



**<ORGANIZATION>**  
**Information Security**  
**Policy Manual**

Draft version 7, June 2009

**SAMPLE EXTRACTED PURELY FOR PRODUCT EVALUATION**

Security principles and axioms approved by the Executive Directors on: ... *[not yet approved]*

Policies approved by the Chief Information Officer on: ... *[not yet approved]*

The generic information security policy manual based on ISO/IEC 27002:2005 is copyright © 2009 IsecT Ltd. Consult your license agreement for the terms and conditions of use. **The generic manual *must not* be distributed to third parties unless explicitly permitted in the license.**

## **Statement of support from the Managing Director / Chief Executive Officer**

Information is an extremely valuable and important corporate asset that requires protection against risks that would threaten its confidentiality, integrity and/or availability. Suitable information security controls must therefore be selected and implemented. The security controls identified in this manual are based on ISO/IEC standards that document internationally-accepted good practice. **Along with my colleagues on the senior management team, I fully endorse this information security policy manual and expect the controls to be implemented consistently throughout <ORGANIZATION>.**

Signed: Joe Bloggs, MD/CEO, <ORGANIZATION>

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

***AUTHOR'S NOTE:** The statement above is a "straw man", a suggestion to get you started. Discussing and working on this with the MD/CEO and other executives is an opportunity to raise their awareness of the value of information security and get them engaged with the implementation of ISO/IEC 27002. Do not underestimate the value of this explicit management endorsement!*

### **Disclaimer of Warranty and Liability**

This is not legal or professional advice. This Manual, including its appendix, is provided for general information purposes only. The manual provides various types and levels of information about compliance with standards, laws, regulations and practices. Information is not the same as advice. The application of law to individual circumstances must be addressed in each unique situation. IsecT Ltd. is not engaged in rendering legal, tax or other professional advice or services. IsecT Ltd. does not purport to identify all conceivable compliance requirements or recommended security controls. It is the responsibility of each organization to understand which information security, legal, accounting and other compliance requirements apply to its activities. Users of this Manual are advised to seek specific advice from suitably qualified practitioners. Using the Manual or any part thereof does not create a lawyer-client relationship or any other type of professional relationship with IsecT Ltd.

While IsecT Ltd. attempts to provide accurate, complete and up to date content, errors and omissions may occur. This product is offered "as is". IsecT Ltd. makes no representations or warranties regarding the completeness, accuracy or timeliness of the contents, and disclaims all implied warranties (including merchantability, fitness for a particular purpose and non-infringement) and all liability for any loss, damage or claim, whether due to an error or omission or otherwise.

To the fullest extent permitted by applicable law, IsecT Ltd. does not warrant or guarantee the quality, accuracy or completeness of any information on this Manual. IsecT Ltd. shall not be liable for any damages or costs, including any direct, consequential, incidental, indirect, punitive or special damages (including loss of profits, data, business or good will) in connection with use of this Manual, whether or not liability is based on breach of contract, tort, strict liability, breach of warranty, failure of essential purpose or otherwise, and even if a party is advised of the likelihood of such damages.

# Contents

- 1 Scope..... 9**
  - 1.1 Introduction and objectives..... 9**
  - 1.2 Status and applicability ..... 9**
  - 1.3 Intended audience ..... 10**
  - 1.4 Policy exceptions ..... 10**
    - 1.4.2 Routine policy exceptions ..... 10
    - 1.4.3 Emergency policy exceptions ..... 11
  - 1.5 Origin, structure and design of this manual ..... 11**
    - 1.5.1 Origin in ISO/IEC 27002 ..... 11
    - 1.5.2 Structure and overview ..... 12
    - 1.5.3 Formatting and presentation ..... 13
  - 1.6 References ..... 13**
  - 1.7 Document change control ..... 15**
- 2 Terms and definitions ..... 17**
  - 2.1 <ORGANIZATION> information security glossary ..... 17**
- 3 Structure of this manual ..... 44**
  - 3.1 Policy hierarchy..... 44**
  - 3.2 Layers in the policy hierarchy..... 45**
    - 3.2.1 Guiding principles ..... 45
    - 3.2.2 Axioms ..... 45
    - 3.2.3 Policies ..... 45
    - 3.2.4 Standards ..... 45
    - 3.2.5 Procedures ..... 45
    - 3.2.6 Guidelines..... 45
- 4 Risk assessment and treatment ..... 46**
  - 4.1 Assessing security risks ..... 46**
  - 4.2 Treating security risks ..... 46**
- 5 Security policy ..... 48**
  - 5.1 Information security policy..... 48**
    - 5.1.1 This Information Security Policy Manual..... 48
    - 5.1.2 Review of the Information Security Policy Manual..... 49
- 6 Organization of information security ..... 51**
  - 6.1 Internal organization ..... 51**
    - 6.1.1 Management commitment to information security ..... 52
    - 6.1.2 Information security co-ordination..... 52
    - 6.1.3 Allocation of information security responsibilities ..... 53
    - 6.1.4 Authorization process for information processing facilities ..... 55
    - 6.1.5 Confidentiality agreements ..... 55

- 6.1.6 Contact with authorities ..... 56
- 6.1.7 Contact with special interest groups ..... 56
- 6.1.8 Independent review of information security ..... 56
- 6.2 External parties ..... 57**
  - 6.2.1 Identification of risks related to external parties..... 57
  - 6.2.2 Addressing security when dealing with customers ..... 59
  - 6.2.3 Addressing security in third party agreements..... 60
- 7 Asset management ..... 62**
  - 7.1 Responsibility for assets ..... 62**
    - 7.1.1 Inventory of assets..... 62
    - 7.1.2 Ownership of assets ..... 62
    - 7.1.3 Acceptable use of assets..... 63
  - 7.2 Information classification ..... 63**
    - 7.2.1 Classification guidelines ..... 63
    - 7.2.2 Information labeling and handling..... 64
- 8 Human resources security ..... 65**
  - 8.1 Prior to employment ..... 65**
    - 8.1.1 Rôles and responsibilities ..... 65
    - 8.1.2 Screening..... 65
    - 8.1.3 Terms and conditions of employment..... 66
  - 8.2 During employment..... 67**
    - 8.2.1 Management responsibilities ..... 67
    - 8.2.2 Information security awareness, education and training..... 67
    - 8.2.3 Disciplinary process..... 67
  - 8.3 Termination or change of employment ..... 68**
    - 8.3.1 Termination responsibilities ..... 68
    - 8.3.2 Return of assets..... 68
    - 8.3.3 Removal of access rights..... 68
- 9 Physical and environmental security ..... 70**
  - 9.1 Secure areas ..... 70**
    - 9.1.1 Physical security perimeter..... 70
    - 9.1.2 Physical entry controls..... 70
    - 9.1.3 Securing offices, rooms and facilities ..... 71
    - 9.1.4 Protecting against external and environmental threats..... 71
    - 9.1.5 Working in secure areas ..... 72
    - 9.1.6 Public access, delivery and loading areas..... 72
  - 9.2 Equipment security ..... 73**
    - 9.2.1 Equipment siting and protection ..... 73
    - 9.2.2 Supporting utilities ..... 73
    - 9.2.3 Cabling security ..... 74
    - 9.2.4 Equipment maintenance ..... 74

