

## **MINIMUM SECURITY STANDARDS FOR INTERCONNECTING COMMUNICATIONS PROVIDERS**

---

NICC Standards Limited

Michael Faraday House,  
Six Dials Way,  
Stevenage  
SG1 2AY

Tel.: +44(0) 20 7036 3636

Registered in England and Wales under number 6613589

## NOTICE OF COPYRIGHT AND LIABILITY

**© 2009 NICC Standards Limited**

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on NICC printers of the PDF version kept on a specific network drive within the NICC.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other NICC documents is available at:

<http://www.nicc.org.uk/nicc-public/publication.htm>

If you find errors in the present document, please send your comments to:

mailto: [help@niccstandards.org.uk](mailto:help@niccstandards.org.uk)

**Copyright**

All right, title where and interest in this document are owned by NICC Standards Limited ("NICC") and/or the contributors to the document (unless otherwise indicated that copyright is owned or shared with a third party). Such title and interest is protected by United Kingdom copyright laws and international treaty provisions.

The contents of the document are believed to be accurate at the time of publishing, but no representation or warranty is given as to their accuracy, completeness or correctness. You may freely download, copy, store or distribute this document provided it is not modified in any way and it includes this copyright and liability statement.

You may not modify the contents of this document. You may produce a derived copyright work based on this document provided that you clearly indicate that it was created by yourself and that it was derived from this document and provided further that you ensure that any risk of confusion with this document is avoided.

**Liability**

Whilst every care has been taken in the preparation and publication of this document, neither NICC, nor any working group, committee, member, director, officer, agent, consultant or adviser of or to, or any person acting on behalf of NICC, nor any member of any such working group or committee, nor the companies, entities or organisations they represent, nor any other person contributing to the contents of this document (together the "Generators") accepts liability for any loss or damage whatsoever which may arise from the use of or reliance on the information contained in this document or from any errors or omissions, typographical or otherwise in the contents.

Nothing in this document constitutes advice. Nor does the transmission, downloading or sending of this document create any contractual relationship. In particular no licence is granted under any intellectual property right (including trade and service mark rights) save for the above licence to download copy, store and distribute this document and to produce derived copyright works.

The liability and responsibility for implementations based on this document rests with the implementer, and not with any of the Generators. If you implement any of the contents of this document, you agree to indemnify and hold harmless each Generator in any jurisdiction against any claims and legal proceedings alleging that the use of the contents by you or on your behalf infringes any legal or other right of any of the Generators or any third party.

None of the Generators accepts any liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from any use of or reliance on the contents of this document for any purpose.

The NICC Standards Web site contains the definitive information on the [IPR Policy and Anti-trust Compliance Policy](#)

If you have any comments concerning the accuracy of the contents of this document, please write to:

The Technical Secretary, NICC Standards Ltd.,

Michael Faraday House,  
Six Dials Way,  
Stevenage  
SG1 2AY

---

# Contents

|   |    |
|---|----|
| Intellectual Property Rights .....  | 5  |
| Foreword .....  | 5  |
| Introduction .....  | 5  |
| Audit and compliance monitoring .....   | 5  |
| 1 Scope .....   | 6  |
| 1.1 Types of interconnect in scope .....  | 6  |
| 1.2 Scope .....   | 7  |
| 1.3 External parties .....  | 7  |
| 1.4 Interconnect equipment.....   | 8  |
| 2 References .....  | 9  |
| 2.1 Normative references .....  | 9  |
| 2.2 Informative references .....  | 9  |
| 3 Definitions and abbreviations.....  | 9  |
| 3.1 Definitions .....   | 9  |
| 3.3 Abbreviations.....  | 9  |
| 4 Security policy .....   | 10 |
| 4.1 Information security policy document .....  | 10 |
| 5 Organisation of information security .....  | 10 |
| 5.1 Management commitment to information security .....                                 | 10 |
| 5.2 Addressing security in third party agreements.....                                  | 11 |
| 6 Human resources .....   | 13 |
| 6.1 Roles and responsibilities .....  | 13 |
| 6.2 Screening .....   | 13 |
| 6.3 Terms and conditions of employment.....   | 14 |
| 6.4 Management responsibilities .....   | 14 |
| 6.5 Removal of access rights .....  | 15 |
| 7 Physical .....  | 17 |
| 7.1 Physical security perimeter .....   | 17 |
| 7.2 Physical entry controls.....  | 17 |
| 7.3 Equipment maintenance.....  | 18 |
| 8 Communications & operations management .....  | 19 |
| 8.1 Documented operating procedures .....   | 19 |
| 8.2 Change management.....  | 19 |
| 8.3 Network controls .....  | 20 |
| 8.4 Audit logging.....  | 20 |
| 8.5 Administrator and operator logs .....   | 21 |
| 9 Access control .....  | 22 |
| 9.1 Access control policy.....  | 22 |
| 9.2 User authentication for external connections.....                                   | 23 |
| 10 Information systems acquisition, development and maintenance .....                   | 24 |
| 10.1 Control of technical vulnerabilities.....  | 24 |
| 11 Information security incident management.....  | 25 |
| 11.1 Reporting information security events.....   | 25 |
| 11.2 Reporting information security events.....   | 25 |
| 12 Business continuity management .....   | 26 |
| 12.1 Including information security in the business continuity management process ..... | 26 |

