Eskom	Standard	

Title: **INFORMATION SECURITY – IT/OT AND THIRD PARTY REMOTE ACCESS STANDARD**

Document Identifier:	**32-373**
Alternative Reference Number:	**Not applicable**
Area of Applicability:	**Eskom Holdings SOC Ltd**
Functional Area:	**Group IT**
Revision:	**5**
Total Pages:	**28**
Next Review Date:	**November 2022**
Disclosure Classification:	**Controlled Disclosure**

Revised by	Functional Responsibility	Supported by
S Amrithlall	Nhlanhla Tshabalala	Richard McCurrach
Senior Advisor ITSO-TSG	Senior Manager ITSO-TSG (Acting)	SCOT PTM&C TC Chair
Date: 21/01/2020	Date: 21/01/2020	Date: 29/1/2020

Functional Responsibility	Supported By SCOT/SC	Authorized by
Lloyd Chego	Adv. Karen Pillay	Nico Harris
Senior Manager Security Solutions (Cyber)	GM Security (Acting)	GM Group Information Technology (Acting)
Date: 24/01/2020	Date: 5/02/2020	Date: 17/02/2020

CONTENTS

1. INTRODUCTION

Providing remote access services to Eskom Holdings SOC Ltd.'s (Eskom) systems users is seen as an essential service to improve operational efficiency. Remote access refers to access to Eskom's systems that originate from outside the perimeter of Eskom's internal network.
The nature of Eskom business requires its employees (permanent and non-permanent) and Third Party contractors to connect remotely to the company from outside of the company's premises.
Remote access can pose a security risk to Eskom's network if it is not adequately managed and co-ordinated. Eskom management has recognised this threat and have therefore requested that this standard be developed.

2. SUPPORTING CLAUSES

2.1 SCOPE

This standard covers all the employees of Eskom and Third Party contractors connecting to Eskom and non-Eskom locations where these premises are under the jurisdiction and/or ownership of Eskom, and any personal computers and/or servers/systems/applications authorised to access Eskom's data networks.

2.1.1 Purpose

This standard covers the remote access to all Eskom networks, servers and computers (stand-alone or network enabled), located at Eskom and non-Eskom locations, where these systems are under the jurisdiction and/or ownership of Eskom, and any computers and/or servers authorized to access Eskom's networks.

This standard focuses on Eskom's standard requirements for remote access.

2.1.2 Applicability

This standard is applicable to Eskom Holdings SOC Ltd, its divisions and owned subsidiaries, including temporary staff, contractors, consultants, third parties and service providers utilising Eskom's information resources.

2.2 NORMATIVE/INFORMATIVE REFERENCES

The following documents contain provisions that, through reference in the text, constitute requirements of this standard. At the time of publication, the edition indicated was valid. All controlled documents are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent edition of the documents listed below. Information on currently valid national and international standards and specifications can be obtained from the Information Centre and Eskom Documentation Centre at Megawatt Park.

2.2.1 Normative

[1] EST 32-351: Information Security – Logical Access Control Standard.
[2] EST 32-375: Information Security - Malicious Code (Anti-Virus) Standard.
[3] EST 32-438: Information Security – System Classification Standard.
[4] EST 32-435: Information Security – End User Usage and Computing Standard.
[5] EST 32-372: Information Security – Physical and Environmental Security Standard.
[6] EPL 32-85: Eskom Information Security Policy.
[7] EPC 32-361: Information Security – Change Control Procedure.
[8] EPC 32-362: Information Security – Incident Management Procedure.
[9] 240-55410927: Cyber Security Standard for Operational Technology.
[10] EST 474-65: Operating Manual of the Steering Committee of Wires Technologies (SCOWT).
[11] 240-55863502: Definition of Operational Technology (OT) and OT/IT Collaboration Accountabilities.
[12] EST 32-644: Eskom documentation management standard.
[13] EST 32-385: Information Security – IT Continuity Standard.
[14] EST 32-368: Information Security - Incident Management Standard.

2.2.2 Informative

[1] ISO 9001 Quality Management Systems.
[2] ISO27001: Code of practice for Information Security Management.
[3] ISO 27033: Information technology — Security techniques — Network security
[4] 240-79669677 Demilitarised zone (DMZ) designs for Operational Technology
[5] 240-xxxx Remote Access Procedure

2.3 ASSUMPTIONS

This document has been created primarily for system administrators and security administrators who are responsible for the technical aspects of securing the network. The material in this document is technically oriented, and it is assumed that readers have at least a basic understanding of system and network security.

2.4 DEFINITIONS

2.4.1 Standards

Standards: Rules which must be followed to enable an effective information security program. Compliance with the standards is mandatory, but deviation is possible if approved by the Information Security Officer or an approved governance committee. Standards define the minimum, baseline procedures, practices, and configurations for systems, applications, controls, networks, and related topics. They are designed to provide a single reference point for use during software development and adoption, installation of systems and tools, and during the contracts process with vendors and service providers.

