ACCESS MANAGEMENT SUB-GUIDELINE

Document Version Control

Date	Author	Version
12 June 2017	DPSA	Version 1.13

Table of Contents

1. INTRODUCTION

The South African Public Service transformation is, at a strategic level, informed by public service-wide strategic priority areas and is guided by principles of equal access to services, increased productivity and lowering of costs. In this regard the continuance of the business of government in support of service delivery is of utmost importance.

As information is the backbone of the achievement of business objectives and government service delivery, security breaches can cause crippling effects detrimental to the functioning of government institutions and service delivery, with major inconveniences to the users of services.

Information security involves the application and management of appropriate security measures that involves consideration of a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimising impacts of information security incidents. Information security includes three main dimensions: confidentiality, availability and integrity.

Confidentiality: information designated as confidential is protected by the system as committed or agreed. Information is not to be made available or disclosed to unauthorized individuals, entities, or processes. Espionage and data theft are threats to confidentiality.

Availability: the system is available for operation and use as committed or agreed property and information is accessible and usable upon demand by an authorised entity. It means to keep services running, and giving administrators access to key networks and controls. Denial of service and data deletion attacks threatens availability.

Integrity: the system processing is complete, accurate, timely, and authorised. It means assessing whether the software and critical data within the institution's networks and systems are compromised with malicious or unauthorised code or bugs. Viruses and malware compromise the integrity of the systems they infect.

Protecting information is an institutional prerequisite and in many cases also an ethical and legal requirement (Refer applicable laws hereunder). Hence a key concern for institutions today is to derive the optimal information security possible.

1.1 Purpose

In order to protect electronic information of an institution it is of the essence to put in place encompassing Access Management and controls, which requires an institutional ICT Access Management policy, system, process and procedures and the allocation of roles, responsibility and accountability.

Access management policies provide the blueprint for the management of user access, authorisations and control mechanisms for computer networks, operating systems, applications and electronic information.

This Access Management sub-guideline (hereafter called the sub-guideline) seeks to assist Information and Communication Technology (ICT) practitioners in the Public Service to craft Access Management Policies that are adapted or suited to their institutional environment.

These Access Management Policies should encompass the institutional security access control focus areas and should as a minimum addresses the following areas:

a) User Access Management;
b) User Responsibilities;
c) Network Access Control;
d) Operating Systems Access Controls;
e) Application and Information Access Control; and
f) Mobile and Remote Computing

This sub-guideline identifies the mechanisms, processes and procedures that restrict access to government electronic information and information assets.

Access restrictions contribute towards protecting government institutions from security threats such as internal and external intrusions. These restrictions are also guided by legislation that protects particular types of information (e.g. personal, sensitive or cabinet confidential) and by business requirements.

For the purpose of this sub-guideline reference to an ‘‘institution’’ means a national department, a provincial department, a municipality or a national or provincial government component as per the Public Administration Management Act, No. 11 of 2014.

1.2 Scope

This sub-guideline describes security requirements to protect electronic information and systems from an access control failure or breach considerations within government institutions.

1.3 Legislative Requirements

Legal prescripts have a bearing on the development of Access Management Policies. These legal prescripts should guide the development, implementation and maintenance of Access Management in the institution

The prescripts mentioned below are not exhaustive. All other relevant prescripts should be considered.

1.3.1 Constitution of the Republic of South Africa No. 108 of 1996 as amended

Section 32 states that everyone has the right of access to any information held by the state and any information that is held by another person and that is required for the exercise or protection of any rights.

Section 195 enshrines principles such as:

(b) to promote the efficient, economic and effective use of resources;

(f) accountability of the public administration; and

(g) fostering of transparency by providing the public with timely, accessible and accurate information.

1.3.2 Promotion of Access to Information Act No. 2 of 2000

Chapter 4, Section 64: Mandatory protection of privacy - Subject to subsection (2), the head of a private body must refuse a request for access to a record of the body if its disclosure would involve the unreasonable disclosure of personal information about a third party, including a deceased individual.

