

---

## EXAMPLE OF CONTENTS LIST FOR AN AGENCY/DEPARTMENT ICT SECURITY POLICY

1. Introduction
  - 1.1 Overview
  - 1.2 Scope and Purpose of the ICT 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
  - 6.6 PC Security
  - 6.7 Laptop Security

- 7. Communications Security
  - 7.1 Introduction
  - 7.2 The Networking Infrastructure
  - 7.3 Internet
  - 7.4 Encryption/Message Authentication
- 8. Physical Security
  - 8.1 Introduction
  - 8.2 Location of Facilities
  - 8.3 Building Security and Protection
  - 8.4 Protection of Building Services
  - 8.5 Protection of Supporting Services
  - 8.6 Unauthorised Occupation
  - 8.7 PC/Workstation Accessibility
  - 8.8 Access to Magnetic Media
  - 8.9 Protection of Staff
  - 8.10 Protection against the Spread of Fire
  - 8.11 Water/Liquid Protection
  - 8.12 Hazard Detection and Reporting
  - 8.13 Lightning Protection
  - 8.14 Protection of Equipment against Theft
  - 8.15 Protection of the Environment
  - 8.16 Service and Maintenance Control
- 9. Personnel Security
  - 9.1 Introduction
  - 9.2 Terms of Employment
  - 9.3 Security Awareness and Training
  - 9.4 Employees
  - 9.5 Self-employed People under Contract
  - 9.6 Third parties
- 10. Document/Media Security
  - 10.1 Introduction
  - 10.2 Document Security
  - 10.3 Storage of Media
  - 10.4 Disposal of Media

- 11. Business Continuity, including Contingency Planning/Disaster Recovery, Strategy and Plan(s)
  - 11.1 Introduction
  - 11.2 Back-Up
  - 11.3 Business Continuity Strategy
  - 11.4 Business Continuity Plan(s)
- 12. Telecommuting
- 13. Outsourcing Policy
  - 13.1 Introduction
  - 13.2 Security Requirements
- 14. Change Control
  - 14.1 Feedback
  - 14.2 Changes to the Security Policy
  - 14.3 Status of the Document

Source: ISO/IEC 13335 Part 3