbytná bezpečnost informací..... | 10     |
| <b>0.3</b>                                 |        |
| Jak stanovit bezpečnostní požadavky.....   |        |
| 10   |        |
| <b>0.4</b>                                 |        |
| Hodnocení bezpečnostních rizik.....        |        |
| 10   |        |
| <b>0.5</b>                                 |        |
| Výběr opatření                             |        |
| .....                                      |        |
| .....                                      | 11     |
| <b>0.6</b>                                 |        |
| Východiska bezpečnosti informací           |        |
| .....                                      |        |
| .....                                      | 11     |
| <b>0.7</b>                                 |        |
| Kritické faktory úspěchu                   |        |
| .....                                      |        |
| .....                                      | 11     |
| <b>0.8</b>                                 |        |
| Vytváření vlastních směrnic                |        |
| .....                                      |        |
| 12   |        |
| <b>1</b>                                   |        |
| Předmět normy                              |        |
| .....                                      |        |
| .....                                      | 13     |
| <b>2</b>                                   |        |
| Termíny a definice                         |        |
| .....                                      |        |
| .....                                      | 13     |

|              |   |       |       |
|--------------|---|-------|-------|
| <b>3</b>     | Struktura<br>normy                                    | ..... |       |
|              |   | ..... | 14    |
| <b>3.1</b>   | Oblasti<br>bezpečnosti                                | ..... |       |
|              |   | ..... | 14    |
| <b>3.2</b>   | Hlavní kategorie<br>bezpečnosti                       | ..... |       |
|              |   | ..... | 15    |
| <b>4</b>     | Hodnocení a zvládání<br>rizik                         | ..... |       |
|              |   | ..... | .. 15 |
| <b>4.1</b>   | Hodnocení bezpečnostních<br>rizik.....                | ..... |       |
|              |   | ..... | 15    |
| <b>4.2</b>   | Zvládání bezpečnostních<br>rizik                      | ..... |       |
|              |   | ..... | 16    |
| <b>5</b>     | Bezpečnostní<br>politika                              | ..... |       |
|              |   | ..... | 16    |
| <b>5.1</b>   | Politika bezpečnosti<br>informací                     | ..... |       |
|              |   | ..... | 16    |
| <b>5.1.1</b> | Dokument bezpečnostní politiky<br>informací.....      | ..... |       |
|              |   | ..... | 16    |
| <b>5.1.2</b> | Přezkoumání bezpečnostní politiky<br>informací.....   | ..... |       |
|              |   | ..... | 17    |
| <b>6</b>     | Organizace bezpečnosti<br>informací                   | ..... |       |
|              |   | ..... | 18    |
| <b>6.1</b>   | Interní<br>organizace                                 | ..... |       |
|              |   | ..... | 18    |
| <b>6.1.1</b> | Závazek vedení směrem k bezpečnosti<br>informací..... | ..... |       |
|              |   | ..... | 18    |
| <b>6.1.2</b> | Koordinace bezpečnosti<br>informací                   | ..... |       |
|              |   | ..... | 19    |

|              |   |    |
|--------------|---|----|
| <b>6.1.3</b> | Přidělení odpovědností v oblasti bezpečnosti informací.....         | 19 |
| <b>6.1.4</b> | Schvalovací proces prostředků pro zpracování informací.....         | 20 |
| <b>6.1.5</b> | Dohody o ochraně důvěrných informací.....                           | 20 |
| <b>6.1.6</b> | Kontakt s orgány veřejné správy<br>.....                            | 21 |
| <b>6.1.7</b> | Kontakt se zájmovými skupinami<br>.....                             | 21 |
| <b>6.1.8</b> | Nezávislá přezkoumání bezpečnosti informací.....                    | 21 |
| <b>6.2</b>   | Externí subjekty<br>.....<br>.....                                  | 22 |
| <b>6.2.1</b> | Identifikace rizik vyplývajících z přístupu externích subjektů..... | 22 |
| <b>6.2.2</b> | Bezpečnostní požadavky pro přístup klientů.....                     | 23 |
| <b>6.2.3</b> | Bezpečnostní požadavky v dohodách se třetí stranou.....             | 24 |
| <b>7</b>     | Řízení aktiv<br>.....<br>.....                                      | 26 |
| <b>7.1</b>   | Odpovědnost za aktiva<br>.....<br>.....                             | 26 |
| <b>7.1.1</b> | Evidence aktiv<br>.....<br>.....                                    | 26 |
| <b>7.1.2</b> | Vlastnictví aktiv<br>.....<br>.....                                 | 27 |
| <b>7.1.3</b> | Přípustné použití aktiv<br>.....<br>.....                           | 27 |
| <b>7.2</b>   | Klasifikace informací   |    |

