



<ORGANIZATION>  
Information Security  
Policy Manual

DRAFT

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

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

The information security policy manual is copyright © 2011 IsecT Ltd. Consult your license agreement for the full terms and conditions of use.

**The generic/template manual is licensed to an individual organization and *must not* be distributed to third parties unless explicitly permitted in the license.** The restriction on circulation does not apply to organization-specific derivative works, which may be shared with business partners, certification auditors *etc.* as necessary. However, if any of them wish to create their own information security policy manuals using content from this template, they need their own licenses.

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

Information is an extremely valuable and important asset that requires protection against risks to 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 security practices. **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 at the point of supply, 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 exemptions, exceptions and compliance aspects..... 10**
    - 1.4.1 Routine policy exemptions..... 10
    - 1.4.2 Emergency policy exemptions ..... 11
    - 1.4.3 Compliance..... 11
  - 1.5 Origin, structure and design of this manual ..... 12**
    - 1.5.1 Origin in ISO/IEC 27002 and other ISO/IEC 27000-series standards ..... 12
    - 1.5.2 Structure and overview ..... 12
    - 1.5.3 Formatting and presentation ..... 13
  - 1.6 Use of this policy manual ..... 14**
  - 1.7 References ..... 14**
  - 1.8 Document change control ..... 17**
- 2 Terms and definitions ..... 19**
  - 2.1 <ORGANIZATION> information security glossary ..... 19**
- 3 Structure of this manual ..... 67**
  - 3.1 Policy hierarchy..... 67**
  - 3.2 Layers in the policy hierarchy..... 68**
    - 3.2.1 Principles ..... 68
    - 3.2.2 Axioms ..... 68
    - 3.2.3 Policies ..... 68
    - 3.2.4 Standards ..... 68
    - 3.2.5 Procedures, guidelines and other supporting materials..... 68
- 4 Risk assessment and treatment ..... 69**
  - 4.1 Assessing security risks ..... 69**
  - 4.2 Treating security risks ..... 69**
- 5 Security policy..... 71**
  - 5.1 Information security policy..... 71**
    - 5.1.1 This Information Security Policy Manual..... 71
    - 5.1.2 Review of the Information Security Policy Manual..... 72
- 6 Organization of information security ..... 74**
  - 6.1 Internal organization ..... 74**
    - 6.1.1 Management commitment to information security ..... 75
    - 6.1.2 Information security co-ordination..... 76
    - 6.1.3 Allocation of information security responsibilities ..... 77
    - 6.1.4 Authorization process for information processing facilities ..... 79

- 6.1.5 Confidentiality agreements ..... 79
- 6.1.6 Contact with authorities ..... 80
- 6.1.7 Contact with special interest groups ..... 80
- 6.1.8 Independent review of information security ..... 80
- 6.2 External parties ..... 81**
  - 6.2.1 Identification of risks related to external parties..... 81
  - 6.2.2 Addressing security when dealing with customers ..... 83
  - 6.2.3 Addressing security in third party agreements..... 84
- 7 Asset management ..... 86**
  - 7.1 Responsibility for assets ..... 86**
    - 7.1.1 Inventory of assets..... 86
    - 7.1.2 Ownership of assets ..... 86
    - 7.1.3 Acceptable use of assets..... 87
  - 7.2 Information classification ..... 87**
    - 7.2.1 Classification guidelines ..... 87
    - 7.2.2 Information labeling and handling ..... 88
- 8 Human resources security ..... 89**
  - 8.1 Prior to employment ..... 89**
    - 8.1.1 Rôles and responsibilities ..... 89
    - 8.1.2 Screening..... 89
    - 8.1.3 Terms and conditions of employment..... 90
  - 8.2 During employment..... 91**
    - 8.2.1 Management responsibilities ..... 91
    - 8.2.2 Information security awareness, education and training..... 91
    - 8.2.3 Disciplinary process..... 91
  - 8.3 Termination or change of employment ..... 92**
    - 8.3.1 Termination responsibilities ..... 92
    - 8.3.2 Return of assets..... 92
    - 8.3.3 Removal of access rights..... 92
- 9 Physical and environmental security ..... 94**
  - 9.1 Secure areas ..... 94**
    - 9.1.1 Physical security perimeter ..... 94
    - 9.1.2 Physical entry controls..... 94
    - 9.1.3 Securing offices, rooms and facilities ..... 95
    - 9.1.4 Protecting against external and environmental threats..... 95
    - 9.1.5 Working in secure areas ..... 96
    - 9.1.6 Public access, delivery and loading areas ..... 96
  - 9.2 Equipment security ..... 97**
    - 9.2.1 Equipment siting and protection ..... 97
    - 9.2.2 Supporting utilities ..... 97
    - 9.2.3 Cabling security ..... 98

