Appendix D

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

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