Eskom	Standard	Group Technology

Title: **CYBER SECURITY STANDARD FOR OPERATIONAL TECHNOLOGY**

Unique Identifier:	**240-55410927**
Part	**Smart Grid**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**0**
Total Pages:	**33**
Next Review Date:	**March 2018**

Disclosure Classification: **Controlled Disclosure**

Compiled by

Johan Botha

Senior Consultant

Date: 21/02/2013

Approved by (SCOT SC Chairperson)

Philip Groenewald

Chairperson - SCOT Smart Grid Technologies Study Committee

Date: 21/02/2013

Functional Responsibility

Philip Groenewald

Smart Grid Technologies Manager

PTM&C CoE

Date: 21/02/2013

Functional Responsibility

Richard Mccurrach

Senior Manager

PTM&C CoE

Date: 21/2/2013

Authorized by

Prince Moyo

Power Delivery Engineering GM

Date: 22/2/2013

ESKOM COPYRIGHT PROTECTED

Content

Foreword

Not applicable.

Revision history

This is a new document.

Date	Rev.	Compiled By	Clause	Remarks
March 2013	0	J Botha	Clause no.	First issue.

Acceptance

This document has been seen and accepted by:	
Name	**Designation**
P Moyo	Power Delivery Engineering GM
R Mccurrach	Senior Manager – PTM&C CoE
P Groenewald	Smart Grid Technologies Manager - PTM&C CoE
B A Dames	Chief Executive
E Johnson	Group Executive (Enterprise Development)
P O' Flaherty	Finance Director
B Bulunga	Group Executive (Human Resources Division)
M Ntsokolo	Group Executive (Transmission Division)
Dr S J Lennon	Group Executive (Sustainability)
A Noah	Group Executive (Distribution Division)
D Marokane	Group Executive (Technology and Commercial)
T Govender	Group Executive (Generation Division)
T Molefe	Group Executive (Customer Service)

This standard shall apply throughout Eskom Holdings Limited, its divisions, subsidiaries and entities wherein Eskom has a controlling interest

Development team

The following people were involved in the development of this document:

- The OT Cyber Security Workgroup
- The OT Cyber Security Committee

Purpose

The purpose of this document is to ensure that all necessary measures are taken to ensure that the Eskom business continuity is not affected due to any cyber type of incident. It is recognised that there is a difference in the operation and risks associated with the technical assets of the business, as compared to the conventional Information Technology systems. Although there is increasing convergence of the IT technology utilised in both systems, there are unique differences in its application in the Operational Technology systems, and they require a dedicated security approach as described in this Standard.

Applicability

This document shall apply to the Operational Technology environments throughout Eskom Holdings Limited.

Overview

Exploitation of vulnerabilities in computer systems has been growing in frequency and impact for the last decade. Forms of cyber-terrorism have also occurred where industrial systems were deliberately targeted. Detailed security policies need to be formulated and implemented to ensure that the Operational Technology networks and systems in Eskom are protected.

From a security perspective, the management of Eskom's Operational Technology network resources are critical. Weaknesses in network infrastructure and the associated protocols used within these areas are prone to being exploited if employee and management vigilance is not active at all times. Global IT and interconnected systems, expose operational systems of utilities to attacks and Eskom is not exempt from such risks, hence the need to monitor and track vulnerabilities continuously. The success of any security standard implementation hinges on constant review, testing, updating and re-formulating the necessary strategies as issues and risks are encountered.

Introduction

This standard serves to guide the implementation of Cyber Security Principles in the Operational Technology (OT) environment. Although there is a convergence between Operation Technology and Information Technology, the standard practices of Information Technology (IT) are not directly applicable to OT, as OT generally requires stricter access control of external information, and the compromise of such information could have a greater impact. Furthermore, due to the lifespan of OT systems, they run for many years after support ends and for these reasons IT security policies can normally not be implemented in the OT environment without major modification.

This standard applies to the Operational Technology environment where there are Cyber Assets installed. A Cyber Asset is an asset that can be accessed by a routable protocol from or through a non OT environment. This standard divides Cyber Assets according to criticality, and defines rules for protecting the different types. OT System Owners should ensure the systems they are responsible for adheres to the requirements in the standard, and to justify deviations where adherence could not be achieved.

The statements in the document were assigned numbers to indicate criticality, where 1 is most critical, 2 is less critical and 3 is least critical. The purpose of this assignment is, during implementation, to put focus on the most critical areas first to ensure the highest risks are addressed quickly.

Keywords

Cyber, Operational Technology, security

Bibliography

1) Standard CIP-001-1 — Sabotage Reporting

2) Standard CIP–002–3 — Cyber Security — Critical Cyber Asset Identification

3) Standard CIP–003–3 — Cyber Security — Security Management Controls

4) Standard CIP–004–3 — Cyber Security — Personnel and Training

5) Standard CIP–005–3 — Cyber Security — Electronic Security Perimeter(s)

6) Standard CIP-006-3c — Cyber Security — Phys ical Security

7) Standard CIP–007–3 — Cyber Security — Systems Security Management

8) Standard CIP–008–3 — Cyber Security — Incident Reporting and Response Planning

9) Standard CIP–008–3 — Cyber Security — Incident Reporting and Response Planning

10) Eskom Information Security Policy 32-85

1 Scope

The primary aim of this document is to provide guidance on implementing an acceptable level of protection against cyber intrusions and malware in Operational Technology environments within Eskom.

Operational Technology (OT) Systems are defined as follows in the Definition of operational technology (OT) and OT / IT collaboration accountabilities document:

"In the Eskom context Operational Technology (OT) is defined as:

Operational systems which form **part of** Eskom's **plant / network assets**, and which could by virtue of design, maintenance or operation **directly** result in the failure of these assets to meet their **purpose and performance criteria**, where:

1) **Operational systems:** are all systems (including electronic, telecommunications and computer systems and components) which process, store or communicate operational data or information.

2) **Part of:** means contribute to the asset meeting its purpose and performance criteria.

3) **Plant / network assets:** are any part of the "built environment" utilized by Eskom to run its production, delivery and logistics processes, including generation, transmission and distribution of electricity, etc.

4) **Directly:** means in real time or near real time. E.g. would include supervisory control systems, but would exclude spares ordering applications (even though these could eventually result in the failure of the asset).

5) **Purpose and performance criteria:** The "design to", "maintain to" and "operate to" criteria that are generally specified formally.

Systems, sensors, transducers and Programmable Local Controller equipment, which extract signals and measurements from the plant / network asset or its control environment, or facilitate control over the these assets generally meet the above criteria and qualify as OT, since their failure could directly result in the failure of the plant / network asset or its ability to meet its purpose and performance criteria.