- 9.2.4 Equipment maintenance ..... 98
- 9.2.5 Security of equipment off-premises ..... 98
- 9.2.6 Secure disposal or re-use of equipment ..... 99
- 9.2.7 Removal of property ..... 99
- 10 Communications and operations management ..... 100**
  - 10.1 Operational procedures and responsibilities ..... 100**
    - 10.1.1 Documented operating procedures ..... 100
    - 10.1.2 Change management ..... 100
    - 10.1.3 Segregation of duties ..... 101
    - 10.1.4 Separation of development, test and operational facilities ..... 101
  - 10.2 Third party service delivery management ..... 102**
    - 10.2.1 Service delivery ..... 102
    - 10.2.2 Monitoring and review of third party services ..... 102
    - 10.2.3 Managing changes to third party services ..... 102
  - 10.3 System planning and acceptance ..... 103**
    - 10.3.1 Capacity management ..... 103
    - 10.3.2 System acceptance ..... 103
  - 10.4 Protection against malicious and mobile code ..... 104**
    - 10.4.1 Controls against malicious code ..... 104
    - 10.4.2 Controls against mobile code ..... 104
  - 10.5 Back-up ..... 105**
    - 10.5.1 Information back-up ..... 105
  - 10.6 Network security management ..... 106**
    - 10.6.1 Network controls ..... 106
    - 10.6.2 Security of network services ..... 107
  - 10.7 Media handling ..... 107**
    - 10.7.1 Management of removable media ..... 107
    - 10.7.2 Disposal of media ..... 107
    - 10.7.3 Information handling procedures ..... 108
    - 10.7.4 Security of system documentation ..... 108
  - 10.8 Exchange of information ..... 109**
    - 10.8.1 Information exchange policies and procedures ..... 109
    - 10.8.2 Exchange agreements ..... 110
    - 10.8.3 Physical media in transit ..... 110
    - 10.8.4 Electronic messaging ..... 110
    - 10.8.5 Business information systems ..... 111
  - 10.9 Electronic commerce services ..... 111**
    - 10.9.1 Electronic commerce ..... 111
    - 10.9.2 Online transactions ..... 111
    - 10.9.3 Publicly available systems ..... 112
  - 10.10 Monitoring ..... 112**

- 10.10.1 Audit logging ..... 112
- 10.10.2 Monitoring system use ..... 112
- 10.10.3 Protection of log information ..... 113
- 10.10.4 Administrator and operator logs..... 113
- 10.10.5 Fault logging ..... 113
- 10.10.6 Clock synchronization ..... 113
- 11 Access control..... 114**
  - 11.1 Business requirement for access control..... 114**
    - 11.1.1 Access control policy ..... 114
  - 11.2 User access management ..... 114**
    - 11.2.1 User registration ..... 114
    - 11.2.2 Privilege management..... 115
    - 11.2.3 User password management..... 116
    - 11.2.4 Review of user access rights ..... 116
  - 11.3 User responsibilities ..... 117**
    - 11.3.1 Password use ..... 117
    - 11.3.2 Unattended user equipment ..... 117
    - 11.3.3 Clear desk and clear screen policy..... 118
  - 11.4 Network access control ..... 118**
    - 11.4.1 Policy on use of network services..... 118
    - 11.4.2 User authentication for external connections..... 119
    - 11.4.3 Equipment identification in networks ..... 120
    - 11.4.4 Remote diagnostic and configuration port protection ..... 120
    - 11.4.5 Segregation in networks ..... 120
    - 11.4.6 Network connection control ..... 121
    - 11.4.7 Network routing control..... 121
  - 11.5 Operating system access control ..... 122**
    - 11.5.1 Secure logon procedures..... 122
    - 11.5.2 User identification and authentication..... 122
    - 11.5.3 Password management system..... 123
    - 11.5.4 Use of system utilities ..... 123
    - 11.5.5 Session time-out ..... 123
    - 11.5.6 Limitation of connection time ..... 124
  - 11.6 Application and information access control..... 124**
    - 11.6.1 Information access restriction ..... 124
    - 11.6.2 Sensitive system isolation..... 125
  - 11.7 Mobile computing and teleworking ..... 125**
    - 11.7.1 Mobile computing..... 125
    - 11.7.2 Teleworking ..... 126
- 12 Information systems acquisition, development and maintenance. 127**
  - 12.1 Security requirements of information systems ..... 127**