9.2.5 Security of equipment off-premises ..... 74

9.2.6 Secure disposal or re-use of equipment ..... 75

9.2.7 Removal of property ..... 75

**10 Communications and operations management ..... 76**

**10.1 Operational procedures and responsibilities ..... 76**

10.1.1 Documented operating procedures ..... 76

10.1.2 Change management ..... 76

10.1.3 Segregation of duties ..... 77

10.1.4 Separation of development, test and operational facilities ..... 77

**10.2 Third party service delivery management..... 78**

10.2.1 Service delivery ..... 78

10.2.2 Monitoring and review of third party services ..... 78

10.2.3 Managing changes to third party services ..... 78

**10.3 System planning and acceptance..... 79**

10.3.1 Capacity management..... 79

10.3.2 System acceptance ..... 79

**10.4 Protection against malicious and mobile code ..... 80**

10.4.1 Controls against malicious code ..... 80

10.4.2 Controls against mobile code ..... 80

**10.5 Back-up ..... 81**

10.5.1 Information back-up ..... 81

**10.6 Network security management ..... 82**

10.6.1 Network controls ..... 82

10.6.2 Security of network services ..... 83

**10.7 Media handling ..... 83**

10.7.1 Management of removable media ..... 83

10.7.2 Disposal of media ..... 83

10.7.3 Information handling procedures ..... 84

10.7.4 Security of system documentation ..... 84

**10.8 Exchange of information ..... 85**

10.8.1 Information exchange policies and procedures ..... 85

10.8.2 Exchange agreements..... 86

10.8.3 Physical media in transit ..... 86

10.8.4 Electronic messaging..... 86

10.8.5 Business information systems ..... 87

**10.9 Electronic commerce services..... 87**

10.9.1 Electronic commerce ..... 87

10.9.2 Online transactions ..... 87

10.9.3 Publicly available systems ..... 88

**10.10 Monitoring..... 88**

10.10.1 Audit logging ..... 88

- 10.10.2 Monitoring system use..... 88
- 10.10.3 Protection of log information ..... 89
- 10.10.4 Administrator and operator logs..... 89
- 10.10.5 Fault logging ..... 89
- 10.10.6 Clock synchronization ..... 89
- 11 Access control..... 90**
  - 11.1 Business requirement for access control..... 90**
    - 11.1.1 Access control policy ..... 90
  - 11.2 User access management ..... 90**
    - 11.2.1 User registration ..... 90
    - 11.2.2 Privilege management ..... 91
    - 11.2.3 User password management..... 92
    - 11.2.4 Review of user access rights ..... 92
  - 11.3 User responsibilities ..... 93**
    - 11.3.1 Password use ..... 93
    - 11.3.2 Unattended user equipment ..... 93
    - 11.3.3 Clear desk and clear screen policy ..... 94
  - 11.4 Network access control ..... 94**
    - 11.4.1 Policy on use of network services..... 94
    - 11.4.2 User authentication for external connections..... 95
    - 11.4.3 Equipment identification in networks ..... 96
    - 11.4.4 Remote diagnostic and configuration port protection ..... 96
    - 11.4.5 Segregation in networks ..... 96
    - 11.4.6 Network connection control ..... 97
    - 11.4.7 Network routing control..... 97
  - 11.5 Operating system access control..... 98**
    - 11.5.1 Secure logon procedures..... 98
    - 11.5.2 User identification and authentication..... 98
    - 11.5.3 Password management system..... 99
    - 11.5.4 Use of system utilities ..... 99
    - 11.5.5 Session time-out ..... 99
    - 11.5.6 Limitation of connection time ..... 100
  - 11.6 Application and information access control..... 100**
    - 11.6.1 Information access restriction ..... 100
    - 11.6.2 Sensitive system isolation..... 101
  - 11.7 Mobile computing and teleworking ..... 101**
    - 11.7.1 Mobile computing..... 101
    - 11.7.2 Teleworking ..... 102
- 12 Information systems acquisition, development and maintenance. 103**
  - 12.1 Security requirements of information systems ..... 103**
    - 12.1.1 Security requirements analysis and specification ..... 103

- 12.2 Correct processing in applications ..... 105**
  - 12.2.1 Input data validation..... 105
  - 12.2.2 Control of internal processing ..... 106
  - 12.2.3 Message integrity..... 106
  - 12.2.4 Output data validation ..... 107
- 12.3 Cryptographic controls..... 107**
  - 12.3.1 Policy on use of cryptographic controls ..... 107
  - 12.3.2 Key management..... 108
- 12.4 Security of system files ..... 109**
  - 12.4.1 Control of operational software ..... 109
  - 12.4.2 Protection of system test data ..... 110
  - 12.4.3 Access control to program source code ..... 110
- 12.5 Security in development and support activities..... 110**
  - 12.5.1 Change control procedures ..... 110
  - 12.5.2 Technical review of applications after operating system changes ..... 111
  - 12.5.3 Restrictions on changes to software packages ..... 111
  - 12.5.4 Information leakage ..... 112
  - 12.5.5 Outsourced software development ..... 112
- 12.6 Technical vulnerability management..... 113**
  - 12.6.1 Control of technical vulnerabilities ..... 113
- 13 Information security incident management..... 114**
  - 13.1 Reporting information security events and weaknesses ..... 114**
    - 13.1.1 Reporting information security events ..... 114
    - 13.1.2 Reporting security weaknesses ..... 115
  - 13.2 Management of information security incidents and improvements..... 116**
    - 13.2.1 Responsibilities and procedures ..... 116
    - 13.2.2 Learning from information security incidents ..... 117
    - 13.2.3 Collection of evidence..... 117
- 14 Business continuity management ..... 119**
  - 14.1 Information security aspects of business continuity management ..... 119**
    - 14.1.1 Including information security in the business continuity management process 119
    - 14.1.2 Business continuity and risk assessment ..... 119
    - 14.1.3 Developing and implementing continuity plans including information security .. 120
    - 14.1.4 Business continuity planning framework..... 120
    - 14.1.5 Testing, maintaining and re-assessing business continuity plans ..... 121
- 15 Compliance ..... 123**
  - 15.1 Compliance with legal requirements ..... 123**
    - 15.1.1 Identification of applicable legislation ..... 123
    - 15.1.2 Intellectual property rights (IPR) ..... 123
    - 15.1.3 Protection of organizational records ..... 125
    - 15.1.4 Data protection and privacy of personal information ..... 126

---

|                   |   |            |
|-------------------|---|------------|
| 15.1.5            | Prevention of misuse of information processing facilities .....                   | 127        |
| 15.1.6            | Regulation of cryptographic controls .....  | 127        |
| <b>15.2</b>       | <b>Compliance with security policies and standards and technical compliance .</b> | <b>128</b> |
| 15.2.1            | Compliance with security policies and standards .....                             | 128        |
| 15.2.2            | Technical compliance checking .....   | 128        |
| <b>15.3</b>       | <b>Information systems audit considerations .....</b>                             | <b>128</b> |
| 15.3.1            | Information system audit controls .....   | 128        |
| 15.3.2            | Protection of information systems audit tools .....                               | 129        |
| <b>Appendix A</b> | <b>Fundamental information security principles.....</b>                           | <b>130</b> |

# 1 Scope

## 1.1 Introduction and objectives

1.1.1.1 Through a comprehensive suite of information security control objectives and supporting policy statements, this manual explains how ISO/IEC 27002, the international standard code of practice for information security management, applies within <ORGANIZATION>. Its purpose is to communicate management directives and standards of care to ensure consistent and appropriate protection of information throughout <ORGANIZATION>. It can be used as part of an Information Security Management System as specified in ISO/IEC 27001 and related standards.