In some cases, obvious failures of **operational systems** may not directly result in the failure of purpose or performance of the **plant / network asset**, but because of the way it is designed, normal operations or maintenance of the operational system could result in a risk to the plant / network asset. An example is:

- Voltage spike induced in a control circuit due to a lightning strike on the power supply of an IT server not fitted with the same spec of surge protection as used on the control circuit, and inadequate voltage supply decoupling (e.g. optical decoupling).

Such equipment generally meets the above criteria and qualifies as OT, since their design, operation or maintenance could directly result in the failure or impact of the plant / network asset or its ability to meet its purpose and performance criteria."

2 Normative references

Parties using this document shall apply the most recent edition of the documents listed below:

International document(s):

This Standard is based on the requirements defined in the NERC Critical Infrastructure Protection (CIP) guidelines. Eskom specific requirements have been tailored to the Eskom environment, however the intent remains the same. As these CIP guidelines are updated from time to time, they will be periodically reviewed to assess if specific changes to the standard are required.

Standard CIP-001-1 — Sabotage Reporting

Standard CIP–002–3 — Cyber Security — Critical Cyber Asset Identification

Standard CIP–003–3 — Cyber Security — Security Management Controls

Standard CIP–004–3 — Cyber Security — Personnel and Training

Standard CIP–005–3 — Cyber Security — Electronic Security Perimeter(s)

Standard CIP-006-3c — Cyber Security — Physical Security

Standard CIP–007–3 — Cyber Security — Systems Security Management

Standard CIP–008–3 — Cyber Security — Incident Reporting and Response Planning

Standard CIP–009–3 — Cyber Security — Recovery Plans For Critical Cyber Assets

ESKOM COPYRIGHT PROTECTED

When downloaded from the IARC WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the WEB.

South African National document(s):

Minimum Information Security Standards (MISS)

National Key Points Act

Eskom National document(s):

32-9: Definition of Eskom documents.

32-85: Information Security Policy

32-644: Eskom documentation management standard.

474-65: Operating Manual of the Steering Committee of Wires Technologies (SCOWT)

240-55863502: Definition of Operational Technology (OT) and OT/IT Collaboration Accountabilities

Eskom Divisional documents(s):

None

3 Definitions and abbreviations

3.1 Definitions

System Owner: The system owner, is the authorised Eskom representative that has overall accountability for the OT system in which the cyber asset resides

Cyber Security: Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality

Cyber Asset: Programmable electronic devices and communication networks including hardware, software, and data, that is connected to a network with a routable protocol.

Critical cyber assets: Cyber assets essential to the reliable operation of critical assets.

Logical Access: Being able to interact with data through access control procedures such as identification, authentication and authorization.

Physical access: Being able to physically touch and interact with the computers and network devices.

Routable Protocol: A communications protocol that contains a network address as well as a device address. It allows packets to be forwarded from one network to another.

ESKOM COPYRIGHT PROTECTED

When downloaded from the IARC WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the WEB.

Non-routable Protocol: A communications protocol that contains only a device address and not a network address. It does not incorporate an addressing scheme for sending data from one network to another.

Public domain: published in any public forum without constraints (either enforced by law, or discretionary).

Controlled disclosure: controlled disclosure to external parties (either enforced by law, or discretionary).

Confidential: the classification given to information that may be used by malicious/opposing/hostile elements to **harm** the objectives and functions of Eskom Holdings SOC Limited.

Secret: the classification given to information that may be used by malicious/opposing/hostile elements to **disrupt** the objectives and functions of Eskom Holdings SOC Limited.

Top Secret: the classification given to information that may be used by malicious/opposing/hostile elements to **neutralize** the objectives and functions of Eskom Holdings SOC Limited.

3.2 Abbreviations

AES	Advanced Encryption Standard
CD	Compact Disc
CIP	Critical Infrastructure Protection
DDS	Detailed Design Specification
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Dynamic Name Server
DR	Disaster Recovery
DVD	Digital Versatile Disc
FAT	Factory Acceptance Test
FDS	Functional Design Specification
GPRS	General Packet Radio Service
GUI	Graphical User Interface
HMI	Human Machine Interface
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control

MW	Megawatt
NAT	Network Address Translation
NERC	North American Reliability Council
OS	Operating System
OT	Operational Technology
SAT	Site Acceptance Test
SCSI	Small Computer System Interface
TCP	Transport Control Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VM	Virtual Machine

4 Requirements for Cyber Security Management

4.1 Sabotage Reporting

Sabotage reporting is the responsibility of the Corporate Security Department in Eskom. All OT environments shall comply with the Corporate Security Department policies, processes, standards and procedures regarding sabotage reporting.

4.2 Cyber Asset Identification

To enable an appropriate security framework for the monitoring and protection of Critical Assets needed to support reliable operation of the electricity supply network, it is required that a comprehensive identification process be followed to capture and record all critical cyber assets.

The methodology described to in 4.2.1.2 identify critical cyber assets shall be applicable to:

- Control centres and backup control centres
- Distribution and Transmission substations
- Generation resources
- Telecommunication control and backup centres
- Systems and facilities critical to the power system restoration, such as blackstart
- Automatic load shedding schemes and special protection systems
- Any additional assets that support the reliable operating, control and protection of the power system.

ESKOM COPYRIGHT PROTECTED

4.2.1 Critical Cyber Asset Identification Method

4.2.1.1 Identify Critical Assets

The criticality of OT systems can be identified by evaluating its risk exposure (impact and probability) on the ability of Eskom to supply electricity. If, during the specific OT system, or group of systems sharing common technology, under consideration, it is identified that one or more of the following situations could occur due to the OT systems being compromised or have unplanned unavailability, it would be regarded as a Critical System. (Note: to assess criticality, likelihood has been ignored, and only the consequence is used – i.e. Risk Control measures are assumed not in place).

- Result in immediate production losses on multiple Generating units involving a total capacity of ≥ 1 000 MW or sufficient capacity to initiate an under frequency incident
- Result in immediate power delivery loss on the network, resulting in >10,000 general customer disconnection ≥4 hrs.
- Result in immediate power delivery loss on the network, resulting in disconnection of a key customer in contravention of contractual conditions.
- Interruption of the equivalent of 500 MW production for > 1 week
- Interruption of the power delivery equivalent of 50MW on the network, resulting in customer loss of supply > 12hrs
- Compromise of a generation facility's ability to perform black starting
- Seriously injure or kill one or more persons
- Result in a significant environmental contravention situation
- Reduction of life of a significant plant Asset (value ≥ R250 million) by > 20%
- Significantly violating National legislation, policy, licence or permit conditions
- Increasing the longer term production costs of a plant by >20%
- Negatively expose any part of Eskom to national media for ≥ 2 weeks
- Reducing the level of back-up redundancy provided to a significant plant for ≥ two weeks
- Compromise the integrity of, or alter in any way the protection devices, functions, settings or philosophy of significant plant
- Loss in the ability to perform emergency switching according to the definitions of the Plant Safety Regulations and the Operating Regulations for High Voltage Systems
- Initiate the activation of disaster recovery/management plans at an Eskom site
- Under certain situations, auxiliary systems that support Critical Assets should also be considered as critical – these include the access control systems, fire detection systems, power supply systems etc.