|      |   |    |
|------|---|----|
| 13   | Compliance .....                                      | 26 |
| 13.1 | Compliance with security policies and standards ..... | 26 |
| 14   | History .....   | 28 |

---

## Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC. Pursuant to the [NICC IPR Policy](#), no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

---

## Foreword

This NICC Document (ND) has been produced by the NICC Security Working Group.

---

## Introduction

Communications providers interconnect with each other as a result of either regulatory requirements or commercial imperatives. In these situations each communications provider's security is partially dependent on the security of the other. One provider could cause an adverse effect for the other, either deliberately or by omission or neglect.

Each provider should provide their own defence against likely threats. However each provider should only have to apply a proportionate defence. Providers should not have to incur disproportionate costs to defend their network from actions or omissions by an interconnected provider. The controls in this document should be enforced as a minimum standard of security by a provider's interconnect partners to provide protection in these circumstances.

The standard aims to:

- Prevent a provider from incurring an excessive cost in protecting their own network (i.e. the costs that would be incurred if they had to interconnect with communications providers who had no security controls).
- Enable communications providers to commercially differentiate their services in terms of security should they wish to.
- Apply to all types of interconnection, including physical and electronic, although some controls are only relevant in certain circumstances.

## Audit and compliance monitoring

Communications Providers will be expected to audit the suitability of their controls and procedures at least annually and have their compliance to these certified via an agreed industry approved process. This industry agreement will be facilitated and documented by OTA2. It is anticipated that this will be via an appropriate extension of a CPs existing or planned 27001 certification or via an accredited agency(s) agreed and appointed by industry.

---

# 1 Scope

The present document contains controls and measures that constitute the minimum standards required to protect the UK national infrastructure. The controls are based on a subset of ISO27002 [1] and ISO27011/X.1051.

The Minimum Security Standard is applicable to any communications provider that has a direct interconnection with another communications provider.

## 1.1 Types of interconnect in scope

This section defines the types of interconnect which the “minimum security standards for interconnecting communications providers”, or minimum standards will be applied to under the code of practice proposed by the Office of the Telecommunications Adjudicator (OTA2).

The following types of interconnect are in scope:

- SIP, SIP-I and H323 based interconnects, or similar IP session based interconnects. (For example interconnects supporting streaming services, for example, live radio, live TV and video on demand. near real-time interactive services, for example, instant messaging and press-to-talk.)
- Interconnects supporting broadband/NGA access.
- Data connection services, for example IP, Ethernet and MPLS.

Where, the interconnect is between two (or more) operators who are committed to the code of practice.

Specific exclusions are, internet peering, and traditional SS7 PSTN interconnections.

## 1.2 Scope

The scope involves personnel, physical areas and equipment. The scope is restricted to:

- Personnel who have right of access to the shared area;
- Personnel who have access permissions permitting configuration changes, or other privileged access to shared interconnect equipment;
- Equipment within a shared area;
- Other accessible areas containing interconnect equipment;
- Environmental and other services (fire suppression, air-conditioning, power etc.) associated with the shared area;
- The equipment that terminates each layer of the interconnect (see diagram);
- Procedures supporting these.

The scope for each control may be restricted to specific groups of equipment. In these situations this is highlighted in the appropriate section below. Additionally individual controls may only be applicable to local loop unbundling, other interconnect situations, or may be applicable to both. In these situations this is highlighted in the appropriate section below.

Personnel who would not ordinarily be in scope but are required to occasionally work on systems or in areas that are in scope, and who do not comply with the personnel vetting requirements must be supervised.