Shall, Will, Mandatory, Must:

These words indicate that the standard mentioned is a requirement, and must be met.

Should, Recommended, Where Possible:

These words indicate that the standard mentioned is a preferred and accepted control. Deviation may be possible if compensating controls are in place, a risk analysis of the deviation has been done, and management signoff is obtained.

2.4.2 Classification

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

2.4.3 Other

[1] **App:** An application, typically a small, specialized program downloaded onto mobile devices.

[2] **Eskom:** Eskom Holdings Limited, its divisions and owned subsidiaries.

[3] **Eskom Employee:** A permanent or temporary employee of Eskom with a unique number.

[4] **Malware:** A computer program that is secretly placed onto a computer with the intent to compromise the privacy, accuracy, or reliability of the computer's data, applications, or OS. Common types include viruses, worms, malicious mobile code, Trojan horses, rootkits, and spyware.

[5] **Third Party:** an External company/institution/contractor which needs to connect to Eskom's information resources remotely.

[6] **Challenge-Handshake Authentication Protocol (CHAP):** CHAP (Challenge-Handshake Authentication Protocol) is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP). CHAP works as follows:

- After the link is made, the server sends a challenge message to the connection requestor. The requestor responds with a value obtained by using a one-way hash function.

- The server checks the response by comparing its own calculation of the expected hash value.
- If the values match, the authentication is acknowledged; otherwise the connection is usually terminated.
- At any time, the server can request the connected party to send a new challenge message. Because CHAP identifiers are changed frequently and because authentication can be requested by the server at any time, CHAP provides more security than PAP.

[7] **Demilitarized Zone (DMZ):** The DMZ is a physical or logical sub-network that contains and exposes an organisation's external-facing services to a larger untrusted network. The purpose of a DMZ is to add an additional layer of security to an organisation's LAN.

[8] **Internet Engineering Task Force (IETF):** IETF develops and promotes Internet Standards and work closely with W3C and ISO/IEC standards bodies.

[9] **IPsec:** Refers to a protocol for securing Internet Protocol (IP) communications that provides authentication and encryption for each IP Packet of a communication session end-to-end.

[10] **Information Technology:** Information Technology (IT) is a common term used to describe the entire spectrum of technology used for corporate information processing including software, hardware and related services. It involves the electronic representation of business information that is processed by a computer or sent over digital communications (e.g. IP network)

[11] **Operational Technology:** Gartner defines Operational Technology (OT) as "Physical-equipment-oriented technology". In essence OT is the technology that is used to operate, monitor and control the power system. For a formal definition refer to 5.1 in 240-55863502: Definition of Operational Technology (OT) and OT/IT Collaboration Accountabilities.

[12] **Remote Access:** Remote access is the ability for users (including staff, third parties, contractors, consultants and service providers) to access corporate information and systems from a remote location across an external telecommunication service.

[13] **Remote Access connection:** this refers to a connection originating from outside of Eskom/Non Eskom, but Eskom controlled premises to the Eskom controlled network.

[14] **Remote Access Server (RAS):** RAS is a computer in a network that provides access to remote users via the Internet, external telecommunications service or dial-up connections.

2.5 ABBREVIATIONS

Abbreviation	Explanation
BU	Business Unit
CD	Compact Disk
CHAP	Challenge-Handshake Authentication Protocol
DMZ	Demilitarized Zone
EDC	Eskom Documentation Centre
GM	General Manager
HTTPS	Hypertext Transfer Protocol over Secure socket layer, or HTTP over SSL
IAM	Identity and Access Management
ID	Identification
BU	Business Unit
CD	Compact Disk
CHAP	Challenge-Handshake Authentication Protocol
DMZ	Demilitarized Zone
EDC	Eskom Documentation Centre
GM	General Manager
IAM	Identity and Access Management
ID	Identification
IEC	International Electrotechnical Commission
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISO	International Organizational for Standardization
IT	Information Technology
LAN	Local Area Network
OS	Operating System
OT	Operational Technology
PAP	Password Authentication Protocol
PC	Personal Computer
PTM&C	Protection, Telecoms, Metering and Control

Abbreviation	Explanation
RAS	Remote Access Service
SSID	Service Set Identifier
SSL	Secure Socket Layer
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network

3. REMOTE ACCESS ARCHITECTURE

Figure 1: Remote Access Architecture illustrates the Remote Access architecture for both the Information Technology (IT) and Operational Technology (OT) environments. There will be one point of entry for Remote Access:

3.1 CORPORATE RAS

Remote users shall connect via a virtual private network (VPN) into the corporate Remote Access Service (RAS) and upon successful authentication be granted access to the Demilitarized Zone (DMZ) network for which they are duly authorised. This is the typical access path to IT systems such as email servers, web servers, databases, etc. OT remote users who require access to OT networks and who utilise the corporate RAS as their entry point into Eskom's infrastructure shall authenticate against the corporate RAS. Thereafter, the user shall pass through an OT firewall gaining access to the relevant OT DMZ for which the user is authorised.