4.2.1.2 Identify Critical Cyber Assets

Any Cyber Asset which is essential in the operation of a Critical Asset can be a Critical Cyber Asset.

If this Cyber Asset has one of the following characteristics it shall be deemed as a Critical Cyber Asset:

- It uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- a non-routable protocol is used, but it is connected to a data concentrator, which uses a routable protocol outside the Electronic Security Perimeter.

- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is accessible via dial-up or a Virtual Private Network (VPN).

The following diagrams illustrate which cyber assets are regarded as critical cyber assets in various scenarios:

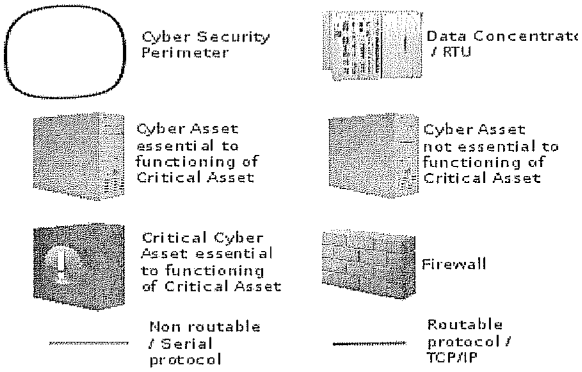
Cyber Security Perimeter
Data Concentrat
/ RTU
Cyber Asset essential to functioning of Critical Asset
Cyber Asset not essential to functioning of Critical Asset
Critical Cyber Asset essential to functioning of Critical Asset
Firewall
Non routable / Serial protocol
Routable protocol / TCP/IP

Figure 1: Legend of symbols

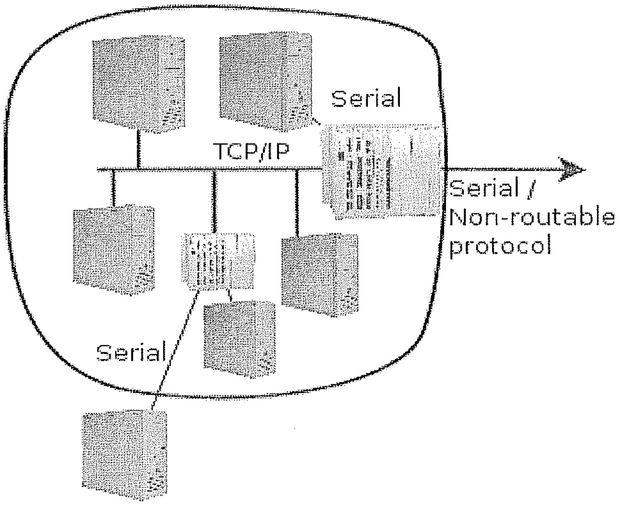

Figure 2: Substation with non-routable protocol connection

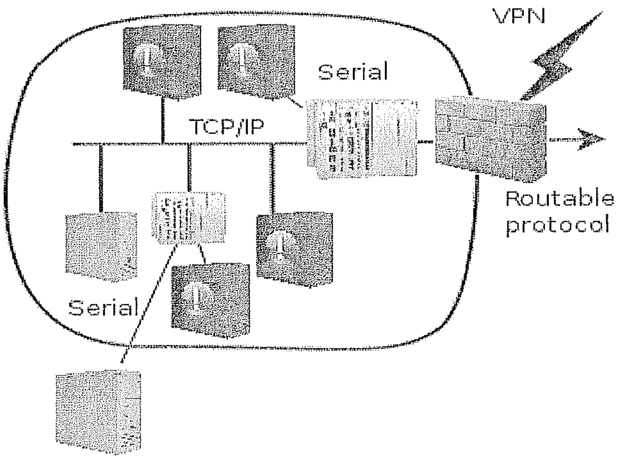

Figure 3: Substation with routable protocol connection

ESKOM COPYRIGHT PROTECTED

When downloaded from the IARC WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the WEB.

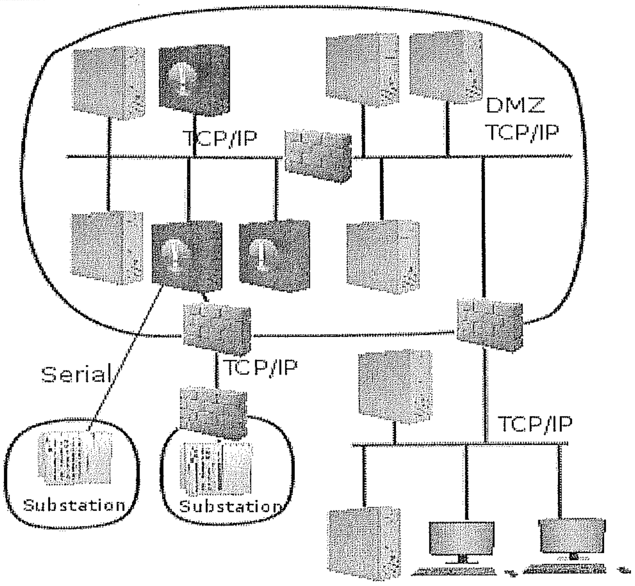

Figure 4: Master station / Data centre

4.2.2 Critical Cyber Assets Identification

a) The *system owner* shall identify the list of critical cyber assets by using the Critical Cyber Asset Identification method prior to putting of the cyber asset in operation. This information shall be formally recorded for control purposes.

b) The *system owner* shall review the list of critical cyber assets annually and after changes in the operating environment or changes to the cyber asset.

c) The *system owner* shall retain an audit trail of the reviews.

4.3 Security Management Controls

4.3.1 Leadership

a) The relevant authority shall be responsible for the implementation of the Cyber Security Standard for Operational Technologies.

4.3.2 Exceptions

a) Any deviation from the Cyber Security Standard for Operational Technologies must be approved by the Architecture Design Review committee or the delegated authority and documented, by the system owner, within 30 days of said approval. Documented exceptions to the cyber security standard must include an explanation as to why the exception is necessary and any compensating measures that was put in place to mitigate possible risk.

b) Authorized exceptions to the cyber security standard shall be reviewed and approved annually by the Architecture Design Review committee or the delegated authority to ensure the exceptions are still required and valid. Such review and approval shall be documented.

4.3.3 Information Protection (3)

a) The *system* owner shall be responsible to manage access to protected critical cyber asset information. This shall include:

- maintaining a list of designated personnel, by name and title, for authorising logical or physical access to protected information,
- the information the designated personnel can authorise access on.

b) The system owner shall review the list of designated personnel annually.

c) The designated personnel shall review the list of granted access privileges annually.

