

# 2013 ISO 27002

Translated into Plain English

ISO 27002 is a comprehensive information security management standard. It has fourteen sections (5 to 18) each of which is structured in the same way. Each section begins with one or more information security objectives. It then introduces the controls that could be used to achieve these objectives and explains how they can be implemented. The following material presents a brief overview of this important information security standard.

## 5. Security Policy Management

### 5.1 Provide management direction and support

- 5.1.1 Develop your information security policies
- 5.1.2 Review your information security policies

## 6. Corporate Security Management

### 6.1 Establish an internal information security organization

- 6.1.1 Allocate information security roles and responsibilities
- 6.1.2 Segregate conflicting duties and responsibilities
- 6.1.3 Maintain contact with all relevant authorities
- 6.1.4 Establish relationships with external organizations
- 6.1.5 Make information security part of project management

### 6.2 Protect your organization's mobile devices and telework

- 6.2.1 Establish a mobile device security risk management policy
- 6.2.2 Establish a teleworking security management policy

## 7. Personnel Security Management

### 7.1 Emphasize security prior to employment

- 7.1.1 Verify the backgrounds of all new personnel
- 7.1.2 Use contracts to protect your information

### 7.2 Emphasize security during employment

- 7.2.1 Expect your managers to emphasize security
- 7.2.2 Deliver information security awareness programs
- 7.2.3 Set up a disciplinary process for security breaches

### 7.3 Emphasize security at termination of employment

- 7.3.1 Emphasize post-employment security requirements

## 8. Organizational Asset Management [DETAILED PDF SAMPLE](#)

### 8.1 Establish responsibility for corporate assets

- 8.1.1 Compile an inventory of assets associated with information
- 8.1.2 Select owners for all assets associated with your information
- 8.1.3 Prepare acceptable use rules for assets associated with information
- 8.1.4 Return all assets associated with information upon termination

### 8.2 Develop an information classification scheme

- 8.2.1 Classify your organization's information
- 8.2.2 Establish information labeling procedures
- 8.2.3 Develop asset handling procedures

### 8.3 Control how physical media are handled

- 8.3.1 Manage removable media
- 8.3.2 Manage the disposal of media
- 8.3.3 Manage the transfer of media

## 9. Information Access Management

### 9.1 Respect business requirements

- 9.1.1 Develop a policy to control access to information
- 9.1.2 Control access to networks and network services

### 9.2 Manage all user access rights

- 9.2.1 Develop a user registration process
- 9.2.2 Set up a user access provisioning process
- 9.2.3 Restrict the use of privileged access rights
- 9.2.4 Control secret authentication information
- 9.2.5 Review access rights at regular intervals
- 9.2.6 Remove or adjust user access rights

### 9.3 Protect user authentication

- 9.3.1 Protect secret authentication information

### 9.4 Control access to systems

- 9.4.1 Restrict access to information and applications
- 9.4.2 Use secure log-on procedures to control access
- 9.4.3 Use formal password management systems
- 9.4.4 Control the use of utility programs
- 9.4.5 Control access to source code

## 10. Cryptography Policy Management

### 10.1 Control the use of cryptographic controls and keys

- 10.1.1 Implement a cryptographic control policy
- 10.1.2 Implement a cryptographic key policy

## 11. Physical Security Management

### 11.1 Establish secure areas to protect assets

- 11.1.1 Create physical security perimeters to protect areas
- 11.1.2 Use physical entry controls to protect secure areas
- 11.1.3 Secure your organization's offices, rooms, and facilities
- 11.1.4 Protect information and facilities from external threats
- 11.1.5 Develop procedures to control work in secure areas
- 11.1.6 Prevent unauthorized persons from accessing premises

### 11.2 Protect your organization's equipment

- 11.2.1 Use siting techniques to protect equipment and assets
- 11.2.2 Safeguard equipment from supporting utility failures
- 11.2.3 Secure your power and telecommunications cables
- 11.2.4 Ensure that your equipment is correctly maintained
- 11.2.5 Restrict the removal of assets to off-site locations
- 11.2.6 Regulate the off-site use of equipment and assets
- 11.2.7 Control the disposal and re-use of storage media
- 11.2.8 Expect users to protect unattended equipment
- 11.2.9 Establish a clear-desk and clear-screen policy

## 12. Operational Security Management

### 12.1 Establish procedures and responsibilities

- 12.1.1 Document and use your operating procedures
- 12.1.2 Control changes that affect information security
- 12.1.3 Monitor usage and carry out capacity planning
- 12.1.4 Keep your operational environment separate

