

# MEZINÁRODNÍ NORMA

## Informační technologie – Směrnice pro řízení bezpečnosti informačních technologií (IT) – Část 2: Řízení a plánování bezpečnosti IT

ISO/IEC TR 13335-2

První vydání

1997-12-15

ICS 35.040

Deskriptory: data processing, information interchange, network interconnection, communication procedure, security techniques, concepts, models, rules (instructions).

Sp 259

ODD. VĚDECKÝCH INFORMACÍ při MZČR  
Palackého nám. 4, 128 01 Praha 2 34  
detašované pracoviště NLK Praha 2  
DIČ CZ00023825 IČO 00023825

11 757

### Obsah

Př. č. 304/2005

Strana

|                                                                                  |    |
|----------------------------------------------------------------------------------|----|
| Předmluva.....                                                                   | 5  |
| Úvod .....                                                                       | 6  |
| 1 Předmět normy .....                                                            | 7  |
| 2 Odkazy .....                                                                   | 7  |
| 3 Termíny a definice .....                                                       | 7  |
| 4 Struktura .....                                                                | 7  |
| 5 Účel .....                                                                     | 7  |
| 6 Základy .....                                                                  | 7  |
| 7 Řízení bezpečnosti IT .....                                                    | 8  |
| 7.1 Přehled plánovacího a řídicího procesu .....                                 | 8  |
| 7.2 Přehled managementu rizik .....                                              | 9  |
| 7.3 Přehled implementace .....                                                   | 10 |
| 7.4 Přehled aktivit sledování .....                                              | 10 |
| 7.5 Integrovaní bezpečnosti IT .....                                             | 10 |
| 8 Politika bezpečnosti IT celé společnosti .....                                 | 10 |
| 8.1 Cíle .....                                                                   | 10 |
| 8.2 Souhlas managementu .....                                                    | 11 |
| 8.3 Vztahy mezi politikami .....                                                 | 11 |
| 8.4 Prvky politiky bezpečnosti IT celé společnosti .....                         | 12 |
| 9 Organizační aspekty bezpečnosti IT .....                                       | 12 |
| 9.1 Role a odpovědnosti .....                                                    | 12 |
| 9.1.1 Fórum bezpečnosti IT .....                                                 | 13 |
| 9.1.2 Pracovník bezpečnosti IT celé společnosti .....                            | 14 |
| 9.1.3 Pracovník bezpečnosti projektů IT a pracovník bezpečnosti systémů IT ..... | 14 |
| 9.2 Závazek managementu .....                                                    | 14 |
| 9.3 Shodný přístup .....                                                         | 15 |
| 10 Volby strategie analýzy rizik celé společnosti .....                          | 15 |
| 10.1 Základní přístup .....                                                      | 16 |
| 10.2 Neformální přístup .....                                                    | 16 |
| 10.3 Podrobná analýza rizik .....                                                | 16 |

|                                          | Strana |
|------------------------------------------|--------|
| 10.4 Kombinovaný přístup.....            | 17     |
| 11 Doporučení pro bezpečnost IT.....     | 17     |
| 11.1 Výběr ochranných opatření.....      | 17     |
| 11.2 Přijetí rizik.....                  | 18     |
| 12 Politika bezpečnosti systému IT.....  | 18     |
| 13 Plán bezpečnosti IT.....              | 19     |
| 14 Implementace ochranných opatření..... | 19     |
| 15 Povědomí o bezpečnosti.....           | 20     |
| 16 Aktivita sledování.....               | 21     |
| 16.1 Aktualizace.....                    | 21     |
| 16.2 Bezpečnostní shoda.....             | 21     |
| 16.3 Monitorování.....                   | 22     |
| 16.4 Řešení incidentů.....               | 22     |
| 17 Shrnutí.....                          | 22     |



Označeno  
23.01.2009  
OVI  
ABE015



Národní lékařská knihovna - OVI

Název: ČSN ISO/IEC TR 13335-2

Autor:

Rok 2000



11000125415M0001

Přír. č.: SP20050304 Sign: Sp 259