4.3.4 Change Control and Configuration Management (3)

Changes to critical cyber asset hardware or software shall be performed according to a formal change control procedure. The change control procedure shall ensure that supporting configuration management activities to identify control and document all Eskom or supplier related changes to hardware and software components of critical cyber assets are reviewed for relevancy and impact (business, technical and financial).

a) At minimum the change control procedure for planned changes shall include:

- a description of the proposed change,
- test procedure and roll-out plan and fallback plan,
- test results of testing in a non-production environment,
- results from commissioning.
- time & duration
- the risk the system is exposed to in implementing the change

b) Change control shall follow the Engineering Change Control Process as per the B2B. The change control shall be take into consideration breakdown versus planned maintenance.

c) Changes to a cyber-asset shall follow the accepted engineering practice for testing, and approved before implementation.

d) Any software change and/or update shall be controlled, where available, with version control and/or supporting documentation.

e) Fall-back procedures for aborting and recovering from unsuccessful changes shall be available and/or communicated.

f) Emergency changes shall be recorded.

g) The documentation for critical cyber assets shall be current, and shall not be kept in the same secure environment or better than that of the cyber asset, and may be kept on the device if a backup device is in place.

h) The decommissioning of any cyber asset shall follow only after verifying that the cyber asset is no longer required or an upgrade/replacement is being installed. The decommissioning procedure shall include the removal of software and information available from the cyber asset. Sensitive software and information shall be securely removed.

i) The use of live data for testing new system or system changes may only be permitted where adequate controls for the security of the data are in place.

4.4 Personnel and Training

It is required that personnel having authorised cyber or authorised unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness prior to being granted access to the system.

4.4.1 Awareness (3)

The *System Owner* shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorised cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.

a) Personnel security responsibilities shall support the Conditions of Service and ensure compliance during an individual's employment.

b) Users' cyber asset security roles and responsibilities shall be documented by the *System Owner*.

c) A cyber asset security awareness program shall be implemented to ensure personnel receive on-going reinforcement in sound security practices on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

4.4.2 Training (3)

a) The attendance records and date the training, at least annual, was completed shall be kept for at least one year by the *System Owners*.

b) Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets, and include, the following required items appropriate to personnel roles and responsibilities:

- The proper use of Critical Cyber Assets;
- Physical and electronic access controls to Critical Cyber Assets;
- The proper handling of Critical Cyber Asset information; and,
- Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

4.4.3 Personnel Risk Assessment (3)

a) New employees' references must be verified.

b) Employees with access to Critical Cyber Assets must be vetted through the Eskom vetting process.

c) The terms and conditions of employment shall include the requirements for compliance with this security standard.

d) Employee's compliance with this security standard, other standards and procedures shall be monitored.

e) All employees shall sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after contractual relations with Eskom.

f) Eskom management has the option of revoking the user's access on notification of resignation or change of job or responsibilities, if the risk is deemed unacceptable.

g) Personnel security responsibilities shall support the Conditions of Service and ensure compliance during an individual's employment.

h) The System Owner can request the risk assessment of employees with access to the system to be reviewed.

4.4.4 Access to Evidence (3)

a) The *System Owner* shall have action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident. These action plans shall ensure that evidence is kept in an unaltered state by cloning the data / machine onto a write-once dvd, or similar procedure.

b) Where Eskom has reasonable grounds to suspect that its security has/is being compromised, Eskom reserves the right to:

- Intercept and peruse any data sent, received or stored by an employee (including any attachment thereto) and to monitor the use of its cyber asset including, but not limited to, hard drives, network drives and other computing systems.
- Conduct inspections of the cyber asset without advance notice to the employees,
- Examine the contents of any cyber asset that contains or is thought to contain Eskom information, including computers that have been purchased by the employees in their personal names and/or capacities.

4.5 Cyber Security — Electronic Security Perimeter(s)

4.5.1 Electronic Security Perimeter

System owners shall identify the Electronic Security Perimeter of their systems. Any access point to the system with a routable protocol crossing the perimeter will be an access point into the system.

a) Access points to the Electronic Security Perimeter can be dial-up modems or VPNs used to retrieve information or to do perform maintenance and configuration on equipment. These remote access connections shall comply to the Information Security – IT/OT Remote Access Standard. (1)

b) All of these access points shall be documented. Any 3G type connections shall also be through a VPN to a central point, where user authentication is done before access is granted to a remote 3G device. All 3G devices shall use an Eskom approved APN and traffic on the 3G network shall be encrypted. Any SIM card shall be locked to the device it is assigned to, to ensure a lost SIM cannot be used by a third party. (2)

c) Dial-up connections shall be from a central point. The remote modem shall only answer calls from authorised pre-programmed numbers. (2)

d) A user shall only have access to devices he is authorised to connect to. (1)

e) Logs should be sent to a log server, and usernames and passwords shall be managed through AAA and a TACACS or radius server. (2)

ESKOM COPYRIGHT PROTECTED

When downloaded from the IARC WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the WEB.

f) Serial communication links are not considered access points, as they use a non-routable serial protocol, as long as both sides of the link fall within an Electronic Security Perimeter.

g) For a Master Station or a Data Centre where data or information is accessed by individuals or systems outside the Electronic Security Perimeter, a Demilitarized Zone (DMZ) shall be established. (1)

h) No Critical Cyber Asset shall reside in the DMZ. (1)

i) No Cyber Asset on the internal secure network shall be directly accessible from a system outside the Electronic Security Perimeter. (1)

j) 802.11 Wi-Fi and Bluetooth networks shall not be used on the Networks in the Electronic Security Perimeter, as it reduces security by eliminating the possibility op implementing physical security to the Cyber Security Perimeter. (1)

k) Where Wireless networks such as GPRS are used for telecommunications, the information shall be encrypted on the link layer with at least 128 bit AES. (2)

l) All cyber security logs, configuration, network layouts, procedures, Disaster Recovery (DR) Plans shall remain within the Secure Perimeter and shall not be referenced in external documents. (1)

m) Where no DMZ is implemented, and ad-hoc connections out of or into the security perimeter are required, perimeter firewalls should be opened and then immediately closed, after completion, instead of leaving them open. The firewall shall only allow access from / to the required source / destination on the required port. (1)

4.5.2 Electronic Access Controls

The *System Owner* shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

a) These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified. (1)

b) At all access points to the Electronic Security Perimeter(s), the *System Owner* shall enable only ports and services required for operations and shall document, individually or by specified grouping, the configuration of those ports and services. (1)

c) Where external interactive access into the Electronic Security Perimeter has been enabled, the System Owner shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible. (2)

d) Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within the Electronic Security Perimeter. (1)

e) The required documentation shall, at least, identify and describe: (3)