|  |       |
|--|-------|
| .....  | 28    |
| <b>7.2.1</b> Doporučení pro klasifikaci                | ..... |
| ..   | 28    |
| <b>7.2.2</b> Označování a zacházení s informacemi..... | 28    |

Strana 5

|   | Strana |
|---|--------|
| <b>8</b> Bezpečnost z hlediska lidských zdrojů.....   | 29     |
| <b>8.1</b> Před vznikem pracovního vztahu   | .....  |
| .....   | 29     |
| <b>8.1.1</b> Role a odpovědnosti  | .....  |
| .....   | 29     |
| <b>8.1.2</b> Prověřování  | .....  |
| .....   | 29     |
| <b>8.1.3</b> Podmínky výkonu pracovní činnosti.....   | 30     |
| <b>8.2</b> Během pracovního vztahu  | .....  |
| ..  | 31     |
| <b>8.2.1</b> Odpovědnosti vedoucích zaměstnanců.....  | 31     |
| <b>8.2.2</b> Bezpečnostní povědomí, vzdělávání a školení v oblasti bezpečnosti informací..... | 31     |
| <b>8.2.3</b> Disciplinární řízení   | .....  |
| .....   | 32     |

|              |  |    |
|--------------|--|----|
| <b>8.3</b>   | Ukončení nebo změna pracovního vztahu.....             | 32 |
| <b>8.3.1</b> | Odpovědnosti při ukončení pracovního vztahu.....       | 32 |
| <b>8.3.2</b> | Navrácení zapůjčených prostředků<br>.....              | 33 |
| <b>8.3.3</b> | Odebrání přístupových práv<br>.....<br>33              |    |
| <b>9</b>     | Fyzická bezpečnost a bezpečnost prostředí.....         | 34 |
| <b>9.1</b>   | Zabezpečené oblasti<br>.....<br>..... 34               |    |
| <b>9.1.1</b> | Fyzický bezpečnostní perimetr<br>.....                 | 34 |
| <b>9.1.2</b> | Fyzické kontroly vstupu osob<br>.....<br>35            |    |
| <b>9.1.3</b> | Zabezpečení kanceláří, místností a prostředků.....     | 35 |
| <b>9.1.4</b> | Ochrana před hrozbami vnějšku a prostředí.....         | 35 |
| <b>9.1.5</b> | Práce v zabezpečených oblastech<br>.....               | 36 |
| <b>9.1.6</b> | Veřejný přístup, prostory pro nakládku a vykládku..... | 36 |
| <b>9.2</b>   | Bezpečnost zařízení<br>.....<br>..... 36               |    |
| <b>9.2.1</b> | Umístění zařízení a jeho ochrana<br>.....              | 36 |

|               |   |  |
|---------------|---|--|
| <b>9.2.2</b>  | Podpůrná<br>zařízení<br>.....<br>..... 37                     |  |
| <b>9.2.3</b>  | Bezpečnost kabelových<br>rozvodů<br>..... 38                  |  |
| <b>9.2.4</b>  | Údržba<br>zařízení<br>.....<br>..... 38                       |  |
| <b>9.2.5</b>  | Bezpečnost zařízení mimo prostory<br>organizace..... 38       |  |
| <b>9.2.6</b>  | Bezpečná likvidace nebo opakované použití<br>zařízení..... 39 |  |
| <b>9.2.7</b>  | Přemístění<br>majetku<br>.....<br>..... 39                    |  |
| <b>10</b>     | Řízení komunikací a řízení<br>provozu.....<br>40              |  |
| <b>10.1</b>   | Provozní postupy a<br>odpovědnosti<br>..... 40                |  |
| <b>10.1.1</b> | Dokumentace provozních<br>postupů.....<br>40                  |  |
| <b>10.1.2</b> | Řízení<br>změn<br>.....<br>..... 40                           |  |
| <b>10.1.3</b> | Oddělení<br>povinností<br>.....<br>..... 41                   |  |
| <b>10.1.4</b> | Oddělení vývoje, testování a<br>provozu.....<br>41            |  |
| <b>10.2</b>   | Řízení dodávek služeb třetích<br>stran..... 42                |  |