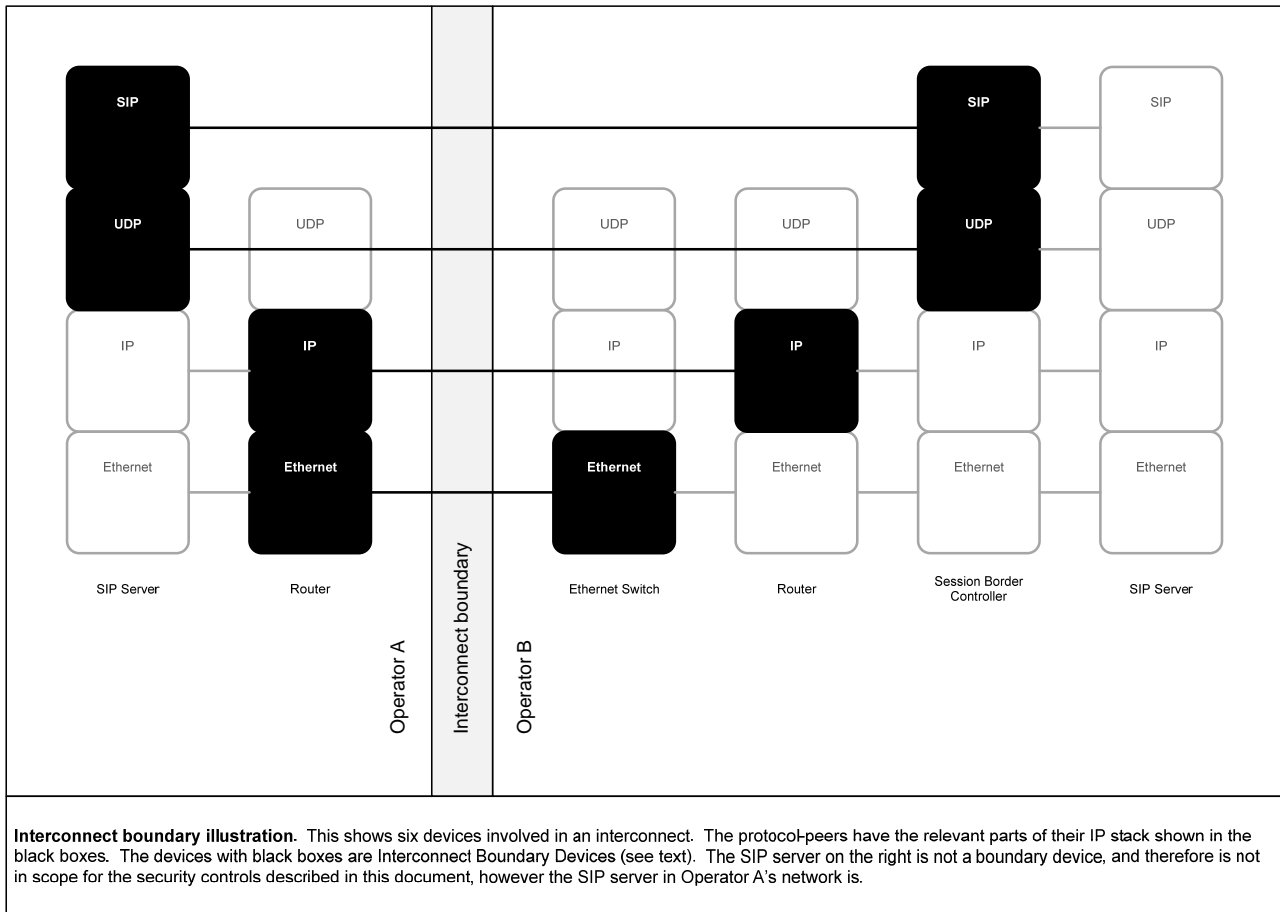
## 1.3 External parties

The controls also apply to people, equipment and processes managed by external parties on your behalf. They must be contractually obliged to meet the appropriate controls from this standard.

## 1.4 Interconnect equipment

An interconnect boundary device (IBD) is a device which communicates with a protocol-peer on the opposite side of an interconnect, and where the protocol is functional across the interconnect. Protocols which have no peer in one or both of the CP networks being interconnected are not functional across the interconnect.

A common example of a non-functional protocol stack occurs when traffic is tunnelled across a transit network interconnecting two CPs. Any device containing a functional protocol-peer is an Interconnect Boundary Device. Each functional protocol should have either a single protocol-peer, or a resilient set of protocol-peers on each side of the interconnect. All of the devices in such a resilient set are Interconnect Boundary Devices. Because protocol-peers may be directly connected or remote, Interconnect Boundary Devices may be local to the interconnect point or remote. Devices such as those offering 'packet inspection' are not considered to be part of the protocol peering arrangement. Devices with full protocol implementations, e.g. a proxy firewall are considered to act as a protocol peer.