- The processes for access request and authorization.
- The authentication methods.
- The review process for authorization rights.
- The controls used to secure VPN access connections.

f) Devices that are capable of configuring a banner shall contain a banner similar to the following: (3)

```
****************************************************************************************************
*                                                                                                  *
*  WARNING  Access to this system is restricted to Authorized Personnel only                       *
*                                                                                                  *
    * Terminate this session immediately if this system has been accessed in error  *
*                                                                                                  *
*  You are warned:                                                                                 *
*                                                                                                  *
*   a) That unauthorised access to or modification of information held in this                   *
*    system,                                                                                       *
*    and/or;                                                                                       *
*   b) Unauthorised copying of software; shall render you liable to civil damages                 *
*    and/or criminal penalties in South Africa and other countries;                                *
*    and;                                                                                          *
*   c) That all sessions on this system are monitored, logged and recorded.                       *
*                                                                                                  *
*  By continuing with this session you represent and warrant that you are                         *
*   authorised to access this system.                                                              *
*                                                                                                  *
****************************************************************************************************
```

4.5.3 Monitoring Electronic Access

The System Owner shall implement and document a process for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

a) For dial-up accessible Critical Cyber Assets that use non-routable protocols, the System Owner shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible. (2)

b) Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the System Owner shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days. (2)

c) Firewall rules allowing access from outside the Electronic Security Perimeter should be set to at least log successful logins and failed attempts. (2)

d) All firewall rules shall have the identity of the person making the change, the date implemented, and the reason for the change in the description field. (1)

4.5.4 Cyber Vulnerability Assessment

The System Owner shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, as a minimum, the following:

a) A document identifying the vulnerability assessment process; (3)

b) A review to verify that only ports and services required for operations at these access points are enabled; (1)

c) The discovery of all access points to the Electronic Security Perimeter; (1)

d) A review of controls for default accounts, passwords, and network management community strings; (1)

e) Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan. (1)

4.5.5 Documentation Review and Maintenance

The System Owner shall review, update, and maintain all documentation to support compliance with the requirements of this security standard.

a) The System Owner shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change. (1)

b) The System Owner shall retain electronic access logs for at least ninety calendar days. (2)

4.6 Cyber Security — Physical Security of Critical Cyber Assets (2)

The facilities chosen to locate information resources and to store data must be suitably protected from physical intrusion, theft, fire, flood and other hazards.

a) Information resources premises must be safeguarded against unlawful and un-authorised physical intrusion.

b) When locating information resources and other hardware, suitable precautions are to be taken to guard against the environmental threats of fire, flood, hazardous material and excessive ambient temperature / humidity.

c) All computer premises must be protected from un-authorised access using an appropriate balance between simple ID cards to more complex technologies to identify, authenticate and monitor all access attempts.

d) All employees are to be aware of the need to challenge strangers on Eskom premises.

e) Criteria shall exist for the categorisation of all information resource areas, and the appropriate control requirements developed for each category.

f) Photographic, video, audio or other recording equipment shall not be used in an area housing critical information resources as categorised.

g) Procedures shall be developed to address secure disposal of information resources.

ESKOM COPYRIGHT PROTECTED

When downloaded from the IARC WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the WEB.

h) Agreements shall be in place to ensure the security, and confidentiality of information stored on information resources that are subject to third party repair and maintenance.

i) The System owner will be responsible to grant physical access to cyber assets

4.6.1 Physical Security Plan

A physical security plan, approved by the senior manager or delegate(s) shall be documented, implemented and maintained. The plan shall address, at a minimum, the following:

a) All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets. (1)

b) The identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points. (1)

c) Processes, tools, and procedures to monitor physical access to the perimeter(s). (2)

d) Appropriate use of physical access controls, including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls. (2)

e) Review of access authorization requests and revocation of access authorization (2)

f) A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing as a minimum the following:

- Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters. (2)
- Continuous escorted access of visitors within the Physical Security Perimeter. (1)

g) Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

h) Annual review of the physical security plan. (2)

4.6.2 Protection of Physical Access Control Systems

Protection of physical Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

a) Be protected from unauthorised physical access. (1)

b) Be protected from unauthorised logical access to the same level as other Critical Cyber Assets. (1)

4.6.3 Protection of Electronic Access Control Systems

a) Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter in Eskom. (1)

ESKOM COPYRIGHT PROTECTED

b) Management of the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside in an Electronic Security Perimeter and protected from external access to the same level as the Critical Cyber Asset. (1)

c) The access control to a Critical Cyber Asset shall not be managed from a third party's premises. (2)

4.6.4 Physical Access Controls

Physical Access Controls are discussed in Section 5

4.7 Cyber Security — Systems Security Management

This section describes methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (less critical) Cyber Assets within the Electronic Security Perimeter(s).

4.7.1 System Design and Configuration

a) A process to ensure that only those ports and services required for normal and emergency operations are enabled on all Critical Cyber Assets / Cyber Assets within the Electronic Security Perimeter, shall be established, documented and implemented.

b) No protocols using clear text to transmit usernames and passwords shall be used on the network, and no password shall be stored in clear text on any system. (2)

c) No internet / intranet access or corporate email retrieval access shall be possible from any Cyber Asset within the Electronic Security Perimeter. (1)

d) DNS shall not be used for access to Critical Cyber Assets. Nodes can be listed in the hosts file, to eliminate the risk of a DNS malfunction preventing logical access to critical Assets. (3)

e) ICMP (ping) traffic shall not be allowed to leave the Electronic Security Perimeter. (2)

f) DHCP shall not be used for Cyber Assets permanently connected to the network, and the use of DHCP shall be avoided where possible. This is to prevent an asset used on the OT network, being connected to the business LAN, and reconnected to the OT LAN or visa-versa. (1)

g) Where possible, a host firewall shall be configured on all Critical Cyber Assets that only allows access from authorised clients on authorised ports, and denies all other access to the system. (1)

h) Where possible, an application firewall such as AppArmor shall be implemented on Critical Cyber Assets. (3)

i) The default passwords on all equipment shall be changed. (1)

j) Where possible, unused ports on networking equipment shall be administratively shut down. (2)

k) Where HMI Cyber Assets in the security perimeter are not manned 24/7, 802.1x authentication shall be used on switch ports to ensure only authorised users have access to the network. (3)

l) If, during implementation, the system or a subsystem is available with similar features on multiple platforms, preference shall be given to the operating system / software solution with the lowest cyber risk. As an alternative, where feasible, the system should be installed on a secure host in a virtual machine, using Network Address Translation (NAT) to access the system, with only required ports being forwarded to the guest host. Where a network connection for the update of Anti-virus signatures is not available, the use of Microsoft Windows should be avoided. (2)

m) Avoid using environments such as Java, Adobe Flash, Acrobat and Silverlight where possible. (2)