|               |  |       |       |
|---------------|--|-------|-------|
| <b>10.2.1</b> | Dodávky služeb   | ..... | ..... |
|               |  | ..... | 42    |
| <b>10.2.2</b> | Monitorování a přezkoumávání služeb třetích stran..... |       | 42    |
| <b>10.2.3</b> | Řízení změn služeb poskytovaných třetími stranami..... |       | 43    |
| <b>10.3</b>   | Plánování a přejímání informačních systémů.....        |       | 43    |
| <b>10.3.1</b> | Řízení kapacit   | ..... | ..... |
|               |  | ..... | 43    |
| <b>10.3.2</b> | Přejímání systémů                                      | ..... | ..... |
|               |  | ..... | 44    |

|               |   |       |       |
|---------------|---|-------|-------|
| <b>10.4</b>   | Ochrana proti škodlivým programům a mobilním kódům..... |       | 44    |
| <b>10.4.1</b> | Opatření na ochranu proti škodlivým programům.....      |       | 45    |
| <b>10.4.2</b> | Opatření na ochranu proti mobilním kódům.....           |       | 45    |
| <b>10.5</b>   | Zálohování  | ..... | ..... |
|               |   | ..... | 46    |
| <b>10.5.1</b> | Zálohování informací                                    | ..... | ..... |
|               |   | ..... | 46    |
| <b>10.6</b>   | Správa bezpečnosti sítě                                 | ..... | ..... |
|               |   | ..... | 47    |

|               |   |    |
|---------------|---|----|
| <b>10.6.1</b> | Síťová<br>opatření                                    | 47 |
| <b>10.6.2</b> | Bezpečnost síťových<br>služeb                         | 47 |
| <b>10.7</b>   | Bezpečnost při zacházení s<br>médii                   | 48 |
| <b>10.7.1</b> | Správa výměnných počítačových<br>médii                | 48 |
| <b>10.7.2</b> | Likvidace<br>médii                                    | 48 |
| <b>10.7.3</b> | Postupy pro manipulaci s<br>informacemi               | 49 |
| <b>10.7.4</b> | Bezpečnost systémové<br>dokumentace                   | 49 |
| <b>10.8</b>   | Výměna<br>informací                                   | 50 |
| <b>10.8.1</b> | Postupy a politiky při výměně informací a<br>programů | 50 |
| <b>10.8.2</b> | Dohody o výměně informací a<br>programů               | 51 |
| <b>10.8.3</b> | Bezpečnost médií při<br>přepově                       | 52 |
| <b>10.8.4</b> | Elektronické zasílání<br>zpráv                        | 52 |
| <b>10.8.5</b> | Informační systémy<br>organizace                      | 53 |

|                |                                      |    |
|----------------|--------------------------------------|----|
| <b>10.9</b>    | Služby elektronického obchodu        | 53 |
| <b>10.9.1</b>  | Elektronický obchod                  | 53 |
| <b>10.9.2</b>  | On-line transakce                    | 54 |
| <b>10.9.3</b>  | Veřejně přístupné informace          | 55 |
| <b>10.10</b>   | Monitorování                         | 55 |
| <b>10.10.1</b> | Pořizování auditních záznamů         | 55 |
| <b>10.10.2</b> | Monitorování používání systému       | 56 |
| <b>10.10.3</b> | Ochrana vytvořených záznamů          | 57 |
| <b>10.10.4</b> | Administrátorský a operátorský deník | 57 |
| <b>10.10.5</b> | Záznam selhání                       | 57 |
| <b>10.10.6</b> | Synchronizace hodin                  | 58 |
| <b>11</b>      | Řízení přístupu                      | 58 |