1.3.3 Protection of Personal Information Act No. 4 of 2013

Condition 5 prescribes the quality of information so that personal information is not compromised. Reasonable steps must be taken to ensure that the personal information is complete, accurate, not misleading and up to date and in accordance to the purpose of which personal information is collected or further processed.

Condition 7 addresses Security Safeguards and Section expands on security measures on integrity and confidentiality of personal information. According to Section 19(1) a responsible party must secure the integrity and confidentiality of personal information in its position or under its control by taking appropriate, reasonable technical and organisational measures to prevent:

(a) Loss of, damage to or unauthorised destruction of personal information; and

(b) Unlawful access to or processing of personal information.

In order to give effect to Section 19(1), Section 19(2) requires of the responsible party to take reasonable measures to identify and maintain safeguards against reasonably foreseeable risks to personal information in its possession or under its control.

Section 19(3) specify that the responsible party must have due regard to generally accepted information security practices and procedures which may apply to it.

Section 21 explains security measures applying to information processed by an operator (third party) and occurrences of security breaches where information was compromised.

1.3.4 Electronic Communications Act No. 36 of 2005

Some of the objectives of the Act as related to Access Management are to promote an environment of open, fair and non-discriminatory access to electronic communications networks and services and ensure information security and network reliability.

1.3.5 Public Service Act No. 103 of 1994 as amended

Chapter 6: Access to documents and information by Minister: (1) The Minister, or any person authorised in writing by the Minister, has access to such official documents or may obtain such information from executives authorities and employees in the public service as may be necessary for the performance of his or her functions under this Act or any other law.

1.3.6 Public Administration Management Act No. 11 of 2014

The Public Administration Management (PAM) Act provides for the use of information and communication technologies in the public administration and that information and communication technologies covers all aspects of technology

which are used to manage and support the efficient gathering, processing, storing and dissemination of information.

Section 4 requires that each institution must (b) promote efficient, economic and effective use of resources and (g) foster transparency by providing the public with timely, accessible and accurate information.

Section 14 stipulates that in order to achieve the acceptable use of ICT to deliver services in a secure environment, the head of an institution must—

(a) Acquire and use information and communication technologies in a manner which—

(i) leverages economies of scale to provide for cost effective service;

(ii) ensures the interoperability of its information systems with information systems of other institutions to enhance internal efficiency or service delivery;

(iii) eliminates unnecessary duplication of information and communication technologies in the public administration; and

(iv) ensures security of its information systems;

(b) Use information and communication technologies to develop and enhance the delivery of its services in the public administration;

(c) Align the use by staff of information and communication technologies to achieve optimal service delivery; and

(d) Promote the access to public services through the use of information and communication technologies.

*1.3.7 **Public Service Regulations, 2016***

Section 25 (1) (e) (iii) requires that an executive authority shall prepare a strategic plan for his or her department that specifies information systems that enable service delivery through the use of information and communication technology.

Section 95. (1) A head of department shall ensure the maintenance of information security vigilance at all times in the department.

*1.3.8 **National Archives Act No. 43 of 1996***

Section 12: Access and Use. The National Archives should, in conjunction with those organs of State that originate classified information, establish a

government-wide database of declassified information that heads of organs of State have determined may be made available to the public. Information contained within the database should, at a reasonable cost, be made available and accessible to members of the public.

1.3.9 Minimum Information Security Standards (MISS) 1996

The MISS sets out security measures to protect classified information, including physical security, access control, computer security and communication security.

Chapter 4: Information that is sensitive in nature requires security measures in accordance to the degree of sensitivity. The responsibility for document classification rests with the author, Head of the Institution or his/her delegate.

Access to information is on a need to know basis based on suitable security clearance or authorisation granted. Encryption applies to the transmission of classified electronic information.

Effective access control is required for areas where electronic equipment, which hosts classified information, are kept.

All electronic reproduction equipment should be properly controlled to prevent unauthorised or uncontrolled copying of classified documents.

Chapter 5: All persons who should have access to classified information must be subjected to security vetting. A security clearance gives access to classified information in accordance with the level of security clearance, subject to the need-to-know principle. The MISS provides for specific vetting criteria, security screening procedures and period for the validity of security clearances.