## 1.2 Status and applicability

1.2.1.1 This manual has been reviewed and approved by the Chief Information Officer (CIO), IT managers and the Chief Security Officer (CSO). The axioms (formal policy statements) embedded throughout the manual and the guiding principles listed in [Appendix A](#) have been approved by the Executive Directors to apply throughout <ORGANIZATION>.

1.2.1.2 It is applicable:

- Throughout <ORGANIZATION> including any subsidiaries and joint ventures in which <ORGANIZATION> has a controlling interest;
- At all <ORGANIZATION> locations in all countries;
- To all <ORGANIZATION> employees and others working on behalf of <ORGANIZATION> in a similar capacity including contractors, consultants, temporary workers, student placements *etc.* (known collectively throughout as “workers”);
- To all information/data, information processing/computer systems and networks (collectively known as “information assets”) owned by <ORGANIZATION>, or those entrusted to <ORGANIZATION> by third parties.

1.2.1.3 It supersedes previous versions of the <ORGANIZATION> Information Security Policy Manual.

1.2.1.4 The axioms and other policy statements in this manual are supported by a range of security controls documented within operating procedures, technical controls embedded in information systems and other controls advised to employees from time to time by management through information security standards, procedures and guidelines. The supporting controls refer to, and gain authority from, the information security policy statements included in this manual.

## 1.3 Intended audience

1.3.1.1 This policy manual is primarily intended for use by:

- **“Workers”**\* comprising all <ORGANIZATION> employees (including managers, staff, temporary employees such as student placements) and third parties (such as consultants, contractors, support/maintenance staff) acting in a similar capacity. Workers are broadly informed of <ORGANIZATION>’s main information security requirements through this manual and are specifically informed of any that are directly relevant to their activities through the associated security awareness activities, terms and conditions of employment, management briefings *etc.*;
- **Information technologists** including professionals working within Information Technology department such as Security Administration, Operations, Applications Development, IT Help/Service Desk *etc.* and others IT and knowledge workers within business departments. They use this document as a reference when specifying, designing, building and operating technical, physical and procedural information security controls relating to <ORGANIZATION> information systems and networks;
- **Managers** – the policy manual comprises a set of corporate policy statements and guidance on important information security matters that <ORGANIZATION> managers need to understand and support, especially given their governance responsibilities;
- **Corporate functions** such as Internal Audit, Human Resources, Risk Management, Compliance and Legal who use the manual both to promote and assess compliance with corporate information security policy, and to blend information security controls seamlessly with other forms of control and governance;
- **Third parties** such as business partners, external auditors and industry regulators who refer to the manual to understand <ORGANIZATION>’s overall information security position and, where appropriate, to evaluate or direct the operation of specific information security controls to meet their contractual obligations.

## 1.4 Policy exceptions

1.4.1.1 Despite the care that has been taken in authoring, reviewing and approving this policy manual, the authors cannot possibly foresee all possible circumstances or situations in which it might apply. It is therefore conceivable that exceptional situations or emergencies may occur when practical considerations clearly override or negate the policy statements made herein. Examples include the introduction of new legal or regulatory obligations that conflict with specific policy statements, or where slavishly following the policies to the letter would cause unacceptable health and safety risks.

### 1.4.2 Routine policy exceptions

1.4.2.1 Under normal circumstances where someone identifies a situation in which these policies cannot apply for some reason, it is their responsibility to raise the matter with management. Management, in conjunction with the Information Security Manager, relevant Information Asset Owner/s and other stakeholders, will take an explicit risk-based decision on whether to permit or deny such policy exceptions.

---

\* Note: “Workers” is merely a convenient inclusive term and is not meant to imply that others do not work!

- 1.4.2.2 Where a policy exception is permitted, the person requesting the exception (*i.e.* a manager, normally also an Information Asset Owner) will explicitly assume personal accountability for any security incidents that arise as a direct result of the exception. If, for example, a given IT system cannot be configured to enforce the password length and complexity rules stated in [section 11.3.1](#), the corresponding Information Asset Owner may request a policy exception but will be held to account for any security incidents arising from user authentication failures or incidents as a result of the policy exception.
- 1.4.2.3 The Information Security Manager is responsible for recording exceptions in the exceptions database, and for following-up with the Information Asset Owners at least once a year to assess progress towards resolving the issue that resulted in the need for an exception.

### 1.4.3 Emergency policy exceptions

- 1.4.3.1 Where justified and necessary under exceptional circumstances, limited policy exceptions may be made without prior management approval. Where prior notification and acceptance of policy exceptions is not possible (for example in an emergency), exceptions *must* however be reported to the Information Security Manager as soon as possible thereafter (within a few working days at most) for retrospective processing under the routine policy exceptions process noted above.
- 1.4.3.2 **Deliberate non-compliance with one or more information security policies that has not been notified to and agreed by the Information Security Manager under the terms noted in sections 1.4.2 or 1.4.3 may be treated as a disciplinary matter.**
- 1.4.3.3 By definition, emergency exceptions are not anticipated to be routine in nature. Where the need for policy exceptions arise under routine circumstances in the normal course of business, the routine policy exceptions process noted in section 1.4.2 must be followed.

## 1.5 Origin, structure and design of this manual

### 1.5.1 Origin in ISO/IEC 27002

- 1.5.1.1 In line with a senior management decision, this manual reflects ISO/IEC 27002:2005, an international information security management standard. ISO/IEC 27002 is a 'code of practice' meaning that it contains best practice advice rather than mandating specific security controls that an organization must implement. Organizations that adopt ISO/IEC 27002 must evaluate their own control requirements based on an analysis of the risks to their information assets and the corresponding control objectives.
- 1.5.1.2 Some 39 generic control objectives and literally hundreds of suggested controls are provided in ISO/IEC 27002. Our approach in formulating this manual has been to concentrate firstly on the control objectives. These were reviewed to match <ORGANIZATION>'s situation and adapted to suit the style of this manual as "axioms". Secondly, we selected from ISO/IEC 27002 and other sources a range of supporting security controls that we believe will satisfy the control objectives. The supporting controls are not explained in detail in this manual (we leave that to the technical information security standards, procedures and guidelines); however the manual provides sufficient direction to reinforce the need for particular controls, under management's mandate.