- 12.1.1 Security requirements analysis and specification ..... 127
- 12.2 Correct processing in applications ..... 129**
  - 12.2.1 Input data validation..... 129
  - 12.2.2 Control of internal processing ..... 130
  - 12.2.3 Message integrity..... 130
  - 12.2.4 Output data validation ..... 131
- 12.3 Cryptographic controls..... 131**
  - 12.3.1 Policy on use of cryptographic controls ..... 131
  - 12.3.2 Key management..... 132
- 12.4 Security of system files ..... 133**
  - 12.4.1 Control of operational software ..... 133
  - 12.4.2 Protection of system test data ..... 134
  - 12.4.3 Access control to program source code ..... 134
- 12.5 Security in development and support activities..... 134**
  - 12.5.1 Change control procedures ..... 134
  - 12.5.2 Technical review of applications after operating system changes..... 135
  - 12.5.3 Restrictions on changes to software packages ..... 135
  - 12.5.4 Information leakage ..... 136
  - 12.5.5 Outsourced software development ..... 136
- 12.6 Technical vulnerability management..... 137**
  - 12.6.1 Control of technical vulnerabilities ..... 137
- 13 Information security incident management..... 138**
  - 13.1 Reporting information security events and weaknesses ..... 138**
    - 13.1.1 Reporting information security events ..... 138
    - 13.1.2 Reporting security weaknesses ..... 139
  - 13.2 Management of information security incidents and improvements..... 140**
    - 13.2.1 Responsibilities and procedures ..... 140
    - 13.2.2 Learning from information security incidents ..... 141
    - 13.2.3 Collection of evidence..... 141
- 14 Business continuity management ..... 143**
  - 14.1 Information security aspects of business continuity management ..... 143**
    - 14.1.1 Including information security in the business continuity management process 143
    - 14.1.2 Business continuity and risk assessment ..... 143
    - 14.1.3 Developing and implementing continuity plans including information security .. 144
    - 14.1.4 Business continuity planning framework..... 145
    - 14.1.5 Testing, maintaining and re-assessing business continuity plans ..... 145
- 15 Compliance ..... 147**
  - 15.1 Compliance with legal requirements ..... 147**
    - 15.1.1 Identification of applicable legislation ..... 147
    - 15.1.2 Intellectual property rights (IPR) ..... 148
    - 15.1.3 Protection of organizational records ..... 149

- 15.1.4 Data protection and privacy of personal information ..... 150
- 15.1.5 Prevention of misuse of information processing facilities ..... 151
- 15.1.6 Regulation of cryptographic controls ..... 151
- 15.2 Compliance with security policies and standards and technical compliance . 152**
  - 15.2.1 Compliance with security policies and standards ..... 152
  - 15.2.2 Technical compliance checking ..... 152
- 15.3 Information systems audit considerations ..... 152**
  - 15.3.1 Information system audit controls ..... 152
  - 15.3.2 Protection of information systems audit tools ..... 153
- Appendix A The information security principles and axioms..... 154**

# 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 Information Security Policy Manual interprets [ISO/IEC 27002](#), the international standard code of practice for information security management, in the context of <ORGANIZATION>. Its purpose is to communicate management directives and standards of care to ensure consistent and appropriate protection of information assets throughout <ORGANIZATION>. It is a key part of the Information Security Management System as specified in [ISO/IEC 27001](#).

## 1.2 Status and applicability

1.2.1.1 This manual has been reviewed by the Chief Information Officer (CIO) and various other managers, and approved by the Chief Security Officer (CSO). The seven guiding principles listed in [section 5.1](#) plus the 39 axioms (formal policy statements) embedded throughout the manual and collated at [Appendix A](#), have been mandated by the Executive Directors in the **Corporate Information Security Policy**. [See section 3.1](#) for further details of the policy hierarchy.