### 12.2 Protect your organization from malware

- 12.2.1 Implement controls to manage malware

### 12.3 Make backup copies on a regular basis

- 12.3.1 Control how backups are carried out

### 12.4 Use logs to record security events

- 12.4.1 Establish information security event logs
- 12.4.2 Protect logging facilities and log information
- 12.4.3 Record administrator and operator activities
- 12.4.4 Synchronize clocks to a single reference source

### 12.5 Control your operational software

- 12.5.1 Control installation of operational software

### 12.6 Address your technical vulnerabilities

- 12.6.1 Manage your technical vulnerabilities
- 12.6.2 Establish software installation rules

### 12.7 Minimize the impact of audit activities

- 12.7.1 Control how audit activities are carried out

## 13. Network Security Management

### 13.1 Protect networks and facilities

- 13.1.1 Establish network security controls
- 13.1.2 Control network service providers
- 13.1.3 Use segregation to protect networks

### 13.2 Protect information transfers

- 13.2.1 Develop information transfer policies and procedures
- 13.2.2 Establish security information transfer agreements
- 13.2.3 Protect information sent using electronic messaging
- 13.2.4 Use confidentiality agreements to protect information

## 14. System Security Management

### 14.1 Make security an inherent part of information systems

- 14.1.1 Consider security when changing or acquiring systems
- 14.1.2 Protect application services on all public networks
- 14.1.3 Safeguard your application service transactions

### 14.2 Protect and control system development activities

- 14.2.1 Establish rules to control internal software development
- 14.2.2 Use formal procedures to control changes to systems
- 14.2.3 Review applications after operating platform changes
- 14.2.4 Restrict and control changes to software packages
- 14.2.5 Establish and use secure system engineering principles
- 14.2.6 Establish and protect secure development environments
- 14.2.7 Control outsourced system development projects
- 14.2.8 Test security functionality during development cycle
- 14.2.9 Use acceptance criteria to test information systems

### 14.3 Safeguard data used for system testing purposes

- 14.3.1 Control and protect data used for system testing

## 15. Supplier Relationship Management

### 15.1 Establish security agreements with suppliers

- 15.1.1 Expect suppliers to comply with risk mitigation agreements
- 15.1.2 Expect suppliers to comply with information security agreements
- 15.1.3 Expect suppliers to deal with their own supply chain security risks

### 15.2 Manage supplier security and service delivery

- 15.2.1 Manage supplier services and supplier security
- 15.2.2 Manage changes to services provided by suppliers

## 16. Security Incident Management

### 16.1 Identify and respond to information security incidents

- 16.1.1 Establish incident response procedures and responsibilities
- 16.1.2 Report information security events as quickly as possible
- 16.1.3 Identify and report all information security weaknesses
- 16.1.4 Assess your security events and decide if they are incidents
- 16.1.5 Follow procedures when you respond to security incidents
- 16.1.6 Learn from security incidents and apply your knowledge
- 16.1.7 Collect evidence to document incidents and responses

## 17. Security Continuity Management

### 17.1 Establish information security continuity controls

- 17.1.1 Plan how information security will continue during a disaster
- 17.1.2 Implement your approach to information security continuity
- 17.1.3 Verify the effectiveness of your security continuity controls

### 17.2 Build redundancies into information processing facilities

- 17.2.1 Use redundancies to ensure information processing continuity

## 18. Security Compliance Management

### 18.1 Comply with legal security requirements

- 18.1.1 Identify and comply with legal security requirements
- 18.1.2 Respect intellectual property rights and requirements
- 18.1.3 Meet all appropriate record protection requirements
- 18.1.4 Protect privacy and personally identifiable information
- 18.1.5 Regulate the use of cryptographic methods and controls

### 18.2 Carry out security compliance reviews

- 18.2.1 Perform independent reviews of information security
- 18.2.2 Review compliance with security policies and standards
- 18.2.3 Conduct technical information security compliance reviews

If you like our approach, please consider [Purchasing our Plain English Products.](#)

**Praxiom Research Group Limited**  
First Edmonton Place 14 Floor 10665 Jasper Ave  
Edmonton, Alberta, Canada, T5J 3S9 780-461-4514  
info@praxiom.com info@praxiom.org praxiom@gmail.com  
We ship worldwide. Our products are used in over 100 countries.

©2022 Praxiom Research Group Limited. All Rights Reserved.