## 1.5.2 Structure and overview

1.5.2.1 ISO/IEC 27002 is organized into sixteen sections numbered 0 through 15 (inclusive). After some introductory sections, sections 4 through 15 cover different aspects of information security management, with between one and ten subsections each. **The same section and subsection numbering is used in this manual for consistency and ease of cross-referencing to ISO/IEC 27002.**

1.5.2.2 The twelve main sections cover:

4. **Risk assessment and treatment**: gives a brief overview of the methods used to assess information security risks and define information security control requirements.
5. **Security policy**: more than simply a high-level information security policy, ISO/IEC 27002 promotes the use of an overarching framework of policies, standards and guidelines, coupled with effective communication throughout the organization.
6. **Organization of information security**: describes the governance and management structure of the information security function, and covers the information security aspects of dealing with third parties.
7. **Asset management**: embodies the fundamental concept that IT assets include not only hardware and software but also business data. Identifying and classifying IT assets, and allocating ownership/custodianship responsibilities is the first step towards applying appropriate protective controls.
8. **Human resources security**: given that technical security controls seldom work without effective procedures for their use and management, and that many information security controls are purely procedural, this important section gives advice on information security aspects of dealing with 'joiners, movers and leavers'.
9. **Physical and environmental security**: physical security is obviously an important issue for a data center but is also important for network switches, desktop workstations, portables and handheld devices, and in fact all locations where <ORGANIZATION> workers work. This manual defines the need for controls against unauthorized physical access, fire/smoke, flood, air conditioning and reliable power.
10. **Communications and operations management**: systems and network managers normally require powerful access rights in order to do their jobs, implying a very high degree of trust. Section 10 is the longest section in this manual. It balances the need for IT Operations professionals to have privileged access to our systems and networks against their trustworthiness and competence, and covers several other aspects of systems/network management that directly influence information security (e.g. data backup and change control procedures).
11. **Access control**: controlling logical access to sensitive data is clearly important to protect confidentiality but the manual explicitly includes integrity and availability requirements as well.
12. **Information systems acquisition, development and maintenance**: advises on the need to specify and develop information security controls as an integral part of the software development and implementation process, as well as isolating development, testing and live production environments.
13. **Information security incident management**: explains the need to identify and report security incidents and near misses as soon as possible, and for <ORGANIZATION> to learn the lessons from previous incidents.

14. **Business continuity management**: the manual defines resilience, disaster recovery and general contingency controls to help mitigate the failure of other controls, and links business continuity with IT disaster recovery plans.
15. **Compliance**: the final section covers processes for reviewing the organization's compliance with its own internal policies as well as those imposed externally such as privacy laws, copyright, contractual terms and industry regulations.

### 1.5.3 Formatting and presentation

- 1.5.3.1 The sections of this manual contain a number of **axioms** (*i.e.* formal policy requirements approved by senior management) each followed by policy statements describing the supporting controls and some supplementary guidance. The axioms are derived directly from the control objectives stated in ISO/IEC 27002. They have been explicitly approved by the Executive Directors and are shown throughout the manual in shaded boxes:

**Axioms (policy statements mandated by senior management) look like this**

- 1.5.3.2 Throughout the manual, the words “will” or “must” imply an absolute compulsion *i.e.* the stated policies and controls are mandatory or obligatory, unless exceptions have been explicitly agreed by senior management. In other cases, words such as “should” or “may” imply recommendations with an element of discretion meaning that exceptions are permitted without necessarily requiring formal management approval.
- 1.5.3.3 The manual contains numerous examples, usually preceded by “*e.g.*”. The examples are not intended to be exhaustive, merely illustrative.

## 1.6 References

- 1.6.1.1 Just like ISO/IEC 27002, this policy manual incorporates internal cross-references since certain controls are relevant to more than one section. The definitive on-line version of this manual on the intranet contains fully functional hyperlinks shown underlined [like this](#).
- 1.6.1.2 The manual refers and gives authority to various supporting documents including:
- **Certification Practice Statement (CPS)** - formally defines <ORGANIZATION>'s Public Key Infrastructure in accordance with IETF RFC 2527 assignment 15;
  - **Change Control Procedure** - protects production systems against untested, unauthorized and unsuitable changes;
  - **Clear Screen and Clear Desk Guideline** - expands on [section 11.3.3](#) of this manual;
  - **Code of Conduct** - is referenced by all employment contracts and describes employees' general responsibilities towards <ORGANIZATION>, including the obligation to comply with company policies such as those within this manual. The corporate Code of Conduct is owned and maintained by Human Resources;
  - **Computer Equipment and Storage Media Disposal Standard** - expands on [sections 9.2.6](#) and [10.7.2](#) concerning the need for systems and media to be securely cleansed of <ORGANIZATION> or personal data before being disposed of or reused;
  - **Control Self Assessment Procedures** – explain the management processes for self-checking and reporting of the status of information security and IT governance controls throughout <ORGANIZATION>;
  - **Data Access Request Procedure** – defines a controlled and auditable process for requesting, authorizing/approving and allocating network, system and data access rights;

- **Disaster Recovery Standards, Procedures and Guidelines** – document the arrangements for recovering IT systems and data following major incidents;
- **Information Retention Standard** - determines the period during which various forms of <ORGANIZATION> information must be retained, according to legal and business requirements;
- **Information Security Incident Management Procedures** – documented processes for reporting security events, and for investigating and resolving incidents;
- **Office Systems Security Guidelines** – information and guidance about security risks and controls arising from the use of office computers, emails, faxes, telephones *etc.*;
- **Password Reset Procedure** – describes the process for users to re-authenticate themselves and request replacement passwords;
- **Physical IT Security Guidelines** – advise workers on the physical protection of IT equipment against theft, criminal/accidental damage, loss *etc.*;
- **Portable Computing Security Guideline** – describes the particular security risks associated with the use of laptops, PDAs, mobile phones *etc.* plus controls;
- **Security Logging and Alerting Standard** – explains how systems are to monitor and log security-relevant events and raise real-time alarms for significant events;
- **Security Management Plan** – is a document describing the information security requirements for a contractual arrangement;
- **Software Copyright Compliance Standard** - explains the controls to ensure that unlicensed software is not installed or used on <ORGANIZATION> equipment;
- **Windows Security Baseline Standard** – one example of a technical security standard defining the minimum level of security controls that must be applied to all Windows Vista systems owned by <ORGANIZATION>.

1.6.1.3 The following external standards are referenced in this manual:

- [ISO/IEC 27000:2009](#) International standard **Information security management systems - Fundamentals and vocabulary** (available as a [free PDF download](#) from ISO/ITTF);
- [ISO/IEC 27001:2005](#) International standard **Specification for an Information Security Management System** (currently being revised);
- [ISO/IEC 27002:2005](#) International standard **Code of Practice for Information Security Management** (currently being revised);
- [ISO/IEC 27005:2008](#) International standard for **Information Security Risk Management**;
- ISO/IEC TR 18044 International standard for **Information Security Incident Management** (due to become [ISO/IEC 27035](#));
- [ISO/IEC Guide 73:2002](#) Guideline **Risk management – Vocabulary – Guidelines for use in standards** (currently being revised)
- [FIPS 140-2 Level 3](#) NIST standard **Security Requirements for Cryptographic Modules**;
- [RFC 2527](#) Internet **X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework** – specifies the term Certification Practice Statement.