Chapter 7: Where use is made of computer communications and data is transmitted through an unprotected area, the transmission should be protected in accordance with communication security policies/instructions. All breaches of security in the computer environment must be reported as soon as possible in accordance Chapter 9 of the MISS.

1.4 International Standards

This sub-guideline was informed by International standards on Information Security Management (ISM) such as:

- **ISO/IEC 27000** provides an overview of Information security management;
- **ISO/IEC 27001** provides requirements for establishing and maintaining an ISM system to preserve the confidentiality, integrity and availability of

information through appropriate risk management. Guidance is also provided on access control objectives and controls;

- **ISO/IEC 27002** is a code of practice for information security controls addresses inter alia areas such as access control and logs, mobile devices, teleworking, security incident management and legal compliance;
- **ISO/IEC 27003** provides implementation guidance of an information security management system and the establishment of an ICT security environment, policies, structures, roles and responsibilities;
- **ISO/IEC 27033** relates to securing communications between networks and address issues such as prevention of unauthorised/inappropriate access, misuse of assets and unauthorised traffic;
- **ISO/IEC 27035** provides guidance on information security incident management, their causes, detection categorisation and classification.

2. ACCESS CONTROL

To control access to information an Access Management Policy and related controls should be established, documented, and reviewed. This Policy should be based on business and security requirements for access in order to regulate user access to all electronic applications and systems and to prevent and detect unauthorised access.

It is the line manager's responsibility to ensure that access to the systems is regulated.

3. USER ACCESS MANAGEMENT

To ensure authorised user access and to prevent unauthorised access to electronic information systems and services. The prevention of all unauthorised access to electronic information should be managed through inter alia user registration, privilege management, user password management and the review of user access rights and be guided by the prescripts mentioned in paragraph 1.3.

The following topics will be addressed in this section:

3.1 User registration

3.2 Privilege management

3.3 Password management

3.4 Review of user access rights

3.1 User registration

There should be a formal user registration and de-registration procedure in place for granting and revoking access to all electronic information systems and services.

3.2 Privilege management

The allocation and use of privileges should be restricted and controlled.

Electronic systems requiring protection against unauthorised access should have the allocation of privileges controlled through a formal authorisation process and a record of all privileges allocated should be maintained, monitored and audited. The system owner, in collaboration with the operational heads of different branches, should agree on access privileges.

3.3 Password management

The allocation of passwords should be controlled through a formal management process.

In order to prevent unauthorised access to government and an institution's electronic systems, the institution should have a formalised password standard regarding password length and composition, frequency of change and re-use of passwords.

All stored passwords should be encrypted or hashed.

In order to prevent unauthorised access, passwords for logging on to the windows domain should contain a minimum of 8 characters, (as per the AC-T16 password configuration standard).

Users should be required to report any misuse or unlawful use of User ID's and passwords to the Internal Help Desk of the institution. The Help Desk should record it as a security incident and escalate it to the official responsible for information security, through the incident management process, for further action.

Unsuccessful login attempts should be logged and investigations conducted where unsuccessful login attempts are out of the normal range.

3.4 Review of user access rights

Management should review users' access rights at regular intervals using a formal process.

Privileged access rights, which allow super users to override system controls, should be reviewed frequently.

4. USER RESPONSIBILITIES

User Responsibility serves to prevent unauthorised user access, and compromise or theft of information and information processing facilities.

The prevention of all unauthorised access to electronic information should be managed through *inter alia* password use, contract/account termination, unattended ICT equipment, clean desk /screen policy. These should be guided by the prescripts mentioned in paragraph 1.3.

The following topics will be addressed in this section:

4.1 Password use

4.2 Employee, Contract or Account termination

4.3 Unattended user ICT equipment

4.4 Clean desk policy and clear screen policy

4.1 Password use

The allocation of passwords shall be controlled through a formal management process.

All personnel are responsible for all activities performed with their personal user IDs/passwords. Users should be required to follow good security practices in the selection and use of passwords.

Gross negligence or willful disclosure of this information should be treated as a serious offence.

Users should be required to report any misuse or unlawful use of User ID's and passwords to the internal Help Desk of the institution who should incorporate it into the security incident management process of the institution.