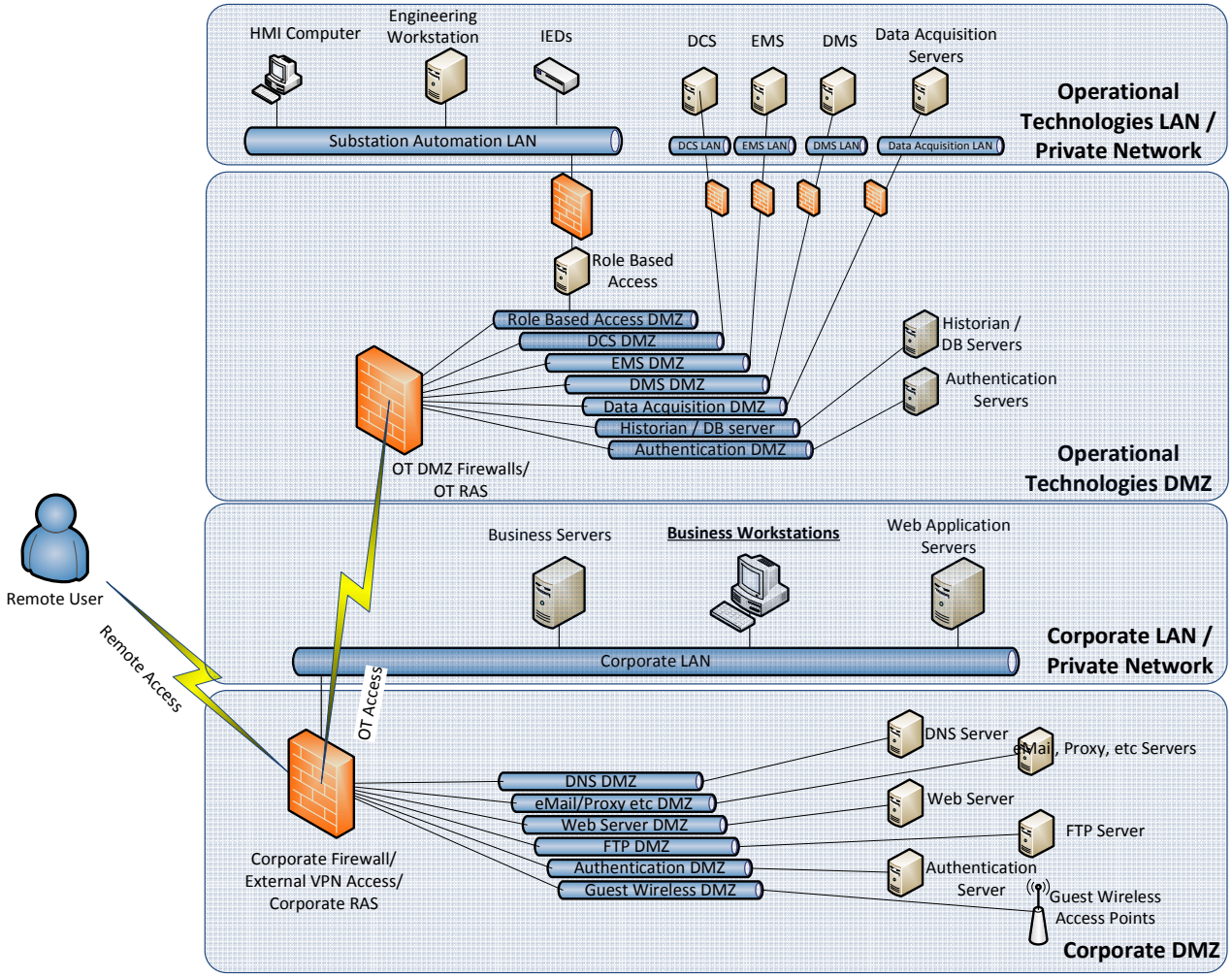

Figure 1: Remote Access Architecture

4. ROLES AND RESPONSIBILITIES

Role	Functional Responsibilities
Eskom Information Security Manager	• Review and update Eskom Information Security Standard in order to meet Eskom identified risks to the organisation. • Communicate to all Stakeholders the content and changes made to Eskom Information Security Standards. • Ensure compliance with this Eskom Information Security Standard and report non-compliance issues to Stakeholders and Eskom Service Providers.
Division Information Manager	• Implement, maintain and update the Division strategy, architecture, standards and procedures for IT and OT Remote Access with input from all Stakeholders. • Evaluate incidents and potential Division risks and introduce counter measures to address these risks. • Responsible for approving, authorising, monitoring and enforcing IT and OT remote access and related security controls within a business unit. • Co-ordinate the implementation of new or additional Division security controls for IT and OT remote access. • Ensure compliance with this standard within the Division and report non-compliance issues to the Division Information Manager and Service Provider.
IT Security Operations and Governance Team	• Implement and maintain the IT portion of the Remote Access Standard for Eskom as indicated in the corporate strategy, architecture, policy, procedures and standards. • Continuously monitor and report to the Information Security Manager and Division Information Security Officers on all incidents. • Provide trend reports on incidents in Eskom and propose solutions to address these possible risks. • Administrate the granting, reviewing and removing of IT and / or OT Remote Access to end users. • Provide event logging reports.