## 1.7 Document change control

1.7.1.1 Since it incorporates formal statements of <ORGANIZATION> policy, this manual is subject to a strict change control process. Notes are published on the intranet when major updates to this manual are published and, if appropriate, emails are circulated to relevant parties notifying them of the changes. Major changes are noted below:

- June 2009: v8 marked the release of ISO/IEC 27000:2009. Added a couple of MS Word comments on items where customers are advised to consider their options.
- June 2008: v7 noted the release of ISO/IEC 27005:2008.
- May 2008: v6 incorporated definitions from the draft ISO/IEC 27000 and ISO/IEC Guide 73 into the glossary. Fixed a few broken links. Removed the NISPOM reference.
- November 2007: miscellaneous minor updates to the glossary. IT Help Desk becomes IT Help/Service Desk for those who use ITIL/ISO 20000.
- July 2007: v5 refers consistently to the ISO/IEC standards. Axiom 32 revised, more glossary entries added and misspellings corrected thanks to customer feedback.
- Apr 2007: v4 with CEO statement of support. Updated ISO/IEC references from ISO/IEC 17799 to ISO/IEC 27002.
- Jan 2007: v3 released for 2007.
- June 2006: v2 manual extensively updated to reflect ISO/IEC 17799:2005 e.g. added new sections on [risk assessment and treatment](#), and [information security incident management](#).
- May 2005: v1 generic policy manual completed, based around ISO/IEC 17799:2000 and more than 10 years' implementation experience with BS 7799.

- 1.7.1.2 Feedback comments, corrections and improvement suggestions on this policy manual (including any areas that are not sufficiently well covered) are welcome from any part of <ORGANIZATION> at any time. Feel free to use the table below to collect your thoughts on the manual as you read it, prior to discussing them with your line manager and/or the Information Security Manager (ISM) or Chief Security Officer (CSO):

| Section number | Comments & suggested changes |
|----------------|------------------------------|
|                |                              |
|                |                              |
|                |                              |
|                |                              |
| <i>General</i> |                              |

- 1.7.1.3 Proposed alterations to the manual will be analyzed and developed by the ISM in conjunction with relevant parties from IT, Risk Management, Compliance, Legal, Human Resources, Internal Audit etc. Updates may be circulated for comment, clearly labeled as DRAFTs. DRAFTs are not intended for implementation and do not necessarily reflect official <ORGANIZATION> policy until they are formally approved by the CSO and/or Executive Directors and released on the intranet.
- 1.7.1.4 The standards manual as a whole must also be comprehensively reviewed by the CSO and updated as necessary every year ([see 5.1.2](#)). The Executive Directors must review and re-approve the policy axioms and guiding principles at least once every two years.
- 1.7.1.5 When DRAFTs have been reviewed and if necessary updated, they must be formally submitted for approval by the CSO. If they contain new policy axioms or significant changes to the interpretation or implementation of axioms, they must be submitted by the CSO to the Board of Directors for final approval. At the point they are approved, the standards become official <ORGANIZATION> policy and must be published on the policies section of the corporate intranet as soon as practicable.

## 2 Terms and definitions

### 2.1 <ORGANIZATION> information security glossary

The following information security-related terms are defined particularly as they are used in the context of ISO/IEC 27002 and in this manual. Click the hyperlinked (underlined) terms for further explanations. Common security abbreviations and acronyms are also listed. *Meanings shown in italics are quoted directly from the cited standards.*

| Term                        | Meaning  |
|-----------------------------|--|
| 419                         | Number of a Nigerian penal code that is supposed to stop <a href="#">advance fee frauds</a> originating in Nigeria but is patently ineffective.  |
| Access, access rights       | Ability of a <a href="#">user</a> or program to interact with an information <a href="#">asset</a> e.g. to read or write data, send messages over the <a href="#">network</a> etc.; also ability of a person to enter a site, building, room, wiring closet etc.   |
| Access control              | Type of <a href="#">control</a> designed to restrict <a href="#">access</a> to an <a href="#">information asset</a> , permitting <a href="#">authorized</a> access while preventing <a href="#">unauthorized access</a> . <i>“Means to ensue that access to <a href="#">assets</a> is authorized and restricted based on business and security requirements” (ISO/IEC 27000).</i>                        |
| Access matrix               | Table relating types of <a href="#">user</a> rôle (on one axis) to IT systems, application functions and/or <a href="#">classes</a> of <a href="#">data</a> (on the other axis), showing the types of <a href="#">access</a> permitted within the body of the matrix.  |
| Accident                    | Although we tend to think that <a href="#">security incidents</a> result from deliberate acts by <a href="#">hackers</a> , <a href="#">malware</a> etc., most are in fact the result of chance <a href="#">events</a> , errors and mistakes.   |
| Accountable, accountability | A person who is held accountable for something is personally <a href="#">responsible</a> for it and may be disciplined if they do not fulfill their obligations. Unlike responsibility, however, accountability is similar to ownership in that it cannot be delegated to another (in short, 'the buck stops here'). <i>“Responsibility of an entity for its actions and decisions” (ISO/IEC 27000).</i> |
| ActiveX                     | Microsoft technology for interactive web pages. Malicious ActiveX controls (a form of <a href="#">malware</a> ) may potentially <a href="#">compromise</a> the users' systems: if the browser security settings allow, even <a href="#">unauthenticated</a> (“unsigned”) ActiveX controls may access files on hard drives.   |
| Advance fee fraud           | Type of <a href="#">fraud</a> in which the <a href="#">fraudster</a> persuades a naïve victim to send money as 'advance fees' supposedly to secure a payment which never actually materializes. Commonly known as a <a href="#">419</a> scam.  |
| Adware                      | Annoying program that displays advertisements etc. Considered by some to be a form of <a href="#">malware</a> since it is often installed <a href="#">secretly</a> and has undesirable effects that may <a href="#">compromise privacy</a> .   |
| Alarm                       | Audio/visual warning that a critical condition requiring an urgent high priority response (e.g. fire/smoke, intruder, flood) has occurred. See also <a href="#">alert</a> .  |

### 3 Structure of this manual

#### 3.1 Policy hierarchy

3.1.1.1 This Information Security Policy Manual defines the top three layers of <ORGANIZATION>'s information security policy hierarchy:

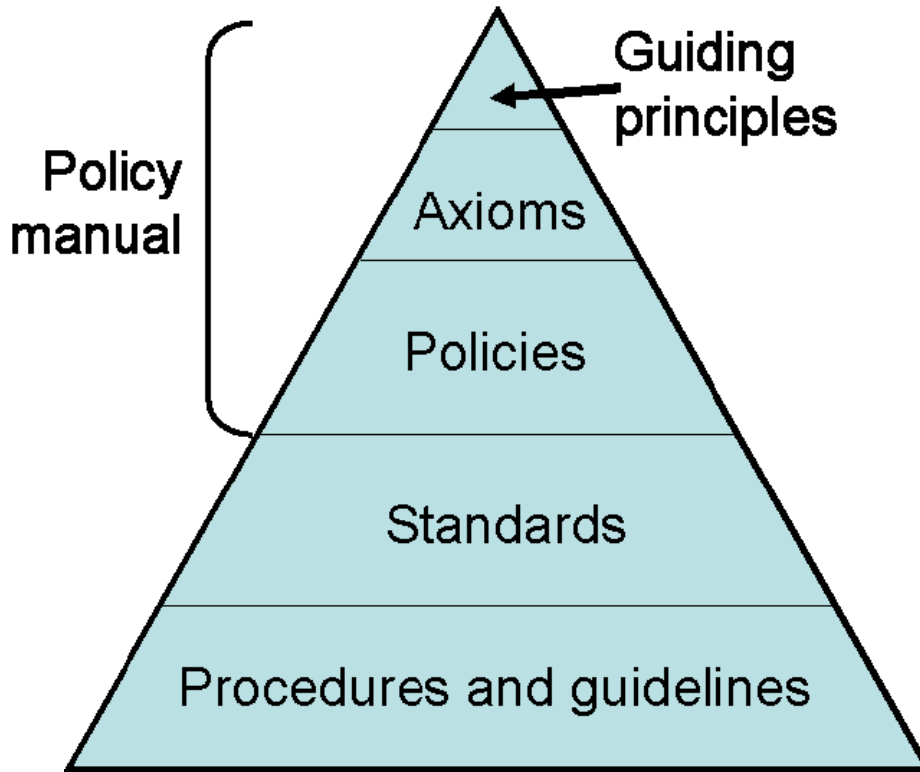


Figure 1: Information security policy hierarchy

3.1.1.2 Several security standards, procedures and guidelines are referenced in this manual in areas where more explicit details about the associated controls are required. The additional detailed materials are likely to evolve considerably during the lifetime of this manual reflecting change in technologies and information security risks. However the manual itself, being 'technology agnostic', is expected to remain relatively stable.

3.1.1.3 A number of governance activities, strategies and plans sit conceptually above the information security policy hierarchy, including corporate governance, information and IT strategies and so forth.

3.1.1.4 The policy hierarchy is supported by various information security management activities (such as procedures for measuring and reporting on security metrics, security awareness activities and a number of compliance activities) which, although important, are not explained in detail within this manual.

3.1.1.5 Great effort has been taken to avoid excessive duplication and avoid significant gaps or discrepancies within this policy manual, and to remain consistent with external requirements and obligations. If you notice possible anomalies in the manual, please submit your comments to the ISM for consideration in or before the next policy manual review and update ([see 5.1.2](#)).

## 3.2 Layers in the policy hierarchy

### 3.2.1 Guiding principles

3.2.1.1 Guiding principles are broad/overarching control objectives for information security giving **strategic direction** to information security at <ORGANIZATION>. The guiding principles are listed in [section 5.1](#) and reproduced in [Appendix A](#).

### 3.2.2 Axioms

3.2.2.1 Axioms are more specific statements of management intent such as “Access to networks, systems and applications must be authorized based on business need, security requirements and least privilege”. There are 39 axioms noted throughout this manual (collated at [Appendix A](#)) which directly relate to the 39 control objectives listed in ISO/IEC 27002. The control objectives define **why** information security is important to <ORGANIZATION>.

### 3.2.3 Policies

3.2.3.1 Policy statements explain **what** information security controls, specifically, are used to satisfy the control objectives referenced by the axioms. The bulk of this manual contains information security policy statements.

### 3.2.4 Standards

3.2.4.1 Standards provide yet more detail on information security controls and explain **how** policy statements are to be satisfied on particular system platforms or in certain circumstances. Contact the ISM for information about information security standards written by <ORGANIZATION> or available publicly.

### 3.2.5 Procedures

3.2.5.1 Procedures are documented information security processes containing manual, administrative or managerial controls, again relating to policy statements.

### 3.2.6 Guidelines

3.2.6.1 Guidelines give further information and helpful advice on information security to users of <ORGANIZATION>'s information assets. Despite the name, guidelines include a mixture of mandatory controls relating to higher-level standards, policies, axioms and principles, as well as optional controls, advice and supporting information to help workers understand and apply information security more effectively. In practice, guidelines include various security awareness materials such as briefings, presentations, training course materials, intranet pages, posters, reminder cards *etc.*

## 7 Asset management

### 7.1 Responsibility for assets

**Axiom 4: Information Asset Owners must be identified to be held accountable for the protection of all Significant Information Assets**

#### 7.1.1 Inventory of assets

7.1.1.1 Management must identify <ORGANIZATION>'s Significant Information Assets meaning information assets, both individual items and related groups of information assets (such as all the computer hardware and software providing a given IT service) having an aggregate replacement value of at least \$50,000 (this value is reviewed annually by the Executive Directors). Management must understand their relative values in order to specify appropriate protection.

7.1.1.2 Information assets include:

- Intangible information assets: the information content of databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information, proprietary knowledge, experience and expertise, reputation and brand;
- Tangible information assets: documentation, printouts *etc.*;
- Software assets: application software, system software, development tools and utilities either owned by or licensed to <ORGANIZATION>;
- IT-related physical assets: computer and telecommunications hardware (processors, monitors, laptops, routers, telephone exchanges, fax machines, answering machines), magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, computer rooms *etc.*;
- IT-related services: computing and communications services, application services and utilities supporting IT equipment such as computer room air-conditioning, lighting, power and earthing.

7.1.1.3 An accurate and complete inventory must be maintained by IT Change Management, identifying all Significant Information Assets along with key parameters such as the corresponding Information Asset Owners, their security classifications ([see 7.2](#)), locations, operating systems, versions *etc.*

#### 7.1.2 Ownership of assets

7.1.2.1 Trustworthy Information Asset Owners\* (IAOs) must be unambiguously designated by the LSC or SC to be accountable for the protection of all Significant Information Assets against information security incidents. Accountability will be distributed at the lowest feasible level of management within the organization. Although responsibility for designing, implementing, managing and/or operating information security controls may be delegated by IAOs to other parties (such as IT and Information Security Management), the IAOs remain personally accountable for their proper protection.

7.1.2.2 IAOs are responsible for classifying their information assets ([see 7.2](#)) and defining/reviewing access restrictions and other information security controls.

---

\* Information assets are legally owned by <ORGANIZATION> not IAOs. "Owner" is used here in the sense of a custodian who management holds accountable for protecting the information asset.

### 7.1.3 Acceptable use of assets

7.1.3.1 Information security aspects of local and remote systems access (e.g. passwords and authentication devices), corporate and personal email, Internet browsing, use of portable computers and Personal Digital Assistants etc. should be covered by a suite of guidelines developed and maintained by Information Security Management under authority of the CIO and CSO; endorsed, supported and enforced by managers throughout <ORGANIZATION>, and communicated to relevant workers by suitable means (e.g. hardcopy leaflets, intranet pages, awareness presentations etc.).