n) Reduce the amount of applications installed on Cyber Assets by only installing required applications. Application white-listing can also be implemented where possible. (2)

o) Reduce the amount of services running on Cyber Assets by removing all services not required for the operation and maintenance of the system. (1)

p) Where possible, the Graphical User Interface (GUI) on a server shall not be started. (1)

q) Technical and procedural controls that enforce access authentication on systems not manned 24/7, and accountability for all user activity shall be documented and implemented. (2)

r) Where mail servers, file server or shared storage device are installed on Cyber Assets, the requirement shall be explicitly defined in the detail design documentation of the Cyber Assets. Compensating controls shall be documented and mail servers, file servers or shared storage devices shall not be used for import of data/information into the Cyber Asset. (3)

s) LANs shall be segregated as much as possible. For example, if a group of Cyber Assets only communicates with another group, a VLAN can be used to remove the group from the default LAN. (2)

t) Where possible, a high security zone shall be established for the most critical cyber assets. (2)

u) Different systems should also be placed in separate firewalled zones where possible. (2)

v) If Management ports on Cyber Assets are used, it shall not be connected to the default LAN, but to its own dedicated LAN or VLAN, with separate dedicated management and configuration workstations. (1)

w) Network routing and management protocols shall be placed in their own VLAN where possible. (2)

x) Session time-outs shall be implemented on all cyber assets. (1)

y) Limits shall be set on the amount of MAC addresses allowed per port on switches to prevent ARP poisoning attacks. (1)

z) The perimeter network security stack shall implement rules on both incoming and outgoing traffic, and an implicit deny rule shall be configured in both directions. Rules shall also be specific with regard to host and host groups as well as ports and port groups. Where possible, the default gateway of the firewall shall not be set, or shall be set to an internal monitoring node, to prevent malware establishing connections to their master stations. The use dynamic NAT shall also be avoided where possible. (1)

aa) No device shall under any circumstances bypass any firewalls by being connected to two different networks simultaneously. (1)

bb) Switches shall be configured to limit the amount of MAC addresses allowed on a port to prevent a ARP poisoning attack. (1)

cc) SSH shall be used to configure routers and switches. (1)

4.7.2 System Maintenance and Operation

a) Regular network scans shall be done on the network to detect unauthorised nodes. (2)

b) If a backup server is implemented on the network, communication with this server shall be encrypted, and the server shall be protected to at least the same level as the most critical backup stored on the server. (1)

c) Log analysis of the log server should be automated as much as possible. (2)

d) Where a cyber asset is configured outside of the secure perimeter for any purpose, and the aim is to reintroduce this cyber asset into the secure perimeter, measures shall be taken to protect this cyber asset from al threats similar to cyber assets inside the secure perimeter. Where adequate protection was not possible, the cyber asset shall be re-installed before reintroduction into the secure perimeter. (2)

4.7.3 Malicious Software Prevention

a) Anti-virus software and other malicious software ("malware") prevention tools shall be implemented, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter. (1)

b) In the case where anti-virus software and malware prevention tools are not installed, compensating measure(s) applied to mitigate risk exposure shall be documented. (1)

c) A process for the updating of anti-virus and malware prevention "signatures" shall be documented. The process must address testing and installing the signatures. (3)

d) Unauthorised software shall not be installed and/or used on Critical Cyber Assets. (1)

e) Removable media (including memory sticks and flash memory devices) that are purchased for business purposes must be safeguarded and protected at all times. (2)

f) Where technically feasible, USB, serial ports, cd/dvd, scsi, and any other medium that can be used for access, for Cyber Assets within the Security Perimeter shall be disabled. (1)

4.7.4 Account Management

a) Users shall not share or divulge their user identification and passwords. (2)

b) A standard to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts shall be documented and implemented. (3)

c) The standard shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service. Accounts of users that are no longer required shall first be disabled for a period before being removed, to be able to associate log entries with the relevant user for investigation purposes. (3)

d) Where possible, remote access using the administrator account shall be disabled. (2)

e) Individual and shared system accounts and authorized access permissions shall be consistent with the concept of "need to know" with respect to work functions performed. (3)

f) All accounts shall have a responsible/accountable person associated with it. (3)

g) User accounts shall be implemented with access rights as approved by designated personnel. (1)

h) Logs of sufficient detail to create historical audit trails of individual user account access activity shall be generated and kept for a minimum of ninety days. (2)

i) User accounts shall be reviewed at least annually to verify access privileges, and no user shall be allowed to work as root / administrator on a continuous basis. (1)

j) Individuals with access to shared accounts shall be identified. Where such accounts must be shared, a standard for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination) shall be documented and implemented. (3)

k) As a minimum, as technically feasible, passwords should adhere to the following:

- Each password shall consist of a minimum of sixteen characters. (1)
- Each password shall consist of a combination of alpha, numeric, and “special” characters. (2)
- Each password shall be changed at least bi-annually, or more frequently based on risk. (2)

l) All Cyber Assets within the Electronic Security Perimeter, as technically feasible, shall implement automated tools or organizational process controls to monitor system events that are related to cyber security. (2)

m) The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents. (2)

n) Organizational processes and technical and procedural mechanisms for monitoring of security events on all Cyber Assets within the Electronic Security Perimeter shall be documented and implemented. (3)

o) Logs of system events related to cyber security shall be kept, where technically feasible, to support incident management as determined in Section 4.8. (2)

p) These logs shall be reviewed for events related to cyber security and retained for ninety calendar days.(2) Formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter shall be established and implemented. (3)

q) All data shall be securely destroyed prior to the disposal or redeployment of such assets to prevent unauthorized retrieval of sensitive cyber security or reliability data. (1)

r) Records shall be kept of such assets that were disposed of or redeployed in accordance with documented procedures (3) The documentation shall be reviewed and updated at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed. (3)

4.7.5 Security Patch Management

a) A security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter shall be established, documented and implemented. (3)

b) Upgrades and patches for Hardware Firmware, Operating Systems or Applications should first be tested on a duplicate of the environment, or on a similar system if a duplicate is not available. This system should be tested to ensure no functionality is lost, and should be run a period to ensure stability of the system is not affected by the released patches. (2)

c) If a separate system is not available, but multiple cyber assets are available that perform the same function, the cyber assets can be divided into groups. Updates can then be applied to one group, and only applied to the other group after confirmation that the updates did not cause a reduction in functionality on the first group. (2)

d) The assessment of security patches and security upgrades for applicability shall be documented within thirty calendar days of availability of the patches or upgrades. Implementation of security patches shall be documented, and in any case where the patch is not installed, compensating measure(s) applied or already in place to mitigate risk exposure shall be documented (3)

e) Where no DMZ is implemented, perimeter firewalls should be opened and then immediately closed, after obtaining the updates, instead of leaving them open. The firewall shall only allow access for a repository server to access the update servers, on the required port. (1)

4.8 Cyber Security – Incident Reporting and Response Planning

The *System Owner* shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents.