---

## 2 References

### 2.1 Normative references

### 2.2 Informative references

- [1] ISO27002: ISO27002 Information technology. Security techniques. Code of practice for information security management<sup>1</sup>
- [2] ISO9001: ISO 9001:2008 Quality management systems – Requirements
- 

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the following definitions apply

**Interconnect scope:** The complete set of personnel, procedures, physical areas and electronic equipment within scope.

**Interconnect:** A connection between two communications providers which includes protocols or services not available to standard customers of either communications provider.

**Shared area:** Any area where the staff, or subcontractors of one communications provider has physical access to equipment supporting another.

**Interconnect equipment:** Equipment involved in providing the interconnect. See below.

### 3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

|      |  |
|------|--|
| iSPD | Interconnect Security Policy Document                |
| CPNI | Center for the Protection of National Infrastructure |
| NGN  | Next Generation Network                              |
| QMS  | Quality Management System                            |

---

<sup>1</sup> Permission to reproduce extracts from British Standards is granted by BSI under Licence No. 2008ET0029. British Standards can be obtained in PDF or hard copy formats from the BSI online shop: [www.bsigroup.com/Shop](http://www.bsigroup.com/Shop) or by contacting BSI Customer Services for hard copies only: Tel: +44 (0)20 8996 9001, Email: [cservices@bsigroup.com](mailto:cservices@bsigroup.com).

The Licensee is permitted to make the publication available for download on the NICC and NGNUK websites. This permission does not cover any other editions of the publication. On no account shall the extracts used be included as part of any other work not permitted under this licence. This permission relates to the extracts listed above. Where the standard is updated and/or if there is a requirement for further reproduction of extracts you will need to make a new application. Only English Language use of the extracts is permitted.

---

## 4 Security policy

### 4.1 Information security policy document

*ISO27002 [1] Section 5.1.1*

#### Control

An information security policy document should be approved by management and published and communicated to all employees and relevant external parties.

#### Guidance

An information security policy document must be approved by management, and published and communicated to all parties within the *interconnect scope*.

The policy must include measures for each of the controls and these minimum standards.

This document could typically be the organisation's overall information security policy, standards and processes, and might comprise various sources and formats, such as Word, HTML and PDF. Some organisations choose to wholly adopt the controls in ISO27002 [1] as their Information Security Policy. However, communications providers may choose to create, in addition to the overall information security policy document, a unique document (Interconnect SPD) limited to the scope of the interconnect.

The iSPD should explain how your organisation implements the controls that are required by the minimum standard. It should explain how you measure the effectiveness of the controls. The document would make reference to the communications provider's overall information security policies, standards and processes, but make it clear which controls were applicable. For example, the organisation might mandate particular controls for third party access, but should these not be applicable within the scope of the Interconnect then the iSPD would record this.

The iSPD would also be the primary document for demonstrating compliance to the Minimum Standard. Communications providers could also consider certification to ISO27001 of the information assets and processes associated with the Interconnects to help demonstrate compliance.

#### Validation

Communications providers must be able to produce the documentation.

#### Rationale

Without this control it is impossible to guarantee any consistency or continuity of the security practices mandated by this document.

---

## 5 Organisation of information security

### 5.1 Management commitment to information security

*ISO27002 [1] Section 6.1.1*

#### Control

Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

## Guidance

Management should actively support the implementation of and compliance with the minimum security standard.

Communications providers must be able to show evidence that security issues are addressed through clear policies and explicit assignment of responsibilities including the appropriate documentation and audit processes.

Top-down commitment from senior management is essential to the success of security controls and mitigation of risks in any organisation. Whilst much of the detail can be delegated to appointed security officers or their equivalent, senior management must, for the Minimum Standard:

- Ensure appropriate funding and resource is available to implement the standard's controls;
- Assign key roles and responsibilities for implementation, operation, monitoring and improvement of the controls;
- Set the strategic approach the organisation will take to achieve compliance, and articulate this through policy documents and planning;
- Ensure those employees within the scope of Interconnects are aware of their responsibilities through training and awareness.

## Validation

Identification of individuals with roles relating to measures in the minimum security standard and related organisational policies.

## Rationale

Without this control it is impossible to guarantee any consistency or continuity of the security practices mandated by this document.

## 5.2 Addressing security in third party agreements

*ISO27002 [1] Section 6.2.3*

### Control

Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

### Guidance

A communications provider may contract a third-party to implement some of the controls in this document. The contract with the third party must clearly cover the relevant security requirements, and should also cover the right to audit.

The communications provider must monitor the enforcement of the requirements. This monitoring is typically performed through logging and auditing procedures.

The communications provider should seek assurances from the third party that the required security behaviours have been communicated to their personnel and are being followed.

Obligations must be passed on by any third-parties, as appropriate for compliance with the standard, to companies and individuals further down the supply chain.

