

Infoturbe poliitika sisukorra näidis.

Üleüldise infoturbepoliitika sisukorra näide

Sisukord

1. Sissejuhatus
 - 1.1. Ülevaade

 - 1.2. Infoturbepoliitika rakendusala ja eesmärk
2. Turvaeesmärgid ja -põhimõtted
 - 2.1. Eesmärgid
 - 2.2. Põhimõtted
3. Turbe organisatsioon ja infrastruktuur
 - 3.1. Kohustused
 - 3.2. Turvapoliitikad
 - 3.3. Turvaintsidentidest teatamine
4. Infoturbe ja riskianalüüsi ning riskihalduse strateegia
 - 4.1. Sissejuhatus
 - 4.2. Riskianalüüs ja riskihaldus
 - 4.3. Turbe vastavuse kontroll
5. Informatsiooni tundlikkus ja riskid
 - 5.1. Sissejuhatus
 - 5.2. Informatsiooni märgistuse süsteem
 - 5.3. Ülevaade organisatsiooni informatsioonist
 - 5.4. Organisatsiooni informatsiooni väärtus ja tundlikkustasemed
 - 5.5. Ülevaade ohtudest, nõrkustest ja riskidest
6. Riistvara ja tarkvara turve
 - 6.1. Identimine ja autentimine
 - 6.2. Pääsu reguleerimine
 - 6.3. Arvestus ja revisjonipäevik
 - 6.4. Täielik kustutus
 - 6.5. Ründetarkvara
 - 6.6. Personaalarvutite turve

An Example Contents List for a Corporate IT Security Policy

Contents

1. Introduction
 - 1.1 Overview

 - 1.2 Scope and Purpose of the IT Security Policy
2. Security Objectives and Principles
 - 2.1 Objectives
 - 2.2 Principles
3. Security Organization/infrastructure
 - 3.1 Responsibilities
 - 3.2 Security Policies
 - 3.3 Security Incident Reporting
4. IT Security/Risk Analysis and Management Strategy
 - 4.1 Introduction
 - 4.2 Risk Analysis and Management
 - 4.3 Security Compliance Checking
5. Information Sensitivity and Risks
 - 5.1 Introduction
 - 5.2 Information Marking Scheme

 - 5.3 Organization Information Overview
 - 5.4 Organization Information Values/Sensitivity Levels
 - 5.5 Threats/Vulnerabilities/Risks Overview
6. Hardware and Software Security
 - 6.1 Identification and Authentication
 - 6.2 Access Control
 - 6.3 Accounting and Audit Trail
 - 6.4 Full Deletion
 - 6.5 Malicious Software
 - 6.7 PC Security

| | |
|--|--|
| 6.7. Sülearvutite turve | 6.8 Laptop Security |
| 7. Side turve | 7. Communications Security |
| 7.1. Sissejuhatus | 7.1 Introduction |
| 7.2. Võrgunduse infrastruktuur | 7.2 The Networking Infrastructure |
| 7.3. Internet | 7.3 INTERNET |
| 7.4. Krüpteerimine ja sõnumiautentimine | 7.4 Encryption/Message Authentication |
| 8. Füüsiline turve | 8. Physical Security |
| 8.1. Sissejuhatus | 8.1 Introduction |
| 8.2. Ruumide asukoht | 8.2 Location of Facilities |
| 8.3. Hoone turvalisus ja kaitse | 8.3 Building Security and Protection |
| 8.4. Hoone teenuste kaitse | 8.4 Protection of Building Services |
| 8.5. Abiteenuste kaitse | 8.5 Protection of Supporting Services |
| 8.6. Volitamata hõive | 8.6 Unauthorised Occupation |
| 8.7. Juurdepääs personaalarvutitele või tööjaamadele | 8.7 PC/Workstation Accessibility |
| 8.8. Juurdepääs magnetkandjatele | 8.8 Access to Magnetic Media |
| 8.9. Personali kaitse | 8.9 Protection of Staff |
| 8.10. Kaitse kahjutule leviku eest | 8.10 Protection against the Spread of Fire |
| 8.11. Kaitse vee ja vedelike eest | 8.11 Water/Liquid Protection |
| 8.12. Ohtude avastamine ja teatamine | 8.12 Hazard Detection and Reporting |
| 8.13. Äikesekaitse | 8.13 Lightning Protection |
| 8.14. Aparatuuri kaitse varguse eest | 8.14 Protection of Equipment against Theft |
| 8.15. Keskkonna kaitse | 8.15 Protection of the Environment |
| 8.16. Teeninduse ja hoolduse reguleerimine | 8.16 Service and Maintenance Control |
| 9. Personali turve | 9. Personnel Security |
| 9.1. Sissejuhatus | 9.1 Introduction |
| 9.2. Palkamistingimused | 9.2 Terms of Employment |
| 9.3. Turvateadlikkus ja -koolitus | 9.3 Security Awareness and Training |
| 9.4. Töötajad | 9.4 Employees |
| 9.5. Lepingulised töötajad | 9.5 Self-employed people under contract |
| 9.6. Kolmandad osapooled | 9.6 Third parties |
| 10. Dokumentide ja andmekandjate turve | 10. Document/Media Security |
| 10.1. Sissejuhatus | 10.1 Introduction |
| 10.2. Dokumentide turve | 10.2 Document Security |
| 10.3. Andmekandjate säilitus | 10.3 Storage of Media |
| 10.4. Andmekandjate kõrvaldamine | 10.4 Disposal of Media |

| | |
|--|---|
| 11. Tegevuseatkematus, sh ootamatuste plaanimise ja avariijärgse taaste, strateegia ja plaan(id) | 11. Business Continuity, including Contingency Planning/Disaster Recovery, Strategy and Plan(s) |
| 11.1. Sissejuhatus | 11.1 Introduction |
| 11.2. Varundamine | 11.2 Back-Up |
| 11.3. Tegevuse atkematus strateegia | 11.3 Business Continuity Strategy |
| 11.4. Tegevuse atkematus plaan(id) | 11.4 Business Continuity Plan(s) |
| 12. Kaugtöö | 12. Teleworking |
| 13. Alltöövõtu poliitika | 13. Outsourcing Policy |
| 13.1. Sissejuhatus | 13.1 Introduction |
| 13.2. Turvanõuded | 13.2 Security Requirements |
| 14. Muudatuste reguleerimine | 14. Change Control |
| 14.1. Tagasiside | 14.1 Feedback |
| 14.2. Turvapoliitika muudatused | 14.2 Changes to the Security Policy |
| 14.3. Käesoleva dokumendi staatus | 14.3 Status of the Document |
| Lisad | Appendices |
| A. Turvajuhendite loend | A. List of Security Guides |
| B. Seadused ja eeskirjad | B. Legislation and Regulation |
| C. Asutuse infoturbe ametniku pädevus | C. Corporate IT Security Officer Terms of Reference |
| D. Infoturbe foorumi või komitee pädevus | D. Terms of Reference for IT Security Forum or Committee |
| E. Infotehnoloogilise süsteemi turvapoliitika sisukord | E. Contents of an IT System Security Policy |
| Allikas: EVS-ISO/IEC TR 13335-3:1999 LISA A | |