## 7.2 Information classification

**Axiom 5: Information assets must be risk assessed, classified and protected according to <ORGANIZATION>'s information security requirements**

### 7.2.1 Classification guidelines

7.2.1.1 The following classifications apply to <ORGANIZATION>'s information assets:

| Security aspect        | Classification label | Examples  |   |
|------------------------|----------------------|---|---|
|                        |                      | Information   | Controls  |
| <b>Confidentiality</b> | SECRET               | Corporate secrets – the most sensitive classification level | Strict access controls e.g. strong encryption routines with long keys; biometric authentication; safes                |
|                        | CONFIDENTIAL         | Sensitive business or personal information                  | Strong access controls e.g. standard encryption routines and keys; multifactor authentication; locked filing cabinets |
|                        | INTERNAL USE         | Most general business information                           | Routine access controls   |
|                        | PUBLIC               | Press releases, marketing brochures                         | No specific requirement   |
| <b>Integrity</b>       | HIGH INTEGRITY       | Important financial, safety or operational information      | Strict data validation; automated periodic system integrity checks  |
|                        | MEDIUM INTEGRITY     | Routine operational information                             | Routine data validation; manual/ad hoc system integrity checks  |
|                        | LOW INTEGRITY        | General advice and background information                   | No specific requirement   |
| <b>Availability</b>    | TIER 1               | Business- and safety-critical information                   | “Live-live” or equivalent highly resilient systems and proven disaster recovery arrangements                          |
|                        | TIER 2               | Information used routinely                                  | Cold standby disaster recovery arrangements   |
|                        | TIER 3               | Supplementary information                                   | No specific requirement   |

**Note:** Significant information assets classified into any of the shaded boxes should have documented information security designs based on formal risk assessment ([see 4.1](#)).

- 7.2.1.2 Classification of information applies to all types or forms of information asset, both tangible and intangible. In practice, however, classification is most important for Significant Information Assets with replacement values of at least \$50,000.
- 7.2.1.3 For the purposes of classification, information assets may consist of related information items, grouped together so that broadly similar controls may be applied to the group, for example:
- **Physical:** computer equipment (servers, desktop PCs, laptops, disk arrays), communications equipment (routers, switches, PABX, fax machines), magnetic media (tapes and disks), other environmental equipment (power supplies, air conditioning), furniture and premises;
  - **Software:** application software, system software, middleware, development tools and utilities;
  - **Information:** databases, data files, system documentation, user manuals, training materials, operation or support procedures, business continuity and IT disaster recovery plans, archived information, proprietary knowledge.
- 7.2.1.4 Each Significant Information Asset must be classified by the IAO or CSO at the earliest practicable opportunity based on the confidentiality, integrity and availability requirements of the most sensitive or business valuable parts of the information, as shown below. Classifications should be reviewed annually or sooner if changes occur (e.g. information that is due to be published in the annual report may be SECRET up to the point of publication, whereupon it becomes PUBLIC).

## 7.2.2 Information labeling and handling

- 7.2.2.1 Classification labels should be used consistently throughout <ORGANIZATION>, such as on printouts, reports, manuals, web pages, tapes *etc.* Other labels should be avoided and ideally replaced with the nearest equivalent.
- 7.2.2.2 Information received from third parties should retain the classification with which it entered <ORGANIZATION>, or be reclassified to an equivalent <ORGANIZATION> level using the classification scheme shown above.
- 7.2.2.3 Unclassified information assets should be considered as INTERNAL USE, LOW INTEGRITY, TIER 3 by default unless it is obvious that stricter classification is warranted (e.g. personal data is likely to be CONFIDENTIAL; customer-facing systems are likely to be TIER 1 or 2).

## 8 Human resources security

### 8.1 Prior to employment

**Axiom 6: Information security responsibilities must be addressed during pre-employment screening, included in employment contracts and monitored by management during an individual's employment**

#### 8.1.1 Rôles and responsibilities

- 8.1.1.1 Security rôles and responsibilities ([see 6.1.3](#)) including compliance with this Information Security Policy Manual as well as any specific responsibilities for the protection of particular information assets or for the execution of particular security processes or activities (such as reporting security incidents or near misses), should be documented where appropriate for example in job descriptions and employment contracts.
- 8.1.1.2 Job descriptions and so forth must be maintained and updated to reflect changes in rôles and responsibilities, particularly in respect of information security aspects. At the very least, job descriptions *etc.* must be reviewed by an employee's manager at the time of the annual appraisal or whenever someone is promoted.

#### 8.1.2 Screening

- 8.1.2.1 All potential recruits (including permanent employees, consultants, contractors and temporary staff) should be adequately screened prior to being offered employment, especially in the case of applicants for particularly sensitive or responsible positions where the candidate's integrity (honesty and trustworthiness) and competence (skills, experience and qualifications) are vital. The screening process cannot absolutely guarantee a candidate's integrity or competence but is a means to reduce the risk of employing unsuitable people. The extent of screening should therefore reflect the risk associated with abuse of the position.
- 8.1.2.2 Where permitted by local law, pre-employment screening for all applicants should include the following checks:
- Availability of satisfactory character references, typically at least one business and one personal;
  - Assessing the completeness and accuracy of the applicant's *curriculum vitae* (including academic and professional history and qualifications) by discussion with the applicant at interview and/or by other means;
  - Checking the identity of the applicant, ideally by reference to their passport or similar authentic identity document having a verified official photograph or listing distinguishing features.

- 8.1.2.3 If permitted by local law, additional checks should be performed if a candidate is anticipated to need significant access to CONFIDENTIAL or SECRET information, such as:
- Taking up the candidate's character references and seeking additional confirmation of the candidate's integrity from previous employers or business associates;
  - Validating CV details such as the candidate's employment history and claimed academic and professional qualifications (for example by calling past employers and checking the original certificates and, if necessary, confirming with the issuing institutions);
  - Actively assessing the candidate's competency for the rôle through pre-employment tests and/or a post-employment probationary period prior to confirming their appointment;
  - Credit, criminal record and/or other background or security checks (the candidate's explicit permission is normally required for checks of this nature).
- 8.1.2.4 Such additional checks should be repeated periodically for workers holding positions of considerable authority, or where there are valid reasons for management to doubt their integrity or competence.
- 8.1.2.5 Where workers are provided through an agency, the contract with the agency ([see 6.2.3](#)) should clearly specify the agency's responsibilities for screening and the notification procedures they must follow if screening has not been completed or if the results give cause for doubt or concern. <ORGANIZATION> must periodically confirm the agency's compliance with these requirements, and be alert for non-compliance (e.g. unsuitable candidates being placed).
- 8.1.2.6 Management must evaluate the need to supervise new and inexperienced workers with access to Significant Information Assets including sensitive information. The work of all workers must be periodically reviewed and approved by managers or other senior or trusted employees.
- 8.1.2.7 Managers should be aware that personal circumstances of their staff may affect their work. Personal or financial problems, changes in their behavior or lifestyle, recurring absences and evidence of stress or depression might lead to fraud, theft, error or other security implications. Fraudsters sometimes betray their activities by 'conspicuous consumption' or 'living beyond their means'. Suspicions of this nature should be reported to Human Resources and/or the ISM.
- 8.1.2.8 Personal information about candidates should be classified as CONFIDENTIAL and protected accordingly.