|               |  |    |
|---------------|--|----|
| <b>11.1</b>   | Požadavky na řízení<br>přístupu                        | 58 |
| <b>11.1.1</b> | Politika řízení<br>přístupu                            | 58 |
| <b>11.2</b>   | Řízení přístupu<br>uživatelů                           | 59 |
| <b>11.2.1</b> | Registrace<br>uživatele                                | 59 |
| <b>11.2.2</b> | Řízení privilegovaného<br>přístupu                     | 60 |
| <b>11.2.3</b> | Správa uživatelských<br>hesel                          | 60 |
| <b>11.2.4</b> | Přezkoumání přístupových práv<br>uživatelů             | 61 |
| <b>11.3</b>   | Odpovědnosti<br>uživatelů                              | 61 |
| <b>11.3.1</b> | Používání<br>hesel                                     | 61 |
| <b>11.3.2</b> | Neobsluhovaná uživatelská<br>zařízení                  | 62 |
| <b>11.3.3</b> | Zásada prázdného stolu a prázdné obrazovky<br>monitoru | 62 |

|               |   |    |
|---------------|---|----|
| <b>11.4</b>   | Řízení přístupu k síti                                | 63 |
| <b>11.4.1</b> | Politika užívání síťových služeb                      | 63 |
| <b>11.4.2</b> | Autentizace uživatele pro externího připojení         | 64 |
| <b>11.4.3</b> | Identifikace zařízení v sítích                        | 64 |
| <b>11.4.4</b> | Ochrana portů pro vzdálenou diagnostiku a konfiguraci | 64 |
| <b>11.4.5</b> | Princip oddělení v sítích                             | 65 |
| <b>11.4.6</b> | Řízení síťových spojení                               | 65 |
| <b>11.4.7</b> | Řízení směrování sítě                                 | 66 |
| <b>11.5</b>   | Řízení přístupu k operačnímu systému                  | 66 |
| <b>11.5.1</b> | Bezpečné postupy přihlášení                           | 66 |
| <b>11.5.2</b> | Identifikace a autentizace uživatelů                  | 67 |
| <b>11.5.3</b> | Systém správy hesel                                   | 68 |

|               |   |    |
|---------------|---|----|
| <b>11.5.4</b> | Použití systémových nástrojů                    | 68 |
| <b>11.5.5</b> | Časové omezení relace                           | 69 |
| <b>11.5.6</b> | Časové omezení spojení                          | 69 |
| <b>11.6</b>   | Řízení přístupu k aplikacím a informacím        | 69 |
| <b>11.6.1</b> | Omezení přístupu k informacím                   | 69 |
| <b>11.6.2</b> | Oddělení citlivých systémů                      | 70 |
| <b>11.7</b>   | Mobilní výpočetní zařízení a práce na dálku     | 70 |
| <b>11.7.1</b> | Mobilní výpočetní zařízení a sdělovací technika | 70 |
| <b>11.7.2</b> | Práce na dálku                                  | 71 |
| <b>12</b>     | Akvizice, vývoj a údržba informačního systémů   | 72 |
| <b>12.1</b>   | Bezpečnostní požadavky informačních systémů     | 72 |
| <b>12.1.1</b> | Analýza a specifikace bezpečnostních požadavků  | 72 |
| <b>12.2</b>   | Správné zpracování v aplikacích                 | 73 |
| <b>12.2.1</b> | Validace vstupních dat                          |    |