4.2 Employee, Contract or Account termination

ICT Management should engage on a regular basis with line management to ensure that any change in employment status of employees, vendors, contractors and third parties are addressed accordingly.

All access rights to the institution's network, systems, application and building facilities must be adjusted upon change or removed upon termination of their employment, contract or agreement.

4.3 Unattended user ICT equipment

Users should ensure that unattended ICT equipment has appropriate protection.

Shutting down a device that does not have the ability to lock is not a control, as these devices can be started up and accessed without authentication.

4.4 Clean desk policy and clear screen policy

A clean desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted to ensure compliance to the Chapter 4 of the MISS.

5. NETWORK ACCESS CONTROL

Network Access Control intends to prevent unauthorised access to networked services.

The policy on the use of network services, user's authentication for connections, equipment identification in networks, remote diagnostic and configuration, segregation of networks, network connection control and network routing control should be guided by the prescripts mentioned in paragraph 1.3.

The following topics will be addressed in this section:

5.1 Policy on use of Network Services

5.2 User Authentication for external connections

5.3 Equipment identification in networks

5.4 Remote diagnostic and configuration port protection

5.5 Segregation in networks

5.6 Network Connection Control

5.7 Network Routing Control

5.1 Policy on use of Network Services

The use of network services should be included in the Access Management policy and related controls.

Users should only be provided with access to the services that they have been specifically authorised to use and approval should be obtained from the GITO.

5.2 User Authentication for external connections

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

5.3 Equipment identification in networks

Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.

5.4 Remote diagnostic and configuration port protection

Physical and logical access to diagnostic and configuration ports should be controlled.

5.5 Segregation in networks

Groups of information services, users, and information systems should be segregated on networks.

Institution and government networks should be segregated into logical and physical segments or network domains based on the value and classification of electronic information or assets that need to be accessed, levels of trust, or lines of business.

5.6 Network Connection Control

For shared networks, especially those extending across the institution's boundaries, the capability of users to connect to the network should be restricted in line with the access control policy and business application requirements.

Any connection to an institution's or government backbone network should be appropriately authorised.

All non-trusted connections such as connections between the internal networks of the institution and the Internet (or any other publicly-accessible electronic networks) should include an approved firewall and related access controls.

A business justification approved by the person responsible for information security and application proxy service via an approved firewall is required.

5.7 Network Routing Control

Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

6. OPERATING SYSTEM ACCESS CONTROL

To prevent unauthorised access to operating systems components such as operational system access control, secure log-on, user identification and authentication, password and management system, use of system utilities, session time and limited connection of time should be addressed and guided by the prescripts mentioned in paragraph 1.3.

The following topics will be addressed in this section:

6.1 Operating system access control

6.2 Secure Log-on

6.3 User Identification and Authentication

6.4 Password Management System

6.5 Use of system utilities

6.6 Session Time

6.7 Limitation of connection time

6.1 Operating system access control

Access to operating systems should be controlled with the utilisation of secure techniques thus ensuring access to authorised users only.

System utilities should be managed and limitations on the use of such systems should be defined.

6.2 Secure Log-on

Access to operating systems should be controlled by a secure log-on procedure.

6.3 User Identification and Authentication

All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.

Multifactor authentication mechanisms should be used when accessing electronic information and building areas classified as confidential, secret and top secret.

6.4 Password Management System

Systems for managing passwords should be interactive and should ensure quality passwords.

6.5 Use of system utilities

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

Administrator and root level system accounts should be strictly controlled.

Processes should be in place to control the allocation, revocation, and review of powerful access-rights. These processes should include authorisation of all access-rights by the appropriate line management, and mechanisms to ensure access-rights are adjusted appropriately should the person leave, or change job description.

Critical logical access activities performed utilising powerful access-rights should generate audit trails, and be logged. All audit trails and logs should be reviewed periodically and stored for a period of 1 year.

The Head of the Institution reserves the right to adjust, suspend, or permanently revoke powerful access-rights at any time, without notice, discussion or disclosure at the entire discretion of the information owner.

Powerful users should be given their own unique usernames, and therefore no system generic usernames will be used. Powerful users may not share usernames.