### 8.1.3 Terms and conditions of employment

- 8.1.3.1 The terms and conditions of employment (whether included directly in employment or similar contracts, or referenced in external documents such as the **Code of Conduct**) must clearly state the worker's obligation to comply with <ORGANIZATION>'s information security policies. The intention to initiate disciplinary actions if an employee disregards their security obligations should be noted unambiguously.
- 8.1.3.2 The worker's obligations and rights regarding Copyright, Data Protection and other applicable laws must also be clearly stated. Responsibility for the classification, handling and management of the employer's information should also be included. If appropriate, terms and conditions of employment should state that these responsibilities extend beyond <ORGANIZATION>'s premises, outside normal working hours (e.g. home- or teleworking - [see also 11.7](#)) and may persist after employment ceases.
- 8.1.3.3 Workers must sign to denote their understanding and explicit acceptance of the terms and conditions of employment prior to being permitted access to <ORGANIZATION>'s information assets.

## 8.2 During employment

**Axiom 7: Workers must be made aware of and motivated to comply with their obligations under these information security policies plus the associated standards, procedures, guidelines, laws and regulations**

### 8.2.1 Management responsibilities

8.2.1.1 All workers must comply with <ORGANIZATION>'s information security principles, axioms, policies, standards, procedures and guidelines, plus requirements identified in the terms and conditions of their employment or service contracts and applicable laws and regulations.

8.2.1.2 Managers are responsible for ensuring that, throughout their employment, workers:

- Are properly briefed and made aware of their security responsibilities (for example, using the **Code of Conduct** supplemented where necessary by more specific guidance in job descriptions, security guidelines and procedures) before being granted access to <ORGANIZATION> networks, systems or data, and periodically thereafter;
- Are motivated to comply with their responsibilities through a combination of ongoing management supervision, encouragement and reinforcement;
- Maintain their information security competencies, skills and qualifications through ongoing awareness, education and training (see below).

### 8.2.2 Information security awareness, education and training

8.2.2.1 All workers should receive appropriate training and regular updates in information security policies, standards, procedures, laws, regulations *etc.* where relevant to their job functions. This includes security requirements, legal responsibilities and business controls (such as security incident reporting processes), as well as induction training in the appropriate and secure use of IT facilities before access to information or IT services is granted.

8.2.2.2 Security awareness, education and training activities should reflect workers' needs *e.g.*:

- Managers should receive information on their information security management, supervisory and governance responsibilities;
- IT professionals, whether or not they are employed within the IT function itself, should be informed about the technical aspects of information security;
- Workers who routinely handle sensitive and valuable proprietary or personal data should be reminded periodically of their confidentiality and integrity obligations;
- All workers should be briefed about information security in general terms, using current security issues, changes, incidents or near-misses, regular appraisals, team meetings *etc.* as convenient opportunities to raise the subject.

### 8.2.3 Disciplinary process

8.2.3.1 Workers who commit a security breach (for example deliberately violating these information security policies or related security standards, procedures, guidelines, laws or regulations) should be disciplined through the standard disciplinary process owned by Human Resources, or (in the case of non-employees) through contractual or legal processes.

8.2.3.2 All workers must be treated fairly and correctly, based on reliable evidence verifying that breaches have occurred ([see 13.2.3](#)).

- 8.2.3.3 The disciplinary process allows for a range of actions according to the severity of the violation, potentially including summary dismissal and legal action to recover losses and consequential damages. Workers who break the law may also be prosecuted.
- 8.2.3.4 The deterrent value of an effective disciplinary process should not be underestimated. Where appropriate and provided that any confidentiality issues are taken into account, uses and outcomes of the disciplinary process should be communicated among managers and peers to reinforce <ORGANIZATION>'s policies in this area.

## 8.3 Termination or change of employment

**Axiom 8: A worker's exit from, or change of status within, the organization must be properly managed and controlled such that information assets are retrieved and information access rights are promptly revoked where no longer justified**

### 8.3.1 Termination responsibilities

- 8.3.1.1 Managers are responsible for ensuring that suitable termination processes are completed when subordinate workers leave <ORGANIZATION>:
- Standard termination checklists (owned by Human Resources) must be completed and returned to HR;
  - Workers must be reminded of their ongoing legal and ethical responsibilities to maintain the confidentiality of proprietary and personal information obtained in the course of their employment.
- 8.3.1.2 Similar considerations apply when a worker transfers between departments or changes status within <ORGANIZATION>. The managers involved in a transfer should jointly agree a fixed transition period, beyond which the worker will no longer have access to information and other assets exclusively associated with their previous rôle. It is particularly important that key controls relating to divisions of responsibility are not compromised at this time e.g. the worker should not be able to initiate a payment under the old rôle and approve it under the new rôle (see also [10.1.3](#)).

### 8.3.2 Return of assets

- 8.3.2.1 Workers must return all <ORGANIZATION> assets (including documents, data, computer systems, mobile phones, corporate credit cards, access tokens and authentication devices *etc.*) in their possession when they leave <ORGANIZATION>. Managers should explicitly request this, for example in the course of completing the termination checklist.
- 8.3.2.2 Workers with vital knowledge should be encouraged to 'hand-over' to their peers before they leave, ideally by preparing procedures and other notes [this process should be happening routinely in any case to minimize reliance on critical people].

### 8.3.3 Removal of access rights

- 8.3.3.1 Workers' access to information, computer/network systems and facilities must be revoked promptly when they leave <ORGANIZATION>, or revised if they transfer or change status. This includes logical and physical access rights e.g. userIDs and passwords (including any shared userIDs and group access rights), authentication tokens, access cards, keys *etc.* Responsibilities for achieving this are shared between the workers' managers, Physical Security and Security Administration, with the managers being accountable.

- 8.3.3.2 In circumstances such as summary dismissal for fraud or theft, the risks relating to a worker's termination may justify the immediate revocation of their access rights. In conjunction with Human Resources, the ISM and Physical Security, the worker's manager should ensure that the risks of continued access are assessed and appropriate action is initiated at the earliest opportunity (e.g. immediate revocation of the worker's network login ID and building access card). In such cases, there may also be a need to retain logs and other files and information for forensic analysis ([see 13.2.3](#)).

----- End of extract -----



# NOTICEBORED

IsecT's NoticeBored security awareness service significantly extends this policy manual, supplying a broad range of security guidelines, briefings, presentations, posters and other security awareness materials, all written to the same high quality standard. The additional materials support implementation of ISO/IEC 27001 and ISO/IEC 27002 and encourage compliance with the good practices detailed in this manual, helping to build a genuine information security culture.

For more information and to purchase the full version of this manual, please visit [www.NoticeBored.com](http://www.NoticeBored.com).