5. IT STANDARD

Employees with remote access privileges to Eskom's corporate network will take responsibility to ensure that their remote access connection is given the same consideration as the users on site connection at Eskom premises.

5.1 REMOTE ACCESS METHODS

There are many options for providing remote access to the company's computing/networking resources. The options used are as follows:

[1] **VPN**: A VPN is a secure tunnel that connects a remote user's computer to the Eskom private network over a public network. One of the follow VPNs shall be used:

- **IPSEC VPN**: Using an IPsec VPN requires IPsec client software to be installed and configured on each telework device.
- **SSL VPN**: similar to IPsec, but it doesn't require a client to be installed.
- **Site-to-Site VPN**:
  A site-to-site VPN allows offices in multiple fixed locations/networks to establish secure connections with each other over a public network such as the Internet. This connection is 'always on', and it's not initiated by the user.
- **A remote-access VPN** allows individual users to establish secure connections with a remote computer network. This type of connection is not always on, and requires a user to initiate the VPN connection on the PC whenever they need to connect to the remote network.
  Both Site-to-Site and Remote access VPNs can use either SSL or IPSEC.

[2] **Remote System Control**: Remote system control allows a teleworker to remotely use a computer at the organization from a remote computer. The remote computer has the software installed that the teleworker needs to run, such as office productivity software (e.g., word processors, spread sheet programs) and organization-specific applications. The remote system control method most commonly used for telework is terminal server access. Terminal server requires the teleworker to either install a client, or a have a web interface with a plug in.

[3] **Individual Application Access**: A remote access user can access an individual application remotely, such as e mail or an App;

[4] **VDI**: Virtual Desktop Infrastructure (VDI) refers to the process of running a user desktop inside a virtual machine that lives on a server in the datacentre with approved access to enterprise applications and data.

[5] In all cases, the communications to the company shall be encrypted, unless accessing information classified as '**Public Domain**'.

[6] No unauthorised remote access applications shall be installed and used. (E.g. TeamViewer, GoToMyPC, etc.)

5.2 REMOTE ACCESS DEVICES

The devices can be divided into 3 categories:

[1] **Personal Computers (PC**), which are desktop and laptop computers running standard PC OSs (like Windows, Linux, and Mac OS).

[2] **Consumer Devices**, which are small, usually mobile computers that do not run standard PC OSs. Examples of consumer devices are smart phones, tablets, etc.

[3] **Servers**: a computer that provides services to other computers on the network.

5.3 USER ADMINISTRATION

[1] Eskom Employees

a. Applications for remote access by employees are done on e-Forms website available on the intranet.
b. The remote access capability of an employee should be terminated / reviewed when the employee's contract/employment with Eskom terminates / changes or the employee does not require the access anymore.
c. Human Resource (HR) shall include the termination of remote access on the termination of service process to ensure that revocation of access to Eskom is enforced.
d. Remote access shall only be granted if it has been authorised by the Information Manager and the user's line manager.
e. Users shall be removed, if one of the following occurs.
   - If the remote access is not needed anymore.
   - Access Expires;
   - On termination of the employment of an employee;
   - If the user has breached the remote access agreement;
f. The remote access solution shall be integrated to an Identity and Access Management (IAM) system where possible so that user may be automatically removed upon leaving Eskom's service.

[2] Third Party Contractors

a. All 3rd party contractors will sign a Non-Disclosure Agreement before access is given.
b. Applications for 3rd party access connection are done using the application form, '**THIRD PARTY REMOTE NETWORK CONNECTION DOCUMENTATION - Form Identifier: 240-51932451'**.
c. The start and termination dates of a 3rd party connection agreement should correspond with the actual contract between Eskom and the 3rd party

contractor/company.

d. Third party connections must comply with requirements as stated in the **'THIRD PARTY REMOTE NETWORK CONNECTION DOCUMENTATION - Form Identifier: 240-51932451'**.
e. All the users who will need access should be stated on the application form, as individual vpn accounts will need to be created for audit and tracking purposes.
f. The process to be followed when giving third parties access to the network is underlined in **'Information Security – Third Party Access Control Procedure: 32-214'**.

[3] All Remote Access connections shall be reviewed to:
a. Determine authorized access.
b. Determine inappropriate access levels.
c. Determine compliance to the standard.

[4] A Remote Access Register shall be established, and record the following
a. Individuals, companies to whom the remote access connections are allocated.
b. Individuals who authorized the remote access connection.
c. Expiry date of the remote access connection.
d. Level of access and description of accessible equipment.
e. An inventory of all the remote access devices and components shall at all times be kept up to date.