There should be a procedure allowing staff to obtain emergency access.

Assigning of emergency access should be reported to IT Operations management and reviewed subsequent to the event, where after this access should be revoked.

6.6 Session Time

Inactive sessions should shut down after a defined period of inactivity.

6.7 Limitation of connection time

Restrictions on connection times should be used to provide additional security for high-risk applications.

7. APPLICATION AND INFORMATION ACCESS CONTROL

To prevent unauthorised access to information held in application systems, components such as information access restriction and sensitive system isolation should be guided by the prescripts mentioned in paragraph 1.3.

The following topics will be addressed in this section:

7.1 Information access restriction

7.2 Sensitive system isolation

7.1 Information access restriction

Logical access controls should be applied to protect application systems and data from unauthorised access.

Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.

7.2 Sensitive system isolation

Sensitive systems should have a dedicated (isolated) computing environment.

Processes and standards to isolate sensitive application systems and related processing environments should be defined and applied.

8. MOBILE COMPUTING AND TELEWORKING

To ensure information security when using mobile computing and teleworking facilities, mobile computing and communications and teleworking should be guided by the prescripts mentioned in paragraph 1.3.

The following topics will be addressed in this section:

8.1 Mobile computing and communications

8.1.1 Remote Access

8.1.2 Equipment

8.1.3 Risk Management

8.1.4 Teleworking

8.1 Mobile computing and communications

A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.

A procedure for remote user access authorisation and management should be established. This includes mobile work or work done during travel but excludes teleworking.

8.1.1 Remote Access

Remote access will only be permitted on written authorisation from the system owners.

All remote access logs will be monitored on a regular basis for failed access attempts, user lockouts and unusual remote access times.

Users should be prohibited from altering or disabling any security features that have been enabled on wireless connections.

Government employees or other personnel should be prohibited from establishing simultaneous connections to external networks and government and/or the institution’s networks.

Users should be prohibited from allowing wireless devices such as cellular telephones and PDA from acting as wireless access points allowing access to laptop computers.

When establishing any alternate connection to any external network, users should ensure that their electronic devices are disconnected from all

government/institutional networks. Such connections include but are not limited to 3G, GPRS, ADSL, Modems, Wireless, etc.

8.1.2 Equipment

All equipment (whether government owned, personal or external party owned) that is used to connect to government's or the institution's networks should meet the government requirements for remote access (hardware and software).

All implementations should support a hardware address that can be registered and tracked.

Equipment identification scans should be performed periodically to identify any unauthorised equipment used to connect to the network.

All computers with wireless Local Area Network (LAN) devices should utilise an approved institutional or government Virtual Private Network (VPN) configured to drop all unauthenticated and/or unencrypted traffic.

Wireless implementations should maintain point to point hardware encryption in accordance with the public service encryption standard.

8.1.3 Risk Management

A formal risk analysis process should be conducted for applications to which remote access is granted, to assess risks and identify controls needed to reduce risks to an acceptable level.

All system owners (persons responsible for individual applications) are responsible for ensuring the risk analysis is performed.

8.1.4 Teleworking

A policy, depicting security measures, operational plans and procedures should be developed and implemented for teleworking activities, allowing an employee to perform authorised work activities from an alternative approved worksite other than the official office worksite. This does not include mobile work or work done during travel

8.2 PHYSICAL ACCESS MANAGEMENT

An institution should prevent unauthorized physical access, damage, and interference to the organization's premises and information. Critical and sensitive information processing facilities (i.e. data centers) should be housed in secure

areas, protected by defined security perimeters, with appropriate security barriers and entry controls.

9. AUDITING

All user and system activities should be logged.

System Owners should allocate audit storage capacity to reduce the likelihood of such capacity being exceeded.

Network, system and application owners should review audit logs on a regular basis for irregularities.

Critical logical access activities performed utilising powerful access-rights should generate audit trails, and be logged.

All audit trails and logs should be reviewed on a monthly basis by the information owner and stored for a period of 1 year.