*CPNI provides advice on a contractual framework for the provision of NGN components and advice on dealing with third-party suppliers, on request (telecommunications@cpni.gov.uk).*

## Validation

Demonstrate that contractual or other agreements with third-parties cover these security requirements.

Communications providers must be able to demonstrate that the controls mandated in this minimum standard are also enforced on and by third-party suppliers as appropriate.

## Rationale

Without this control there will be uncertainty surrounding the implementation of these security requirements by third parties.

---

## 6 Human resources

### 6.1 Roles and responsibilities

*ISO27002 [1] Section 8.1.1*

#### Control

Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.

#### Guidance

Communications providers must be able to show that security roles and responsibilities are defined and documented in the policy documentation.

#### Validation

Review the documentation for clearly defined roles and responsibilities.

#### Rationale

Without this control it is impossible to guarantee any consistency or continuity of the security practices mandated by this document.

### 6.2 Screening

*ISO27002 [1] Section 8.1.2*

#### Control

Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

#### Guidance.

Where local legal restrictions allow organisations must:

- Seek references
- Check accuracy of applicant's CV
- Confirm claimed professional qualifications
- Complete an independent identity check
- Check for any criminal history (e.g. UK criminal records check). As a minimum ask the candidate to complete a criminal record declaration.

Communications providers must be able to demonstrate the process that is followed for personnel in scope.

Employees taken on within the past three years should also be checked retrospectively. There is no requirement to repeat checks on an individual during the duration of their employment.

*These principles are based on BS7858 CPNI advice on Pre-Employment Screening can help with, for example, the issues surrounding the screening of non-UK personnel.*

## Validation

View records of checks on personnel.

## Rationale

Without this control individuals with malicious intent will find it both easy to gain access to the interconnect, and by mis-representing their identity may avoid prosecution in the event of an incident.

## 6.3 Terms and conditions of employment

*ISO27002 [1] Section 8.1.3*

### Control

As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.

### Guidance

Communications providers must be able to demonstrate that the terms and conditions of the employment contract for all employees, contractors and third party users state their and the organization's responsibilities for information security.

Communications providers should verify that a contractor or other third party's parent organisation employment contract makes reference to compliance with the provider's security policy whilst working for the communications provider. These third party organisations should be contractually obliged to include these conditions in their employees' contracts.

### Validation

View a signed contract containing a clause that requires compliance with the appropriate policies.

### Rationale

Without this control it is impossible to guarantee any consistency or continuity of the security practices mandated by this document. It will also be impossible to identify the individuals ultimately responsible for compliance and therefore there can be no accountability for any failure to meet the minimum standard.

## 6.4 Management responsibilities

*ISO27002 [1] Section 8.2.1*

### Control

Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.

### Guidance

Management responsibilities must include ensuring that employees, contractors and third party users conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working.

In order to demonstrate compliance with the minimum standard managers have a number of regular security duties, such as:

- Ensuring they, themselves, are briefed by the security officer or other person responsible for security
- Ensuring the competence of their people and third parties for whom they are responsible.
- Maintaining security awareness and cascading security briefings.
- Motivating personnel to conform to the required security behaviours.
- Periodic reviews of access rights on systems, equipment and to technical facilities.
- Ensuring appropriate asset recovery (computers, access tokens, keys etc) and account closures follow employment terminations.

## Validation

Demonstrate an approach for ensuring compliance.

## Rationale

Without this control it is impossible to guarantee any consistency or continuity of the security practices mandated by this document.

## 6.5 Removal of access rights

*ISO27002 [1] Section 8.3.3*

### Control

The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

### Guidance

The access rights of all employees, contractors and third party users to systems within scope must be removed upon termination of their employment, contract or agreement, or adjusted if their role changes.

Where accounts are created on a interconnect partners equipment the interconnect partner must also be notified to close or modify access permissions as appropriate.

Communications providers should ensure that they have process for the removal of access rights, both physical and logical, in the event of employment termination or role change. This process may be manual or automatic, or a combination of both, and must be completed in a timely manner.

It is also recommended that communications providers operate a policy of regular internal review of access. Where access is granted to an interconnected providers equipment this should also be done in partnership with the interconnected provider.

### Validation

Communications providers must be able to show the linkage between HR and IT departments and describe the process of removal of access rights.

## Rationale

Without this control access to the interconnect will still be available to those who no longer require access, or in some cases who are not longer under any contractual obligation to maintain the security or availability of the interconnect.

---

## 7 Physical

### 7.1 Physical security perimeter

*ISO27002 [1] Section 9.1.1*

#### Control

Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.