4.8.1 Cyber Security Incident Response Plan (3)

a) The Cyber Security Incident response plan shall classify events and document the appropriate response actions, including roles and responsibilities of the response teams, incident handling procedures, and communication plans.

b) Employees shall be made aware of what constitutes an incident, and how to react to incidents.

c) The Cyber Security Incident response plan shall be updated within thirty calendar days of any changes.

d) The Cyber Security Incident response plan shall be reviewed at least annually after a test. The test of the response plan shall be at least annually. A test can range from a paper drill, to a full/training operational exercise, to the response to an actual incident.

e) Cyber Security incidents must be properly investigated by suitably trained and qualified personnel.

f) Where feasible appropriate actions plans shall be developed to permanently mitigate the risk associated with the Cyber Security Incident or control measures shall be documented and communicated to reduce the risk.

g) Where feasible, actions to isolate the affected areas shall be taken after Cyber Security Incidents deemed to be critical to the continuous safe operation of the power system.

4.8.2 Cyber Security Incident Documentation (2)

a) The System Owner must ensure that all reportable Cyber Security Incidents are reported within 60 days. Incidents must be reported to outside authorities through the authorised channels whenever this is required to comply with legal requirements or regulations.

b) The *System Owner* shall keep relevant documentation related to reportable incidents for three calendar years.

5 Recovery Plans for Critical Cyber Assets

5.1 Recovery Plans (2)

The System Owner shall create and annually review recovery plan(s) for Critical Cyber Assets.

a) The recovery plan(s) shall specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

b) The roles and responsibilities of responders shall be documented.

c) The recovery plans shall be reviewed regularly using business impact and risk assessments methodologies.

d) Recovery plans shall be updated with relevant changes, managed through the change control process.

5.1.1 Exercises (3)

a) The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

5.1.2 Recovery Plan Change Control (3)

a) Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident.

b) Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s).

c) Recovery plan(s) shall be updated with relevant changes, managed through the change control process.

5.1.3 Backup and Restore

a) A formal retention procedure to ensure the operational state of the cyber asset shall be developed and maintained by the *System Owner. (3)*

b) The information created and/or stored by a cyber asset must be retained for a minimum period that meets both legal and business requirements where applicable. (3)

c) A backup strategy may include spare electronic components or equipment, written documentation of configuration settings, redundant configurations to be replicated during restoration, tape backup, etc. (2)

5.1.4 Testing Backup Media (3)

a) Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available.

b) Testing can be completed off site.

6 Additional considerations

6.1 Physical Access (1)

Operational and procedural controls shall be documented and implemented to manage physical access at all access points to the Physical Security Perimeter. One or more of the following physical access methods shall be implemented:

a) Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

b) Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

c) Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

d) Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

6.1.1 Monitoring Physical Access (2)

The technical and procedural controls for monitoring physical access at all access points shall be documented and implemented. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified. One or more of the following monitoring methods shall be used:

a) Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

b) Human Observation of Access Points: Monitoring of physical access points by authorized personnel.

6.1.2 Logging Physical Access (2)

Sufficient information to uniquely identify individuals and the time of access shall be logged. The technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter shall be documented and implemented using one or more of the following logging methods or their equivalent:

a) Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

b) Video Recording: Electronic capture of video images of sufficient quality to determine identity.

c) Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

6.1.3 Access Log Retention (2)

Physical Access Logs shall be retained for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Section 4.8.

6.1.4 Maintenance and Testing (2)

The System Owner shall implement a maintenance and testing program to ensure that all physical security systems are tested on a cycle no longer than three years.

All testing and maintenance records shall be kept for a period as determined by Section 4.8. Outage records regarding access controls, logging, and monitoring shall be retained for a minimum of one calendar year.

6.2 Outsourcing

a) Obtaining of an outsourced service has to follow the standard Eskom commercial process. The requirement should include:

- Where possible, outsourcing shall be limited to on-site hardware or software maintenance, installation and configuration, and the accountability shall remain with the System Owner. (2)
- Usernames and passwords that are used by external contractors shall be managed and controlled by Eskom employees. (1)
- Outsourced services shall be from reputable vendors that operate in accordance with Eskom quality standards which should include a suitable Service Level Agreement that meets Eskom security requirements, and a non-disclosure agreement. (1)
- A formal risk assessment shall be performed prior to considering the utilisation of outsourced services (financial & third party assessment). Acceptance of tenders should be subject to both the contracting firm and its personnel being appropriately screened. With vetting criteria being adjusted continuously, even if a particular contractor has obtained clearance previously it will not automatically be renewed. An appropriate and systematic process of security investigation will be exercised on each occasion. (2)
- All security requirements shall be addressed in a contract agreement between the parties.(1)

b) Eskom shall ensure that outsourced service providers comply with all applicable Eskom security policies and procedures, and non-disclosure agreements. (1)

c) Eskom shall ensure that service providers return all Eskom information assets at the external site at the end of the contract, and that all service provider access rights to Eskom information resources, are revoked, (1)

d) No management of the logical and/or physical access control shall be possible from outside the Electronic Security Perimeter of a Critical Cyber Asset. (1)

6.3 NEW Project Implementation

When a new project is planned that would include Critical Cyber Assets, the following criteria shall be met:

The 5 phase Engineering Methodology, or similar methodology, as described shall be followed:

- Phase 1 - Functional Design Specification (FDS)

This phase consists of the production of a Functional Design Specification comprising of a Functional Specification document and a System Design Report. It is the intention of this phase to finalise all requirements and subsequently document the proposed design to form the baseline for the following phases

- Phase 2 - Detailed Design Specification (DDS)

This phase consists of the production of a Detailed Design Specification for both hardware and software components of the system and specifies the procedures for testing.

- Phase 3 - Development, System Integration and Factory Acceptance Test (FAT)

Phase 3 shall commence on completion of Phase 2. This phase consists of the procurement of hardware required for testing, any required development and supply of software, training of the Eskom personnel, database population and system integration if required, which is to be followed by formal testing of the system at the Supplier's premises, in the presence of Eskom personnel.

- Phase 4 - Delivery, Installation, Testing and Commissioning

Phase 4 shall commence on completion of Phase 3. This phase comprises of delivery of hardware, software, documentation and manuals to site, installation in conjunction with Eskom personnel and training. Thereafter, the system shall be commissioned in accordance with operating constraints of the power system.