1.2.1.2 This policy manual 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 this manual 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 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 workers from time to time by management through information security or indeed other standards, procedures and guidelines. The supporting controls gain authority from the policy statements included in this manual which in turn support the information security principles and axioms mandated by the **Corporate Information Security Policy**.

## 1.3 Intended audience

1.3.1.1 This policy manual is primarily intended for use by:

- **Information Security Management** as the **policy** framework for the Information Security Management System;
- **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 operate, evaluate and/or design specific information security controls to meet their contractual obligations towards <ORGANIZATION> and other compliance obligations.

1.3.1.2 While strictly speaking this policy manual is applicable to all **workers** meaning both <ORGANIZATION> employees (including managers, staff, temporary employees such as student placements) plus third party employees (such as consultants, contractors, support/maintenance staff) working for <ORGANIZATION> in a similar capacity, it is not anticipated that most of them will need to read it unless they wish to do so. Workers are generally informed of their specific security responsibilities through the terms and conditions or contracts of employment, security-related procedures and guidelines, and a range of security awareness and training activities such as security seminars, briefings *etc.*

## 1.4 Policy exemptions, exceptions and compliance aspects

### 1.4.1 Routine policy exemptions

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 particular 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.

1.4.1.2 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 exemptions.

## 2 Terms and definitions

### 2.1 <ORGANIZATION> information security glossary

Many of the following information security-related terms are used in this manual, while others are used in the supporting procedures, guidelines and security awareness materials. Some are formally defined elsewhere, for example in the ISO/IEC 27000 standards (particularly ISO/IEC 27000) and in applicable laws (e.g. "personal data"). Click the hyperlinked (underlined) terms for further explanations. Common security abbreviations and acronyms are also listed. *Definitions in italics are quoted directly from the cited external sources.*

Term	Meaning
<b>3DES</b>	See <a href="#">triple-DES</a> .
<b>3G</b>	Third Generation digital networks used for cellphones, SMS text messages and data communications (such as mobile Internet access). Defined by the ITU under the International Mobile Telecommunications-2000 (IMT-2000) standards.
<b>419</b>	Number of the Nigerian penal code section criminalizing <a href="#">advance fee frauds</a> . This term is often used loosely to refer to other similar <a href="#">scams</a> and scammers ("419ers").
<b>Access, access rights</b>	Ability of a <a href="#">user</a> or program to interact with an information <a href="#">asset</a> e.g. to read or write <a href="#">data</a> , send messages over the <a href="#">network</a> etc. Also the ability of a person to enter a site, building, room etc.
<b>Access control</b>	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 whilst preventing <a href="#">unauthorized</a> access. <i>"Means to ensure that access to <a href="#">assets</a> is authorized and restricted based on the business and security requirements" (ISO/IEC 27000).</i>
<b>Access matrix</b>	Table relating types of <a href="#">user</a> rôle (on one axis) to the IT <a href="#">systems</a> , 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).
<b>Access Point (AP)</b>	A wireless network router providing WiFi services. <i>"A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network" (NIST SP 800-48 and SP 800-121)</i>
<b>Accident</b>	While <a href="#">security incidents</a> may result from deliberate acts by <a href="#">hackers</a> , <a href="#">malware</a> , <a href="#">fraudsters</a> etc., the greatest proportion are in fact the result of accidental or chance <a href="#">events</a> or <a href="#">errors</a> .
<b>Accountable, accountability</b>	A person who is held personally accountable for something may be sanctioned in some way ('held to account') by an <a href="#">authority</a> if they do not fulfill their <a href="#">obligations</a> . Unlike <a href="#">responsibility</a> , accountability cannot be delegated from one person to another. In short, 'the buck stops here'. <i>"Responsibility of an entity for its actions and decisions" (ISO/IEC 27000).</i>
<b>Accurate</b>	Precise, truthful and <a href="#">valid</a> . An <a href="#">integrity</a> property.