#### Guidance

Security perimeters should be provided around equipment within information processing facilities. Controls such as locking racks should be used where possible to reduce the possibility of unauthorised access. Communications providers must be able to show that they have taken appropriate precautions to secure their equipment and information, by locking equipment cabinets, protecting access ports on equipment and effectively labelling equipment.

Communications providers must have robust processes/policies in place to ensure that:

- The appropriate level of security is applied to prevent illicit access to their documentation, spares, equipment or network terminations.
- Equipment racks are locked and there should be an appropriate key management process.
- Employees display the appropriate photo id cards, when required to by their organisation or the host's security policy.
- Employees remain within authorised areas within sites.
- Access ports on equipment are disabled where appropriate.
- Equipment is labelled effectively.

#### Validation

Communication providers must be able to show appropriate robust policies and processes and demonstrate the security controls in use.

#### Rationale

Without this control there can be no effective protection of the interconnect and interconnect equipment.

### 7.2 Physical entry controls

*ISO27002 [1] Section 9.1.2*

#### Control

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

## Guidance

Areas containing interconnect equipment and shared areas must be protected by proportionate entry controls in accordance with a risk assessment to ensure that only authorized personnel are allowed access.

In particular it is important to manage the access of third party suppliers and support staff that may demonstrate little loyalty to the host organisation and may have little incentive to pay more than lip service to policy.

Communications providers should have robust processes in place to ensure:

- Keys cards and similar access tokens are protected from misuse and only used by those authorised to do so.
- Employees permitted access are competent or supervised and authorised to work on the equipment.

## Validation

Communications providers must be able to show how they implement access control in secure areas.

## Rationale

Without this control physical security of any interconnect equipment will be limited.

## 7.3 Equipment maintenance

*ISO27002 [1] Section 9.2.4*

### Control

Equipment should be correctly maintained to ensure its continued availability and integrity.

### Guidance

Equipment in shared areas must be correctly maintained to ensure that it has no adverse impact on the availability or integrity of other communications providers' equipment. Communications providers must be able to show that equipment is subject to appropriate routine and regular maintenance.

### Validation

Production of a maintenance plan and evidence that it has been followed.

### Rationale

Without this control catastrophic equipment failure (for example a fire or electrical fault) in a shared area may impact on the facility and other users.

---

## 8 Communications & operations management

### 8.1 Documented operating procedures

*ISO27002 [1] Section 10.1.1*

#### Control

Operating procedures should be documented, maintained, and made available to all users who need them.

#### Guidance

Documented procedures should be prepared for system activities associated with interconnect equipment, including equipment maintenance and safety. Operating procedures, and the documented procedures for system activities, should be treated as formal documents and changes authorized by management.

Operating procedures may be in physical or electronic format. Communications providers must be able to demonstrate that their procedures are the latest version.

It is good practice to subject documents to a change management and authorisation regime, examples of which are to be found in QMS (ISO9001 [2]).

Access to the procedures should be limited to those whose roles require it.

#### Validation

Communications providers must be able to show suitable operating procedure documentation, its availability and its distribution.

#### Rationale

Without this control other security measures mandated by this minimum standard may be rendered ineffective.

### 8.2 Change management

*ISO27002 [1] Section 10.1.2*

#### Control

Changes to information processing systems should be controlled.

#### Guidance

A change control process should exist.

The process should ensure that for changes to systems in scope any impact on compliance with this minimum standard are be considered.

#### Validation

Demonstrate the process.

## Rationale

Without this control security measures in this document may be rendered ineffective after a change.

## 8.3 Network controls

*ISO27002 [1] Section 10.6.1*

### Control

Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

### Guidance

The network should be configured so that only agreed traffic may cross the interconnect. Except where direct communications are required, providers must maintain the separation of the interconnect partner from other external sources (e.g. other interconnects, the Internet). Filters, SIP proxies, firewalls, vLANs or other technology should be used to maintain this separation.

Network design documentation should exist and could include:

- Definition of the network perimeter by IP address
- The ports and protocols allowed across the network perimeter to and from other networks (those not permitted should be blocked)
- The perimeter devices enforcing security and separation (firewalls, intrusion prevention systems etc).
- Reference to the processes for configuration and change management
- Roles and responsibilities
- Schematics

### Validation

View the design documentation.

## Rationale

Without this control interconnecting communications provides may be exposed to unnecessary risk of attack.

## 8.4 Audit logging

*ISO27002 [1] Section 10.10.1*

### Control

Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

## Guidance

Audit logs for the interconnect equipment should record user activities, exceptions, and information security events occurring on shared technical facilities must be produced and kept for an agreed period to assist in future investigations and access control monitoring.

Communications providers must be able to show a complete audit history for 90 days for systems in scope.