10. GLOSSARY

Access Control – A set of rules and procedures implemented within hardware and software to provide for the identification of users, the granting and denying of access, the recording of access attempts, and the administrative tools necessary to manage and monitor access activities.

https://msdn.microsoft.com

Access rights – the permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within the system, as defined by rules established by data owners and the information security policy.

Accountability – the ability to map a given activity or event back to the responsible party to make an individual accountable for their actions.

https://www.isaca.org

Asset - is a major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems.

Audit trail – A series of records either in hard copy or in electronic format that provide a chronological record of user activity and other events that show the details of user and system activity.

Authentication – Is any process by which a system verifies the identity of a User who wishes to access it. Since Access Control is normally based on the identity of the User who requests access to a resource.

Confidentiality – The protection of sensitive or private information from unauthorised disclosure.

Minimum Information Security Standards

Sub-Guidelines – These are guidelines referred to on the issued ICT security guidelines

Institution – means a department or constitutional institution

www.dpsa.gov.za

Individual Accountability – requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of this rules.

www.isaca.org

Information Asset – Information asset refers to any applications, servers, workstations and building facilities that belongs to a department.

Information security – is the prevention of, and recovery from, unauthorised or undesirable destruction, modification, disclosure, or use of information and information resources, whether accidental or intentional.

Information Owner – is responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains the responsibility even when the data/information is shared with other organizations.

Integrity – The accuracy, completeness and validity of information in accordance with business values and expectations.

https://www.isaca.org/

Line Management – It is the administration of activities that contribute directly to the output of products or services in an environment.

Multifactor authentication: Multi-factor authentication, also known as Two-factor authentication, is an approach to authentication which requires the presentation of two or more of the three authentication factors: a knowledge factor ("something the user knows"), your User ID, a possession factor ("something the user has") PIN or password, and an inherence factor ("something the user is") your fingerprint.

www.mcafee.com

Networks –Communications capability that allows one user or system to connect to another user or system and can be part of a system or a separate system.

Privilege – a special right, advantage, or immunity granted or available only to a particular person or group on the system

Procedures – A detailed description of the steps necessary to perform specific operations in conformance with applicable standards.

Remote Access – is the ability to get **access** to a computer or a network from a **remote** distance.

Risk – is the possibility of harm or loss to any software, information hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

https://www.prince2.com

Standards – Definition of the metrics used to determine the correctness of a thing or process; A set of rules or specifications that, when taken together, define a software or hardware device.

System – is a generic term used for briefness to mean either a major application or general support system.

System Owner – is a key contributor in developing **system** design specifications to ensure the security and user operational needs are documented, tested, and implemented.

Threat – is an event or activity, deliberate or unintentional, with the potential for causing harm to an IT system or activity.

User – IS an employee, contractor or anyone with management approved access to information and information assets. Users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers).

11. REFERENCES

[1] Constitution of the Republic of South Africa No. 108 of 1996 as amended

[2] Public Service Act No. 103 of 1994 as amended

[3] Minimum Information Security Standards (MISS) of 1996

[4] Promotion of Access to Information Act 2 of 2000

[5] South Africa. Electronic Transactions and Communication Act No 25 of 2002

[6] Electronic Communications Act No. 36 of 2005

[7] King Code III of Governance. 2009.

[8] Protection of Personal Information Act No. 4 of 2013

[9] Public Administration Management Act No 11 of 2014

[10] Public Service Regulations, 2016

[11] National Archives Act No. 43 of 1996

[12] International Organization for Standardisation: ISO / IEC 27000, 2014. Information technology – Security techniques – Information security management systems – Overview and vocabulary

[13] International Organization for Standardisation: ISO / IEC 27001, 2013. Information Technology – Information Security Management Systems – Requirements

[14] International Organization for Standardisation: ISO / IEC 27002, 2013. Information Technology – Code of Practice for information security controls

[15] International Organization for Standardisation: ISO / IEC 27003, 2010. Information technology – Security techniques – Information security management system implementation guidance

[16] International Organization for Standardisation: ISO / IEC 27033, 2014. Information technology – Security techniques – Securing communications between networks using security gateways

[17] International Organization for Standardisation: ISO / IEC 27035, 2011. Information technology – Security techniques – Information security incident management