The suggested contents for a security policy are shown below. Each heading requires a policy statement to be developed detailing the organisation's policy in respect of each item.

1.0 SECURITY POLICY

1.1 Information Security Policy

  Information security policy
  Communication to employees

1.2 Information Security Policy Review

  Information security policy review
  Independent review of information security policy

2.0 ORGANISATION OF INFORMATION SECURITY

2.1 Internal Organisation

  Senior management support
  Information security responsibilities

2.2 External Parties

  Third party risks
  Customer access to information

3.0 ASSET MANAGEMENT

3.1 Assets

  Up to inventory
  Ownership of assets

3.2 Information Classification

  Defining information
  Classifying information
  Labelling information

4.0 HUMAN RESOURCES SECURITY

4.1 Prior to Employment

  Define roles and responsibilities
  Preparing terms and conditions of employment
  Security vetting
4.2 **During Employment**

- Security policies and procedures
- Information security awareness
- Information Security Officer training
- User information security training
- Technical Staff information security training
- Third party contractor awareness programmes
- Providing regular information updates to staff
- Acceptable usage policy
- Disciplinary processes

4.3 **Staff Leaving Employment**

- Handling staff resignations
- Procedures for terminating staff or contractors
- Removal of access rights

5.0 **PHYSICAL AND ENVIRONMENTAL SECURITY**

5.1 **Secure Areas**

- Securing physical protection of computer premises
- High security locations
- Delivery and loading areas
- Ensuring suitable environmental conditions
- Physical access control to secure areas
- Environmental and other external threats

5.2 **Equipment Security**

- Uninterruptable power supplies
- Encryption
- Disposal procedure

6.0 **COMMUNICATIONS AND OPERATIONS MANAGEMENT**

6.1 **Operational Procedures and Responsibilities**

- Documented procedures
- Change management process
- System use procedures
- Appointing system administrators

6.2 **Third Party Service Delivery**

- Security controls
- Service monitoring
- Third party access agreement
- Service level agreements
- Scope and methods of work
6.3 Systems Planning and Acceptance

- Capacity planning
- Performance Monitoring
- Product lifecycle
- Acceptance tests

6.4 Protection against mobile code

- Anti-virus software
- Internet threat databases
- Email filtering
- Firewalls

6.5 Backups

- Backup policy
- Archiving Information
- Backing up data on portable computers
- Managing backup and recovery procedures
- Recovery of data files

6.6 Network Security Management

- Network configuration
- Managing the network
- Controlling shared networks
- Routing controls
- Network security
- Accessing the network remotely
- Time-out facility
- Synchronising network time

6.7 Media Handling

- Removable media management
- Media encryption
- Media disposal
- Managing hard copy printouts
- Photocopying confidential information
- Filing of documents and information
- Transporting sensitive documents
- Shredding of unwanted hardcopy
- Clear desk policy

6.8 Exchange of Information

- Information sharing agreements
- Protection of information in transit

6.9 Electronic Commerce

- Securing e-Commerce systems and web sites
- Using external service providers for e-Commerce
- Protecting online transactions
- Publicly available information
6.10 Monitoring

Maintain audit logs
System clock synchronisation

7.0 ACCESS CONTROL

7.1 Requirement for Access Control

Access control policy
Access control standard
Business application security

7.2 User Access Management

Managing User Access
Starter process
Leaver process
Access Control Framework
Managing Passwords
Review of user access

7.3 User Responsibilities

Password policy
Securing Unattended Workstations
Clear desk policy

7.4 Network Access Control

Managing Network Access Controls
Controlling Remote User Access
Control of configuration ports
Node authentication
Restricting Access

7.5 Operating System Access Control

User identification
User authentication
Password management
Session timeout

7.6 Application and Information Access Control

User identification
User authentication
Password management
Session timeout
Sensitive information control

7.7 Mobile computing and teleworking

Home working policy
Flexible working policy
Mobile working security
Using mobile phones
Issuing laptop / portable computers to personnel
Using laptop / portable computers
8.0 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, MAINTENANCE

8.1 Security Requirements of Information Systems

Specification includes security requirements

8.2 Correct processing

Input data validation
Output data validation
Internal processing controls

8.3 Cryptographic controls

Key management
Certificate authorities
Digital certificates
Key control

8.4 Security of System Files

Control of software installation
Protection of source code
Controlling test environments

8.5 Security in development and support process

Formal change control procedure
Software development

8.6 Technical Vulnerability Management

Awareness of current vulnerabilities
Vulnerability scanning
Patch management

9.0 Information Security Incident Management

9.1 Reporting Information Security Events and Weaknesses

Reporting information security events policy
Reporting Information security incidents
Reporting incidents to outside authorities
Witnessing an Information Security Breach
Reporting security weaknesses policy
Software Errors and Weaknesses
Notifying Information Security Weaknesses
Being Alert for Fraudulent Activities

9.2 Management of Information Security Incidents

Responsibilities
Responding to information security incidents
Investigating the cause and impact of incidents
Collecting evidence of an information security breach
Establishing remedies to information security breaches
10.0 BUSINESS CONTINUITY MANAGEMENT

10.1 Business Continuity Management

- Initiating the business continuity project
- Assessing the business continuity security risk
- Developing the business continuity plan
- Testing the business continuity plan
- Training and staff awareness on business continuity
- Maintaining and updating the business continuity plan

11.0 COMPLIANCE

11.1 Compliance with legal requirements

- Being aware of legal obligations
- Copyright legislation
- Software licensing
- Data protection or equivalent
- Safeguards against computer misuse
- Renewing domain name licenses

11.2 Compliance with Security Standards and Policies

- Implementation of security procedures
- Scheduled checking to ensure compliance with policies

11.3 Information Systems Audit Considerations

- Planning to minimise risk of disruption
- Protection of system audit tools

Copyright © Ruskwig – Ruskwig provides you with the right to copy and amend this document for your own use – You may not resell, ask for donations for, or otherwise transfer for value the document.