## 10 Communications and operations management

### 10.1 Operational procedures and responsibilities

**Axiom 11: Responsibilities and procedures for the management of all information processing facilities must be documented to ensure the correct and secure operation of information processing facilities**

#### 10.1.1 Documented operating procedures

10.1.1.1 All operating procedures having significant information security implications must be formally documented and maintained, with all changes explicitly authorized by management.

10.1.1.2 The procedures should cover:

- Computer startup and shutdown, including restart and recovery procedures for use in the event of system failure;
- Backups and media handling ([see 10.5](#));
- Processing and handling of information;
- Batch scheduling requirements, including interdependencies with other batches and systems, earliest job start and latest job completion times;
- Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities ([see 11.5.4](#));
- Support contacts in the event of unexpected operational or technical difficulties;
- Special output handling instructions including the use of special stationery (such as checks and PIN mailers) and the management of confidential output, plus procedures for secure disposal of output from failed jobs ([see 10.7.2](#) and [10.7.3](#));
- Management of system, security and audit logs ([see 10.10](#));
- Equipment maintenance;
- Computer room management.

10.1.1.3 Where feasible, systems should be managed consistently using similar procedures, tools and utilities.

#### 10.1.2 Change management

10.1.2.1 Changes to information processing facilities, equipment, systems, applications and procedures must be controlled through formal management responsibilities and procedures in proportion to the risks involved.

10.1.2.2 Promotion of new systems or significant changes from development into production is a high-risk activity, particularly where existing production systems and services may be impacted, and especially so if those systems and services are supporting business critical business processes. Such significant changes must be strictly controlled ([see 12.5.1](#)). This implies that all proposed changes should be consistently risk assessed to determine their significance, and the associated management decisions and approvals must be recorded.

10.1.2.3 Significant changes must be identified and recorded in the change management system. Procedures relating to the implementation of significant changes must also be suitably planned and documented, along with fallback procedures for verifying/aborting and recovering from unsuccessful changes (e.g. restoration of immediate pre-change backups).

- 10.1.2.4 Changes must be tested prior to implementation, reflecting a rational assessment of the potential impacts including any security implications ([see 12.1.1](#)).
- 10.1.2.5 Change details must be communicated to the relevant people in IT and in the business.

### 10.1.3 Segregation of duties

- 10.1.3.1 Care must be taken to prevent the perpetration of fraud by individuals with excessive access rights. Duties and areas of responsibility must be segregated between individuals to reduce opportunities for unauthorized or unintentional modification or misuse of <ORGANIZATION>'s information assets.
- 10.1.3.2 Systems and processes must require the involvement of at least two people for important transactions, normally by separating the initiation and authorization steps between individuals.
- 10.1.3.3 If there is a danger of the primary controls being bypassed (e.g. through collusion), additional controls must be designed and implemented e.g. secure logs/records of transactions, regularly reviewed, and alarms/alerts on significant security events. Staff performing checks such as security audits and system acceptance tests must be independent of the management and operation of the systems and processes being reviewed.

### 10.1.4 Separation of development, test and operational facilities

- 10.1.4.1 Pre-production environments (including the systems, networks and data associated with specification, design, development and testing of computer software) must be fully isolated from production environments to minimize the risk of production incidents, using physically different systems, processors, domains, directories and networks ("air gaps") or, where physical isolation is not feasible, strong logical controls such as encryption.
- 10.1.4.2 Development and test environments must also be at least logically isolated from each other to ensure their respective integrity.
- 10.1.4.3 The promotion of new or modified software into production must be controlled through the formal **Change Control Procedure**.
- 10.1.4.4 Test systems should emulate production as closely as possible except that:
- Testers and developers should not have userIDs on production systems (excluding firecall userIDs which are only enabled for use by authorized IT support workers for specific support purposes through the emergency changes process within the **Change Control Procedure**);
  - Production data should only be available on production systems. Development and testing should use dummy data wherever possible. If production data must be used, fields containing highly sensitive data (such as credit card numbers and personal data) must first be obfuscated ([see also 12.4.2](#));
  - On-screen messages, screen colors *etc.* should clearly indicate whether a system is in test or production to minimize the risk of someone accidentally submitting test transactions on production systems.
- 10.1.4.5 Compilers, editors and similar powerful system utilities must not be installed on production systems unless absolutely necessary, and then may only be used by authorized users for legitimate purposes under authority of an approved change control record.