|  |       |
|--|-------|
| .....  | 73    |
| <b>12.2.2</b> Kontrola vnitřního<br>zpracování                       | ..... |
| 74   |       |
| <b>12.2.3</b> Integrita<br>zpráv                                     | ..... |
| ..... 74   |       |
| <b>12.2.4</b> Validace výstupních<br>dat                             | ..... |
| ..... 75   |       |
| <b>12.3</b> Kryptografická<br>opatření                               | ..... |
| ..... 75   |       |
| <b>12.3.1</b> Politika pro použití kryptografických<br>opatření..... | 75    |
| <b>12.3.2</b> Správa<br>klíčů  | ..... |
| ..... 76   |       |
| <b>12.4</b> Bezpečnost systémových<br>souborů.....                   | 77    |
| <b>12.4.1</b> Správa provozního programového<br>vybavení.....        | 77    |
| <b>12.4.2</b> Ochrana dat pro testování<br>systému.....              | 78    |
| <b>12.4.3</b> Řízení přístupu ke knihovně zdrojových<br>kódů.....    | 78    |
| <b>12.5</b> Bezpečnost procesů vývoje a<br>podpory.....              | 79    |
| <b>12.5.1</b> Postupy řízení<br>změn                                 | ..... |
| ..... 79   |       |

|               |   |    |
|---------------|---|----|
| <b>12.5.2</b> | Technické přezkoumání aplikací po změnách operačního systému..... | 80 |
| <b>12.5.3</b> | Omezení změn programových balíčků.....                            | 80 |
| <b>12.5.4</b> | Únik informací<br>.....   | 80 |
| <b>12.5.5</b> | Programové vybavení vyvíjené externím dodavatelem.....            | 81 |

Strana 8

|               | Strana   |    |
|---------------|--|----|
| <b>12.6</b>   | Řízení technických zranitelností<br>.....                | 81 |
| <b>12.6.1</b> | Řízení, správa a kontrola technických zranitelností..... | 81 |
| <b>13</b>     | Zvládání bezpečnostních incidentů<br>.....               | 82 |
| <b>13.1</b>   | Hlášení bezpečnostních událostí a slabín.....            | 82 |
| <b>13.1.1</b> | Hlášení bezpečnostních událostí<br>.....                 | 83 |
| <b>13.1.2</b> | Hlášení bezpečnostních slabín<br>.....                   | 84 |
| <b>13.2</b>   | Zvládání bezpečnostních incidentů a kroky k nápravě..... | 84 |
| <b>13.2.1</b> | Odpovědnosti a postupy<br>.....                          | 84 |
| <b>13.2.2</b> | Ponaučení z bezpečnostních incidentů.....                | 85 |
| <b>13.2.3</b> | Shromažďování  |    |

|               |  |    |
|---------------|--|----|
|               | důkazů   |    |
|               | .....  | 85 |
| <b>14</b>     | Řízení kontinuity činností organizace  | 86 |
| <b>14.1</b>   | Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací.....  | 86 |
| <b>14.1.1</b> | Zahrnutí bezpečnosti informací do procesu řízení kontinuity činností organizace..... | 86 |
| <b>14.1.2</b> | Kontinuita činností organizace a hodnocení rizik.....                                | 87 |
| <b>14.1.3</b> | Vytváření a implementace plánů kontinuity.....                                       | 87 |
| <b>14.1.4</b> | Systém plánování kontinuity činností organizace.....                                 | 88 |
| <b>14.1.5</b> | Testování, udržování a přezkoumávání plánů kontinuity.....                           | 89 |
| <b>15</b>     | Soulad s požadavky   | 89 |
| <b>15.1</b>   | Soulad s právními normami  | 89 |
| <b>15.1.1</b> | Identifikace odpovídajících předpisů.....  | 90 |
| <b>15.1.2</b> | Ochrana duševního vlastnictví  | 90 |
| <b>15.1.3</b> | Ochrana záznamů organizace   | 91 |
| <b>15.1.4</b> | Ochrana dat a soukromí osobních údajů.....   | 91 |
| <b>15.1.5</b> | Prevence zneužití prostředků pro zpracování informací.....                           | 92 |

|               |  |    |
|---------------|--|----|
| <b>15.1.6</b> | Regulace kryptografických opatření.....                            | 92 |
| <b>15.2</b>   | Soulad s bezpečnostními politikami, normami a technická shoda..... | 93 |
| <b>15.2.1</b> | Shoda s bezpečnostními politikami a normami.....                   | 93 |
| <b>15.2.2</b> | Kontrola technické shody<br>.....<br>... 93                        |    |
| <b>15.3</b>   | Hlediska auditu informačních systémů.....                          | 94 |
| <b>15.3.1</b> | Opatření k auditu informačních systémů.....                        | 94 |
| <b>15.3.2</b> | Ochrana nástrojů pro audit informačních systémů.....               | 94 |
|               | Abeecední rejstřík<br>.....<br>.....                               | 95 |

## Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím technických komisí zřízených příslušnou organizací k tomu, aby se zabývaly určitou oblastí technické činnosti. V oblastech společného zájmu technické komise ISO a IEC spolupracují. Práce se zúčastňují i jiné mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou zpracovány v souladu s pravidly uvedenými v části 2 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je připravovat mezinárodní normy. Návrhy mezinárodních norem přijaté společnou technickou komisí se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Pozornost je třeba věnovat možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nenesou odpovědnost za identifikaci všech patentových práv nebo kteréhokoliv z nich.

Mezinárodní norma ISO/IEC 17799 byla připravena společnou technickou komisí ISO/IEC JTC 1 *Information technology*, subkomise SC 27, *IT Security techniques*.

Toto druhé vydání ruší a nahrazuje první vydání (ISO/IEC 17799:2000), které bylo technicky revidováno.

Technická komise ISO/IEC JTC 1/SC 27 připravuje soubor mezinárodních norem věnovaných systému řízení bezpečnosti informací (ISMS). Soubor norem zahrnuje požadavky na systém řízení bezpečnosti informací, managementu rizik, metriky a měření výkonu a doporučení k implementaci. Soubor těchto norem bude vydán v sérii 27000.

ISO/IEC 17799 by měla být do této nové řady začleněna v roce 2007 a to jako ISO/IEC 27002.

Strana 10

---

## 0 Úvod

### 0.1 Co je bezpečnost informací?

Informace jsou aktiva, která mají pro organizaci hodnotu. Je tedy nutné je vhodným způsobem chránit. Obzvláště se vzrůstající propojeností prostředí jednotlivých organizací je tato potřeba stále více aktuální. S rostoucí propojeností jsou informace vystaveny zvyšujícímu se počtu různých hrozeb a zranitelností (viz také Směrnice OECD pro bezpečnost informačních systémů a sítí: směrem ke kultuře bezpečnosti<sup>1</sup>).

Informace mohou existovat v různých podobách. Mohou být vytištěny nebo napsány na papíře, uloženy v elektronické podobě, posílány poštou nebo elektronickou cestou, zachyceny na film nebo vyřčeny při konverzaci.

Bezpečnost informací je zaměřena na širokou škálu hrozeb a zajiš»uje tak kontinuitu činností organizace, minimalizuje obchodní ztráty a maximalizuje návratnost investic a podnikatelských příležitostí.

Bezpečnosti informací lze dosáhnout implementací soustavy opatření, která mohou existovat ve formě pravidel, postupů, procedur, organizační struktury, programových a hardwarových funkcí. Tato opatření musí být ustavena, zavedena, provozována, monitorována, přezkoumávána a zlepšována proto, aby bylo dosaženo specifických bezpečnostních cílů organizace. Toto všechno by mělo být prováděno v souladu s ostatními řídicími procesy organizace.

### 0.2 Proč je nezbytná bezpečnost informací

Informace a podpůrné procesy, systémy a sítě jsou důležitými aktivy organizace. Vymezení, zavádění, podpora a zlepšování bezpečnosti informací může být zásadní pro udržení konkurenceschopnosti, peněžních toků (cash-flow), ziskovosti, právní shody a dobrého jména organizace.

Stále rostoucí měrou jsou organizace a jejich informační systémy vystavovány bezpečnostním hrozbám z různých zdrojů, včetně počítačových podvodů, špionáže, sabotáže, vandalizmu, požárů a povodní. Zdroje škod, jako jsou počítačové viry, útoky hackerů a útoky typu odepření služby (denial of service), jsou stále častější, roste jejich nebezpečnost a sofistikovanost.