5.4 OWNERSHIP

[1] Each remote access connection shall have a business owner. The business owner shall be responsible for risk management of the connection.

[2] The Information Manager shall at all times keep a list of all authorised remote access connections.

5.5 SECURING THE REMOTE ACCESS EQUIPMENT

[1] Any use of techniques or vulnerability assessment and discovery tools such as network scanners and sniffers, or any other tool capable of hacking or have unauthorized penetration is strictly prohibited.

[2] The presence of malicious code (Trojans, viruses, etc.) capable of causing harm to Eskom networks is strictly prohibited.

[3] If one party discovers a virus/worms/malware on its network which has affected, or could affect the other party, then the first party shall immediately inform the other party and give details about the virus/worm/malware.

[4] Eskom Employees

a. The remote access connection should be initiated from a machine/modem managed by Eskom; no personal machines should connect remotely to the Eskom network, unless prior written approval is obtained by the user from the Information Security team. The approval shall be reviewed periodically to ensure its relevancy.

b. All reasonable efforts are made to protect Eskom data, keeping it "in house" on secured servers and devices wherever possible.

[5] Third Party Contractors

a. Third parties shall use their own machines to connect to Eskom, but they will familiarise themselves and comply with Eskom Security Standards.

5.5.1 Software Updates

[1] For Windows machines, Antivirus/antimalware software on the user's machine should be configured properly and pull daily updates, according to *(***Information Security – Malicious Code (Anti-Virus) Standard***).*

[2] Eskom Employees

a. The Windows desktop/laptop, web browsers, and common applications used have all latest security patches as released by Eskom on a regular basis.

[3] Third Party Contractors

a. Network Security Governance team must obtain a security vulnerability scan/report for the systems/applications accessed before they approve a 3rd party network access.
b. Third parties will familiarise themselves and comply with *'***Malicious Code Standard EST 32-351'**.

5.5.2 User Accounts and Sessions

[1] Access is given per user; no user will share login credentials.

[2] All user accounts must be reviewed periodically (at least bi-annually) to ensure that only necessary accounts are enabled.

[3] Users have to re-authenticate after every 12 hours of a session, and 6 hours of idle time.

[4] Remote connection users shall not be connected to any other network when they're connected remotely to Eskom network via VPN. Split tunnel is not allowed.

[5] All users shall use multi-factor authentication to connect to the network.

[6] At no time shall any contractor/employees/Third Party contractor with remote access provide their login credentials to anyone, not even family members.

[7] Generic/shared accounts are prohibited.

5.5.3 Application Configuration

Many attacks, particularly malware, take advantage of features provided by common applications like web browsers, mail clients, etc.

[1] Use a separate brand of web browser for remote work from general browsing.

[2] E mail Clients
Prevent automatic loading of remote e mail images. This helps by limiting a form of spyware known as Web bug. With this setting in place, the user's activity cannot be tracked.

[3] Office Productivity Suites
Limit personal Information: Most office productivity tools allow personal information. This information becomes embedded within the document and can be distributed with the file. Users should limit the information shared on these tools.

5.6 SECURING REMOTE USER EQUIPMENT AND CONSUMER DEVICES

[1] **Limit Access to the Device**:

a. Restrict the access to the device by setting a sort of authentication, such as a PIN, finger print, etc.

b. Configure the devices to auto lock after a certain idle time.

[2] **Disable some networking capabilities except when they're needed**: Keeping network features like Bluetooth off while connected, unless needed. Each enabled network increases the risk of successful attacks on the Eskom network.

[3] Users are responsible for protecting user sessions and machines/devices against Unauthorized Physical Access (**Information Security – Physical and Environmental Security Standard- EST 32-372***).*

5.7 SECURING REMOTE USER CONSUMER DEVICES

[1] **Keep Devices updated**: Keep the device patched to the latest patches, and software updates. Most of these updates don't only update functionality, but address known security loopholes which could be used by malicious attackers.

[2] **Avoid Connecting from untrusted networks:** A lot of free Wi-Fi spot networks exist out there, and some of them are malicious in nature.

[3] **Connecting devices to computers:** Users should make sure the computers they're synchronizing with are properly secured before they connect their devices.

5.8 CONNECTING YOUR DEVICE/EQUIPMENT ON A WIFI NETWORK

There is a proliferation of Wi-Fi networks mushrooming everywhere. Some of these 'free' Wi-Fi networks are malicious in nature, and are setup by attackers who would like to pry. Cyber-attacks occur on corporate networks, they often gain entry through a single employee's computer. So even if your server is locked down pretty well, any employee who travels with a computer or mobile device can be a good source for a security breach.

[1] Users must only connect to trusted networks, stick to SSIDs the user recognize.

[2] User must only connect to Wi-Fi accounts that require authentication. When a user connects to a network, and it doesn't require any authentication, that Wi-Fi network poses a great danger.