- Phase 5 - Site Acceptance Test (SAT)

Phase 5 shall commence on completion of Phase 4. This phase consists of conducting tests according to the SAT Procedure document.

a) All Software developments shall follow an approved system development methodology.

b) The integrity of Eskom operational software code shall be safeguarded using a combination of technical access controls and restricted privilege allocation and robust procedures.

c) If any component of the system was connected to an insecure network during any phase of the system development or testing, all nodes shall be re-installed before performing the SAT. This includes cases where the firewall, that connected the system to any less secure network, was not properly configured while parts of the system was being developed or tested.

d) The development of software is only to be considered, if warranted by a strong Business Case and supported both by management and adequate resources over the projected lifetime of the resultant software.

e) If the system or a subsystem is available with similar features on multiple platforms, preference shall be the operating system / software solution with the lowest cyber security risk. As an alternative, where feasible, the system should be installed on a secure host in a virtual machine, using Network Address Translation (NAT) to access the system, with only required ports being forwarded to the guest host.

f) Documentation pertaining to Systems Acquisition, Development and Maintenance and security controls shall be retained, and kept up to date.

g) The production, test and development environment shall be segregated.

h) The acquisition and development procedure of application systems shall take into account the security requirements and controls, which must be tested as part of the system development-testing phase.

i) Post-implementation reviews shall be conducted for new or significantly changed application systems.

j) Formal change control procedures must be utilised for all amendments to systems.

k) All username and passwords shall be changed when the system is put into operation.

l) Any changes to routine systems operations are to be fully tested and approved before being implemented.

m) Necessary upgrades and patches to the systems shall have the associated risks identified and be carefully planned, incorporating tested fall-back procedures.

n) System faults are to be formally recorded and reported to those responsible for software support / maintenance.

o) Data used for testing purposes shall be protected and controlled in accordance with item 2.2 - Information Classification.

p) Newly acquired systems shall be signed off by Eskom Information Security and other relevant governing structures.

q) Procedures to have the ability to reload all OS and software from scratch. This is a vital step after an attack, and should be tested at FAT and SAT.

Annex A – Impact Assessment

(Normative)

Impact assessment form to be completed for all documents.

1 Guidelines

- All comments must be completed.
- Motivate why items are N/A (not applicable)
- Indicate actions to be taken, persons or organisations responsible for actions and deadline for action.
- Change control committees to discuss the impact assessment, and if necessary give feedback to the compiler of any omissions or errors.

2 Critical points

2.1 Importance of this document. E.g. is implementation required due to safety deficiencies, statutory requirements, technology changes, document revisions, improved service quality, improved service performance, optimised costs.

Comment: This document is required, because OT and IT are functionally different, and needs to adhere to different Security Policies. The Policies for OT can be and needs to be made stricter than that of IT. It would also introduce risks in the OT environment if certain IT policies and standards needs to be followed.

2.2 If the document to be released impacts on statutory or legal compliance - this need to be very clearly stated and so highlighted.

Comment: The document does not impact on statutory or legal compliance

2.3 Impact on stock holding and depletion of existing stock prior to switch over.

Comment: Should have minimal impact on stock

2.4 When will new stock be available?

Comment: N/A – The document covers standards, and not specific products

2.5 Has the interchangeability of the product or item been verified - i.e. when it fails is a straight swop possible with a competitor's product?

Comment: N/A – The document covers standards, and not specific products

2.6 Identify and provide details of other critical (items required for the successful implementation of this document) points to be considered in the implementation of this document.

Comment:

2.7 Provide details of any comments made by the Regions regarding the implementation of this document.

Comment: (N/A during commenting phase)

Annex A
(continued)

3 Implementation timeframe

3.1 Time period for implementation of requirements.

Comment: Would depend on the severity of the deviation

3.2 Deadline for changeover to new item and personnel to be informed of DX wide change-over.

Comment:

4 Buyers Guide and Power Office

4.1 Does the Buyers Guide or Buyers List need updating?

Comment: No

4.2 What Buyer's Guides or items have been created?

Comment: N/A – Not specific products

4.3 List all assembly drawing changes that have been revised in conjunction with this document.

Comment: None

4.4 If the implementation of this document requires assessment by CAP, provide details under 5

4.5 Which Power Office packages have been created, modified or removed?

Comment: None

5 CAP / LAP Pre-Qualification Process related impacts

5.1 Is an ad-hoc re-evaluation of all currently accepted suppliers required as a result of implementation of this document?

Comment: No

5.2 If NO, provide motivation for issuing this specification before Acceptance Cycle Expiry date.

Comment: Unrelated

5.3 Are ALL suppliers (currently accepted per LAP), aware of the nature of changes contained in this document?

Comment: No

ESKOM COPYRIGHT PROTECTED

When downloaded from the IARC WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the WEB.

Annex A
(continued)

5.4 Is implementation of the provisions of this document required during the current supplier qualification period?

Comment: No

5.5 If Yes to 5.4, what date has been set for all currently accepted suppliers to comply fully?

Comment:

5.6 If Yes to 5.4, have all currently accepted suppliers been sent a prior formal notification informing them of Eskom's expectations, including the implementation date deadline?

Comment: No

5.7 Can the changes made, potentially impact upon the purchase price of the material/equipment?

Comment: Yes. If systems need added security to meet requirements in the document.

5.8 Material group(s) affected by specification: (Refer to Pre-Qualification invitation schedule for list of material groups)

Comment: N/A

6 Training or communication

6.1 Is training required?

Comment: Yes

6.2 State the level of training required to implement this document. (E.g. awareness training, practical / on job, module, etc.)

Comment: Awareness training

6.3 State designations of personnel that will require training.

Comment: All Engineering personnel in Operating Units and Technology & Support personnel that works on OT equipment

6.4 Is the training material available? Identify person responsible for the development of training material.

Comment: No, it will be developed later.

6.5 If applicable, provide details of training that will take place. (E.G. sponsor, costs, trainer, schedule of training, course material availability, training in erection / use of new equipment, maintenance training, etc).

Comment: Training will differ for different employees. Trainers may be trained for certain areas, and short courses presented in other areas

ESKOM COPYRIGHT PROTECTED

Annex A
(continued)

6.6 Was Technical Training Section consulted w.r.t module development process?

Comment: No

6.7 State communications channels to be used to inform target audience.

Comment: Email, and meetings

7 Special tools, equipment, software

7.1 What special tools, equipment, software, etc will need to be purchased by the Region to effectively implement?

Comment: None

7.2 Are there stock numbers available for the new equipment?

Comment: N/A

7.3 What will be the costs of these special tools, equipment, software? N/A

8 Finances

8.1 What total costs would the Regions be required to incur in implementing this document? Identify all cost activities associated with implementation, e.g. labour, training, tooling, stock, obsolescence

Time for training of employees.

Certain modifications may be needed to existing systems to address the most critical security problems, but these will need fixing in any case.

New systems may require additional equipment i.e. firewalls to meet requirements

Comment:

....

....

....

Impact assessment completed by:

Name: __Johan Botha____

Designation: ___Senior Consultant____

ESKOM COPYRIGHT PROTECTED

When downloaded from the IARC WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the WEB.