Bezpečnost informací je důležitá z hlediska ochrany kritické infrastruktury a to jak v soukromém, tak

ve státním sektoru. V obou sektorech je bezpečnost informací důležitá pro existenci některých služeb, například e-governmentu nebo e-komerce a zároveň kvůli vyhnutí se nebo snížení relevantních rizik. Propojení veřejných a privátních sítí i sdílení informačních zdrojů zvyšuje obtížnost řízení přístupu. Trend směřující k distribuovanému zpracování oslabil efektivnost centrální kontroly prováděné specialisty.

Mnoho informačních systémů nebylo navrženo tak, aby byly bezpečné. Bezpečnost, která může být dosažena technickými prostředky, je nedostačující a měla by být doplněna odpovídajícím řízením a postupy. Pro určení opatření, která je třeba přijmout, je nutné pečlivé plánování a rozbor každého detailu. Řízení bezpečnosti informací proto vyžaduje alespoň nějakou spoluúčasť všech zaměstnanců organizace. Může rovněž zahrnovat spolupráci majitelů organizace (akcionářů), dodavatelů, třetích stran, zákazníků a dalších externích subjektů. V neposlední řadě může být potřebná i rada od specialistů z jiných organizací.

### 0.3 Jak stanovit bezpečnostní požadavky

Je nezbytné, aby organizace určila své bezpečnostní požadavky. K tomu existují tři hlavní zdroje.

- 1) Prvním zdrojem je hodnocení rizik, která organizaci hrozí, beroucí v potaz celkovou strategii a cíle organizace. V rámci hodnocení rizik se identifikují hrozby působící vůči aktivům, zranitelnosti, které mohou být hrozbami využity i pravděpodobnost jejich výskytu, a provádí se odhad jejich potenciálního dopadu.
- 2) Druhým zdrojem jsou požadavky zákonů a podzákonných norem, smluvní ujednání a místní zvyklosti, které organizace, její obchodní, smluvní partneři a poskytovatelé služeb musí splňovat.
- 3) Třetím zdrojem jsou konkrétní principy, cíle a požadavky na zpracování informací, které si organizace vytvořila pro podporu své činnosti.

### 0.4 Hodnocení bezpečnostních rizik

Požadavky na bezpečnost jsou stanoveny za pomoci metodického hodnocení bezpečnostních rizik. Výdaje na bezpečnostní opatření by měly odpovídat ztrátám způsobeným narušením bezpečnosti.

---

<sup>1)</sup> OECD Guidelines for the Security of Information systems and Network – Towards a Culture of Security.

Výsledky hodnocení rizik pomohou určit vedení organizace odpovídající kroky i priority pro řízení bezpečnostních rizik u informací a pro realizaci opatření určených k zamezení jejich výskytu.

Hodnocení rizik by mělo být prováděno periodicky, aby bylo možné včas reagovat na jakékoliv změny v bezpečnostních požadavcích.

Více informací o hodnocení rizik je uvedeno v 4.1 „Hodnocení bezpečnostních rizik“.

### 0.5 Výběr opatření

Jakmile jsou identifikovány bezpečnostní požadavky a rizika, a bylo rozhodnuto jakým způsobem bude se zjištěnými riziky naloženo, měla by být vybrána a implementována opatření zajišťující snížení rizik na přijatelnou úroveň. Taková opatření mohou být vybrána z tohoto dokumentu nebo i z jiných souborů opatření. Pro pokrytí specifických potřeb mohou být vytvořena zcela nová opatření. Výběr konkrétních opatření je na rozhodnutí každé organizace. Rozhodnutí je založeno na kritériích určujících akceptaci nebo zvládnání rizika a celkovém přístupu organizace k řízení rizik. Při výběru opatření by měla být zohledněna příslušná národní a mezinárodní legislativa a regulace.

Některá opatření v tomto dokumentu mohou být chápána jako základní doporučení pro řízení bezpečnosti informací a mohou být využita ve většině organizací. Detailněji jsou vysvětlena v části „Východiska bezpečnosti informací“.

Další informace o výběru opatření a způsobech zvládnání rizik jsou uvedeny v 4.2 „Zvládnání bezpečnostních rizik“.

## 0.6 Východiska bezpečnosti informací

Řada opatření může být považována za základní principy představující dobrá východiska pro implementaci bezpečnosti informací. Mohou vycházet ze základních legislativních požadavků nebo jsou obecně považována za nejlepších způsob řešení bezpečnosti informací.