[3] Compromised PCs/devices may also be connected on the local network. When connecting, the user should select 'Public Network' Wi-Fi option in Windows. The 'Public Network' option locks down the connection, ensuring Windows is not sharing any files or other sensitive data.

5.9 SECURING ESKOM NETWORK

[1] Remote connection users shall not bypass Eskom computer security measures or gain access to Eskom systems for which proper authorizations have not been given.

[2] Peer-to-Peer software's such as BitTorrent are prohibited and should be blocked, as these carry malware and malicious code.

[3] Block and remove unapproved proxies and encrypted tunnel technologies, such as UltraSurf and Hamachi.

[4] Inspect embedded objects, and treat the object similar to those which are not embedded, i.e., if the file embedded would normally be blocked if transmitted on its own, then block the embedded file.

[5] Only secured file transfer is allowed, FTP shall not be allowed.

[6] Direct file transfer to systems/servers on the network should only be used if no other option is viable. This shall be documented.

[7] Applications must be designed with a tiered approach and separation of security zones must be instituted to minimize the compromise of the database layer of applications.

[8] All servers, systems, applications, databases accessed on the network should all be hardened and have latest patches.

[9] Unless an application and its information has been classified as public, application communication must be encrypted, and require login.

[10] Direct access to a database shall be prohibited. Database support users will need to log in to the server with remote access to manage the database.

[11] With an exception of Eskom Proxy server, no server/computer shall have its network interfaces connected to more than one network security zones on the Eskom network, as this bypasses network security measures.

[12] Eskom Employees
Users shall not be allowed to use 'Site-to-Site' VPN.

[13] Third Party Contractors

a. All services, servers, applications, systems, etc., accessed by 3rd parties must be in segregated secure zones/DMZs, secured by firewalls. If this is not possible due to costs, a risk shall be raised, and the system owners shall accept the risk.

b. Third Party network connections to internal Eskom corporate LAN are prohibited.

[14] Site-to-Site VPN will only be given to the Third Party users if there's a business requirement for a continuous connection without user initiation or Remote Access VPN is simply impractical (e.g., too many centralized users).

[15] Each Third Party user will be allocated a fixed IP address when using Remote Access VPN.

[16] Where technology supports, VPN access should be setup to auto expiry date on the VPN box, which should be one week after the expiry date of the contract with the 3rd Party. If VPN/Firewalls do not support this technology, removing/disabling of users should be done manually.

5.10 CHANGE MANAGEMENT

Changes done through the remote access, or which could affect the remote access, shall follow the Change Control Procedure (Information Security – Change Control Procedure).

5.11 PROCESS FOR MONITORING

The following reports shall be drawn and/or reviewed to assess compliance with this standard:

[1] Annual review of all 3rd Party connection users.

[2] Where possible, relevant assurance and security testing should be conducted (such as penetration testing and audits)

[3] Where relevant, Incident Management Reports.

[4] The remote access service shall log all remote access connections, the following information shall be logged at a minimum.

a. Remote access user ID.

b. Starting and end time of connection.

c. Login attempts by the user.

d. Systems accessed during the connection.

[5] A monthly operational report shall be drafted and will include (but is not limited to) the number of active remote access VPN's, and will provide commentary of the difference.

5.12 SECURITY INCIDENTS

Remote access security incidents shall be determined by the Incident Management Procedure (**Information Security – Incident Management Procedure**).

5.13 SECURITY AWARENESS

Remote access users shall be trained in order to make them more security aware when using the remote access facilities (Information Security – End User Usage and Computing Standard).

6. OT STANDARD

6.1 PROCESS FOR MONITORING

6.1.1 Continuous Reports

The following reports shall be continuously monitored and reviewed to assess compliance with this standard:

[1] Unsuccessful remote connections

Table 1: Unsuccessful Remote Connections Report Definition outlines the definitions of the report.

Report Information	Report Consumer	Report Purpose	Report Outcomes
The report shall contain information of all unsuccessful **remote connection attempts**	Remote Access Administrator	The Remote Access Administrator shall be able to verify the legitimacy of the connection attempts.	The Remote Access Administrator would be able to launch an investigation for illegitimate connection attempts. Authorised users with legitimate connection attempts shall be contacted.

Table 1: Unsuccessful Remote Connections Report Definition

[2] Attempted unauthorised remote access connections

Table 2 : Attempted Unauthorised Remote Access Connections Report Definitions outlines the definitions of the report.

Report Information	Report Consumer	Report Purpose	Report Outcomes
The report shall contain information of all attempted unauthorised remote access connections	Remote Access Administrator	The Remote Access Administrator shall be able to action unauthorised connection attempts.	The Remote Access Administrator would be able to launch an investigation for unauthorised connection attempts.

Table 2 : Attempted Unauthorised Remote Access Connections Report Definitions

[3] Locked user accounts

Table 3: Locked User Accounts Report Definitions outlines the definitions of the report.