Audit logs should be appropriately protected in accordance with the procedures defined in *Access Control Policy*.

Where audit trail and system log information is deemed sensitive, consider:

- Restricting access to those with an official audit role and on a need to use basis.
- Controlling update access to audit files and monitoring tools.
- Ensuring log files continue to be recorded
- Secure storage of the logs

## Validation

Demonstrate a log entry from 90 days ago. If logs are not available as a result of the youth of a system then demonstrate any recent log entry and the relevant settings for the storage period.

## Rationale

Without this control investigations into network events may prove difficult to complete and maintenance of security may therefore become difficult.

## 8.5 Administrator and operator logs

*ISO27002 [1] Section 10.10.4*

### Control

System administrator and system operator activities should be logged.

### Guidelines

Communications providers must be able to log and subsequently show full history of system administrator and system operator activities on shared technical facilities.

Successful and failed authentication attempts.

Configuration, management and operational changes to the interconnect equipment should be logged where possible.

Change management should record why logons occurred where changes are not automatically logged.

Logs should be retained for 90 days.

## Validation

Demonstrate a log entry from 90 days ago. If logs are not available as a result of the youth of a system then demonstrate any recent log entry and the relevant settings for the storage period.

## Rationale

Without this control investigations into network events may prove difficult to complete and maintenance of security may therefore become difficult.

---

# 9 Access control

## 9.1 Access control policy

*ISO27002 [1] Section 11.1.1*

### Control

An access control policy should be established, documented, and reviewed based on business and security requirements for access.

### Guidelines

The access control policy should apply to the interconnect equipment. It should cover:

- Formal authorisation of access requests
- Requirements for periodic review of access rights
- Removal of access rights

Care should be taken to establish rules on the premise *everything is generally forbidden unless expressly permitted*.

The access control policy could be the Communications provider's overarching policy or explicitly for the interconnect equipment, perhaps defined in the interconnect security policy document.

It will include:

#### Formal authorisation of access requests

Access requests must follow a formal process. The role responsible for operating access control must verify the identity of the individual, the individual's role is appropriate to the access, and that management has approved the request. The individual's manager must confirm that the security briefing has taken place (see 9.4 and ISO27002 [1] 11.2.1).

Where third parties e.g. other communications provider or vendor, have accounts on equipment communication channels must be established to fulfil this requirement for access, logical and physical, to interconnect equipment.

#### Requirements for periodic review of access rights.

As previously discussed, and whilst this could be a line management duty it is often responsibility of an Access Control duty or system administrator.

#### Removal of access rights

See *Removal of Access Rights*, section 0.

### Validation

Communications providers must be able to show an access control policy for interconnect equipment and describe the review process, based on business and security requirements for access.

### Rationale

Without this control excessive numbers of people may have access to interconnect equipment increasing the number of people who could exploit a vulnerability via the interconnect.

## 9.2 User authentication for external connections

*ISO27002 [1] 11.4.2*

### Control

Appropriate authentication methods should be used to control access by remote users.

### Guidelines

Management access to the interconnect equipment from remote locations should be controlled using a mechanism that provides protection against unauthorised configuration of the interconnect equipment.

Authentication in these circumstances can be achieved using a public key cryptography based technique or other two factor authentication mechanism.

Password authentication may be used if combined with a restriction on the possible sources of authentication to known source locations.

There are various vendors providing remote access authentication solutions. Communications providers should satisfy themselves that the selected solution meets, as a minimum, the requirements of this standard.

It is strongly recommended that where the remote user's role does not require them to have access to other equipment, that the design of the network is such that they cannot get onward access from a permitted device to other resources on the network.

### Rationale

Without this control external access to the interconnect equipment may be easily compromised by a malicious party. The size of the potential attack population here is large so it is important to focus strong authentication on external connections.

---

## 10 Information systems acquisition, development and maintenance

### 10.1 Control of technical vulnerabilities

*ISO 27002 Section 12.6.1*

#### Control

Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

#### Measure

Communications providers must be able to demonstrate the measures taken to obtain timely information about technical vulnerabilities affecting the interconnect equipment and show how the organization's exposure to such vulnerabilities is evaluated, and addressed.

This may refer to the patching of vulnerabilities, the disabling of unnecessary services or the secure configuration of services that are in use.

There are various sources of information available depending upon the platforms used and products offered. Organisations must have a trustworthy source of advice so that corrective action can be taken in a timely fashion. Organisations must have a well defined process for applying patches and upgrades.

Technical vulnerabilities occur at all levels from hardware to operating systems to applications.

Vulnerabilities can be exploited with malicious intent, often before they become public knowledge. There are various sources of vulnerability and solution notification, most typically vendors and specialist security organisations. Many vendors will provide as part of the maintenance agreement a notification and patching distribution service.