Opatření, která by měla být pro organizaci podstatná z pohledu legislativy, jsou:

- a) ochrana osobních údajů (viz 15.1.4);
- b) ochrana důležité dokumentace organizace, jako například účetních záznamů (viz 15.1.3);
- c) ochrana duševního vlastnictví (viz 15.1.2).

Opatření, považovaná za základ nejlepších praktik (best practices) pro zajištění bezpečnosti informací, jsou:

- a) dokument bezpečnostní politiky informací (viz 5.1.1);
- b) přidělení odpovědností v oblasti bezpečnosti informací (viz 6.1.3);
- c) vzdělávání, školení a zvyšování povědomí v oblasti bezpečnosti informací (viz 8.2.2);
- d) bezchybné zpracování v aplikačních systémech (viz 12.2);
- e) řízení technických zranitelností (viz 12.6);
- f) řízení kontinuity činností organizace (viz 14);
- g) zvládnání bezpečnostních incidentů a kroky k nápravě (viz 13.2).

Tato opatření fungují ve většině organizací a prostředí.

Ačkoliv všechna opatření uvedená v tomto dokumentu jsou důležitá, je nutné si uvědomit, že o výběru a aplikaci konkrétních opatření by mělo být rozhodnuto až ve světle specifických rizik, kterým organizace čelí. I když výše uvedené doporučení může být považováno za dobré východisko, nenahrazuje výběr opatření vycházející z hodnocení rizik.

## 0.7 Kritické faktory úspěchu

Jak ukazuje zkušenost, pro úspěšnou implementaci bezpečnosti informací v organizaci jsou často kritické následující faktory:

- a) bezpečnostní politika, bezpečnostní cíle a činnosti, které respektují cíle činností organizace;
- b) přístup k zavádění, udržování, monitorování a zlepšování bezpečnosti informací v souladu s kulturou organizace;

Strana 12

---

- c) zřetelná podpora a angažovanost ze strany vedení organizace;
- d) dobré pochopení bezpečnostních požadavků, hodnocení a managementu rizik;
- e) účinný marketing bezpečnosti vůči vedení organizace, zaměstnancům a jiným stranám;
- f) rozšíření směrnic a norem bezpečnostní politiky informací mezi všechny zaměstnance, vedení organizace a třetí strany;
- g) zdroje na financování činností souvisejících s řízením bezpečnosti informací;
- h) realizace odpovídajících školení, vzdělávání a programů zvyšování povědomí;
- i) zavedení procesu zvládnání bezpečnostních incidentů;
- j) komplexní a vyvážený systém pro ohodnocení míry účinnosti<sup>2</sup> řízení bezpečnosti informací a získávání návrhů ke zlepšení na základě zpětné vazby.

## 0.8 Vytváření vlastních směrnic

Tento soubor postupů může být chápán jako východisko pro vytváření specifických směrnic organizace. Ne všechna doporučení a opatření tohoto souboru postupů mohou být použitelná. Kromě toho mohou být nezbytná i další opatření, která nejsou v tomto dokumentu uvedena. V takovém případě je užitečné zanechat v nich odkaz na tuto normu a usnadnit tak ověření shody prováděné auditory a obchodními partnery.

---

<sup>2</sup> Měření účinnosti implementovaného ISMS je mimo rozsah této normy.

Strana 13

---

## 1 Předmět normy

Tato mezinárodní norma poskytuje doporučení a obecné principy pro vymezení, zavedení, udržování a zlepšování systému managementu bezpečnosti informací v organizaci. Cíle, popsané v normě, poskytují rady o obecně přijímaných cílech managementu bezpečnosti.

Cíle opatření a jednotlivá opatření obsažená v této mezinárodní normě by měla být implementována na základě požadavků zjištěných v rámci analýzy rizik. Norma může sloužit jako praktický průvodce při vývoji bezpečnostních standardů organizace, účinných řídicích bezpečnostních postupů a také při

budování důvěry mezi organizacemi.

---

**-- Vynechaný text --**