Report Information	Report Consumer	Report Purpose	Report Outcomes
The report shall contain information of all users whose accounts were locked out.	Remote Access Administrator	The Remote Access Administrator shall be able to contact locked out users.	The Remote Access Administrator would be able to reset user passwords if required.

Table 3: Locked User Accounts Report Definitions

6.1.2 On Demand Information

[1] On demand the following information shall be made available:

a. An authorisation trail for each new user that is granted remote access.

b. A report of all authorised remote access users.

c. A report showing remote access facilities connected to Eskom OT systems along with telephone extensions and departments that has been authorised to bypass Eskom's remote access infrastructure and business cases for these remote access facilities where applicable.

d. A log available for inspection that shows all successful and unsuccessful remote access connections.

e. A design showing security controls used to protect information travelling across remote access connections.

f. A report of users whose passwords were reset.

Table 4: On Demand Information Definition outlines the definitions of the on demand reports, logs and information.

Report Information	Report Consumer	Report Purpose	Report Outcomes
The report shall contain user authorisation trails, authorised remote access users, remote access facilities, successful and unsuccessful remote access connections, security control designs and reset users passwords.	Remote Access Administrator	The purpose is dependent on the on demand information required.	The outcome is dependent on the on demand information.

Table 4: On Demand Information Definition

6.1.3 Logging Information

[1] Where possible the remote access server shall log all remote access connections.

[2] The following information shall be logged as a minimum:

a. Remote access user ID;
b. Starting time of connection;
c. Ending time of connection;
d. Login attempts by user;
e. Sites accessed during the connection.

6.1.4 Remote Access Register

[1] All remote access connections shall be identified and documented in the remote access register.

[2] The remote access register shall contain the following information:

a. Individual to whom the remote access connection is allocated;
b. Individual who authorised remote access connections;
c. The expiry date of the remote access connection;
d. Intended use of remote access connection;
e. Level of access, and
f. Description of accessible equipment or systems

[3] An inventory of all remote access devices and components shall at all times be kept up to date.

6.2 REQUEST REMOTE ACCESS

[1] An Eskom employee shall gain remote access to an OT network through the IT network utilising the corporate RAS servers as well as an OT DMZ firewalls.

[2] A remote Eskom user connecting through the IT network to an OT network shall complete both the relevant IT authorisation form (Third Party Remote Network Connection Documentation: 240-51932451) as well as the applicable OT authorisation forms.

[3] Third party access into the OT DMZ shall typically receive authorisations from turn-key projects/maintenance agreements or could be done through a standard form.

[4] Third party access into the OT network via the IT corporate RAS shall comply with the 'Information Security – Third Party Access Control Procedure: 32-214'.

[5] Remote access shall only be granted for valid business purposes.

[6] The remote access form shall clearly indicate the start and termination date.

[7] The start and termination dates of a 3rd party connection agreement should correspond with the actual contract between Eskom and the 3rd party contractor/company.

6.3 GRANT REMOTE ACCESS

[1] Remote access shall only be granted if it has been authorised by the accountable manager and the user's line manager.

[2] Remote access shall be granted in line with the DST 240-55410927: Cyber Security Standard for Operational Technology.

[3] Remote access shall only be granted when the user has signed a formal agreement, which:

a. Clearly defines the responsibilities of the remote user

b. Outlines a code of conduct that the remote user must adhere to;

c. Requires the user to comply with all requirements of the DST 240-55410927: Cyber Security Standard for Operational Technology.

d. Emphasises the user's responsibility to protect their username and password. Should anyone else use their credentials, the user and business owner will be held responsible for all activity on that account.

6.4 REVIEW REMOTE ACCESS

[1] Remote access connections shall be reviewed by the Eskom OT accountable manager and relevant remote access administrator:

a. Annually or more frequently depending on the risk.

b. At the expiration date as specified on the request for remote access; and at least it should expire at the end of June each year unless specified on the remote access agreement or relevant 3rd party contract.

c. When the user transfers internally within Eskom.

d. When the role or responsibility of the use changes.

[2] Remote access connections shall be reviewed to:

a. Determine unauthorised access;

b. Determine if it is still applicable;

c. Determine inappropriate access levels;

d. Determine compliance to the standard; and

e. Determine inactive connections.

6.5 REMOVE REMOTE ACCESS

[1] Remote access connections shall be removed:

a. On the expiration date of the remote access;

b. On termination of the employment of an employee;

c. If the user has breached the remote access agreement; and

d. If the remote access is not needed anymore.

[2] Human resources shall supply the remote access administrator with all the names of the persons who have left Eskom's service.

[3] The remote access solution shall be integrated to an Identity and Access Management [IAM] system where possible so that user may be automatically removed upon leaving Eskom's service.

6.6 ADMINISTRATION

[1] Where it is difficult to obtain information or it is suspected that unauthorised connections are in use, one or more of the following actions shall take place:

- Manual audits of the network equipment and documentation shall be done to identify any discrepancies with records of known remote access connections;

- Network management and diagnostic tools shall be used to identify any unauthorised connections; and
- Other forensic methods that are deemed appropriate.