However, vulnerability solutions should consider testing them before they are applied; it is not unknown for security patches to introduce new problems. It may also be the case that vulnerabilities are low risk and so are deemed not applicable. The deployment of vulnerability solutions should follow change management processes.

Communications providers should have policy and procedures for vulnerability management.

#### Rationale

Without this control vulnerabilities in a provider's equipment may make it easy for a malicious party to launch an attack on an interconnected provider.

---

## 11 Information security incident management

### 11.1 Reporting information security events

*ISO27002 [1] Section 13.1.1*

#### Control

Information security events should be reported through appropriate management channels as quickly as possible.

#### Guidance

Communications providers must be able to show how information security events within the interconnect scope are reported:

- through appropriate management channels;
- externally where appropriate.

Communications providers must also demonstrate the existence of an escalation path for unresolved security issues.

Security events may lead to security incidents. Events should be reported for pragmatic analysis to determine if they warrant further action. Security incidents require an immediate response; the communications provider should establish communication channels internally and with interconnect partners. All personnel within scope should be fully briefed on the reporting process.

#### Rationale

Without this control threats or incidents may be left to escalate until they have a serious impact on another communications provider.

### 11.2 Reporting information security events

*ISO27002 [1] Section 13.2.1*

#### Control

Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.

#### Guidance

Communications providers must be able to describe the management responsibilities and procedures for a quick, effective, and orderly response to information security incidents on shared technical facilities.

The incident response procedures, in addition to those defined in ISO27002 [1] 13.2.1, must take into account the impact on other communications providers in the facility whether they be the owner or tenant. The procedures should include liaison with interconnected communications providers.

## Rationale

Without this control threats or incidents may be left to escalate until they have a serious impact on another communications provider.

---

## 12 Business continuity management

### 12.1 Including information security in the business continuity management process

*ISO27002 [1] Section 14.1.1*

#### Control

A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.

#### Guidance

Where business continuity plans exist they must maintain your obligation to meet this standard. For example, during an incident, it is not acceptable to rely on personnel who have not met the Screening requirements.

Although one of the primary concerns is to maintain the availability of information following an incident, business continuity processes must ensure that the confidentiality and integrity of information is not compromised during the recovery and restoration phases. ISO27001 14.1.1 contains more detail.

#### Validation

View business continuity plans and validate against controls in this document.

#### Rationale

Without this control an incident requiring the implementation of a business continuity plan may suddenly affect another provider's security stance.

---

## 13 Compliance

### 13.1 Compliance with security policies and standards

*ISO27002 [1] Section 15.2.1*

#### Control

Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

#### Guidance

Managers should regularly review the compliance of information processing within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

If any non-compliance is found as a result of the review, managers should:

- a) determine the causes of the non-compliance;
- b) evaluate the need for actions to ensure that non-compliance do not recur;
- c) determine and implement appropriate corrective action;
- d) review the corrective action taken.

Results of reviews and corrective actions carried out by managers should be recorded and these records should be maintained.

Compliance reviews need not be a blanket approach. They may be various and subject-matter specific, such as firewall rule-sets, administrator log history, on-site checks that verify only authorised personnel are present, and so on. Compliance checking provides the communications provider with a degree of assurance that risks are being mitigated, and as such could be pragmatically programmed to cover areas of concern, or for where no recent events or incidents have occurred. However, compliance with this standard does need to be checked as a whole, albeit annually.

The organisation will need to operate effective corrective and preventive action processes to remedy and learn from non-compliances, and to take into account the two month remedy requirement in the standard. The ISO quality methods are recommended.

### Validation

Managers should report the results to the auditor during any security audit against this standard.

### Rationale

Without this control it is impossible to guarantee any consistency or continuity of the security practices mandated by this document.

## 14 History.

| <b>Document history</b> |          |  |
|-------------------------|----------|--|
| Version                 | Date     | Milestone  |
| 0.0.4                   |          | <p>Final comments, section 14.2 removed.</p> <p>Addition of section on <i>audit and compliance monitoring</i>.</p> <p>Changes for consistency and clarity in section 8.1.</p> <p>Changes to include personnel who have logical access to equipment in interconnect scope.</p> <p>Changed criminal records check wording to match standard assurance documentation.</p> <p>Added “Obligations must be passed on by any third-parties, as appropriate for compliance with the standard, to companies and individuals further down the supply chain.” On page 9 for further clarity about third party agreements.</p> |
| 0.0.5                   | 31/08/09 | Applied NICC Template (IS)   |
| 1.1.1                   | 1/09/09  | Formal Issue   |
|                         |          |  |