[2] Time and resources shall be allocated to regularly audit the remote access infrastructure.

6.7 OWNERSHIP

[1] Each remote access connection shall have a business owner.

[2] The business owner shall be responsible for risk management of the connection.

[3] The accountable manager shall at all times keep a list of all authorised remote access connections.

6.8 REMOTE ACCESS SOLUTION

[1] It is preferred that IPsec VPN be used to remotely connect to an Eskom OT network.

[2] It is preferred that when accessing the OT network through the IT network, the user shall VPN into the corporate RAS and upon successful authentication, shall initiate a second VPN or encrypted channel from his machine to the relevant OT DMZ. This will reduce the risk of a single point of attack on all OT networks in Eskom.

[3] Only Eskom approved solutions shall be used to remote connect to an OT network.

[4] An approved bootable VPN CD shall preferably be used to remote connect to an OT network.

6.9 REMOTE ACCESS CONNECTIONS

[1] Only Eskom approved equipment and software shall be used to remotely connect to an OT network.

[2] Remote access connections shall only be made to Eskom approved remote access servers.

[3] Users shall not have a remote access connection to an Eskom OT network and another network (e.g. private electronic mail on the Internet) at the same time.

[4] Users shall not make a remote access connection with an unapproved modem within the Eskom OT environment.

[5] Users shall disconnect the remote access connection when it is no longer needed.

[6] Information sent over remote access connections shall be protected and encrypted.

[7] Third parties equipment that is used to perform remote access connections to Eskom's OT network shall have the latest version of patches and anti-virus signatures.

[8] Third parties using their own equipment shall familiarise themselves and comply with the Eskom OT Security Standards.

6.10 SECURING REMOTE ACCESS EQUIPMENT

[1] Equipment shall be handled and protected in line with the manufacturer's instructions, e.g. protection against exposure to strong electromagnetic fields.

[2] Remote access equipment shall not be used by anyone except the user it was assigned to.

[3] Users shall not leave modems connected to PCs in auto-answer mode.

[4] Equipment shall be physically secured in line with the **(Information Security – Physical and Environmental Security Standard- EST 32-372) and 240-55410927: Cyber Security Standard for Operational Technology**.

6.11 DIAL-UP CONTROLS

[1] Users shall not provide IP addresses or dial-up access phone numbers to vendors or any other unauthorised parties.

[2] All dial-up/dial-out access ports shall be strictly controlled, using only designated ports for this purpose.

6.12 MALICIOUS CODE

The malicious software prevention and security patch management shall be implemented in line with **240-55410927: Cyber Security Standard for Operational Technology**.

6.13 SECURITY AWARENESS

Remote access users shall be trained in line with **240-55410927: Cyber Security Standard for Operational Technology.**

6.14 CHANGE MANAGEMENT

[1] All changes that could have an influence on the remote access service shall follow the **Change Control Procedure documented in the 240-55410927: Cyber Standard for Operational Technology**.

[2] All remote access security incidents shall be handled via the **Incident Management Procedure documented in 240-55410927: Cyber Security Standard for Operational Technology**.

7. AUTHORISATION

This document has been seen and accepted by:

Name	Designation
Sham Dhrampal	Corporate Specialist (SSE) - Enterprise Architecture
Prudence Madiba	Senior Manager – Control and Instrumentation
Isabel Fick	Senior Manager – Eskom Telecommunications
Comfort Masike	Senior Manager – System Operator
Sikelela Mkhabela	Senior Manager - Distribution
Mmabatho Motshoane	Middle Manager - Information Security (Acting)
Ezzard De Lange	Middle Manager - Enterprise Architecture
Reshin Moodley	Chief Engineer - Security Solutions (Cyber)
Craig Boesack	Chief Engineer – Control and Instrumentation
Rishi Hariram	Chief Engineer – Control and Automation
Johan Botha	Senior Consultant- System Operator
Matthew Taljaard	Cybersecurity Engineer – Telecommunications Technology and Support

8. REVISIONS

Date	Rev.	Compiler	Remarks
January 2008	0	K.M Sekgaphane	A standard with document number EST 32-373 was developed and published on the Eskom Documentation System.
January 2010	1	M.O.K Motshoane	EST 32-373 was revised and published
Nov 2012	2	N. Rapuleng	EST 32-373 was revised and published to cover both IT and OT
December 2015	4	K. Matau	EST 32-373 and EST 32-376 are combined and reviewed.
Oct 2019	5	Sarish Amrithlall	Reviewed in collaboration with IT, OT, ET

9. DEVELOPMENT TEAM

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

- ITSO TSG – Network Security Team
- Reshin Moodley (Cyber Security).
- OT Cyber Security Care Group.

10. ACKNOWLEDGEMENTS

- Matthew Taljaard