Eskom	**Procedure**	

Title: **IT/OT – Third Party Access Control Procedure**

Document Identifier: **32-214**

Alternative Reference Number:

Area of Applicability: **Eskom Holdings SOC Ltd**

Functional Area: **Group IT**

Revision: **4**

Total Pages: **13**

Next Review Date: **May 2020**

Disclosure Classification: **Controlled Disclosure**

Compiled by	Functional Responsibility	Supported by
Kenneth Matau	Andrea Fortune	Richard McCurrach
Senior Advisor Information Security	Senior Manager ITSO-TSG	SCOT PTM&C TC Chair
Date: 29-05-2017	Date: 25/05/2017	Date: 28/5/2017
Supported by	**Authorized by**	**Authorized by**
Reshin Moodley	Brigadier General (Ret.) Tebogo Rakau	Sean Maritz
Chief Engineer	Divisional Executive Security	Group Executive IT & Chief Information Officer
Cyber Security Solutions		
30/05/2017	Date: 05/06/2017	Date: 29/5/2017

Content

TABLE OF CONTENTS

Page

Figures

1. Introduction

Eskom Information Security Management has recognised a pertinent threat of third parties on the network and has formulated this **'32-214 - Information Security – Third Party Access Control Procedure'** in order to outline the procedure to be followed to apply, obtain approval and implement the business requests in a secure manner.

All third parties accessing Eskom information assets need to be managed in a defined manner to ensure that effective information security controls are maintained by Eskom.

This procedure will support the implementation of **INFORMATION SECURITY – IT and OT THIRD PARTY AND REMOTE ACCESS STANDARD.**

2. Supporting Clauses

2.1 Scope

This procedure covers the data networks, LAN servers, and personal 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 personal computers and/or servers authorized to access Eskom's data networks. The scope of this process also extends to computing equipment within the plant processing systems.

This document focuses on Eskom's corporate process for managing Third Party access to Eskom information resources. Specific processes, procedures and guidelines to facilitate the implementation of this high level framework may be established within groups and business units.

2.1.1 Purpose

The purpose of this document is to establish a series of steps to be followed to apply, obtain approval and opening/removing of third party access while protecting Eskom's information assets and limiting any liabilities.

The procedure ensures effective and efficient management of access to Eskom's information resources including:

- Obtaining authorization.
- Management of access (grant/remove).
- Reviewing access.

a. Management Objectives

- To ensure only legitimate third parties are granted access.
- To ensure access is granted according to the principle of least privilege necessary to perform third parties role.

- To ensure access is removed immediately upon termination or contract expiry.

b. Business Benefits
   - Enable Eskom to reduce unauthorized access.
   - Ensuring there's consistency.
   - Minimizing financial and reputational loss due to unauthorized access.
   - Providing an auditable process that is in generic throughout Eskom.

2.1.2 Applicability

This document shall apply throughout Eskom Holdings SOC Limited, its Divisions and subsidiaries.

2.1.3 Effective date

The Procedure is effective from the date of authorization of the Procedure.

2.2 Normative/Informative References

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

[1] 32-85 - Eskom Information Security Policy.

[2] 32-377 - Information Security Firewall Standard.

[3] 240-56031366 - Information Security Open IP and Open Port Standard.

[4] 240-43333324 - PCM for Manage Information Security (Basic).

[5] 32-373 - Information Security – IT and OT Third Party and Remote Access Standard.

[6] 32-361: Information Security – Change Control Procedure.

[7] 240-55410927 – DST Cyber Security Standard for Operational Technology

[8] 240-55863502 – Definition of Operational Technology (OT) and OT/IT Collaboration Accountabilities

2.2.2 Informative

[1] ISO 27001/2 – Information Security Management System

[2] ISO 9001:2008 Quality Management Systems

2.3 Definitions

2.3.1 Classifications

a. Controlled disclosure: controlled disclosure to external parties.

2.3.2 Third Party:

Third parties are external companies/institutions/contractors which need to connect to Eskom's information resources remotely.

2.3.3 Information owner:

An individual who is responsible for the information asset;

2.3.4 Connection owner:

The connection owner is an Eskom employee who is responsible for the third party connection.

2.4 Abbreviations

Abbreviation	Explanation
AD	Active Directory
CIO	Chief Information Officer
CRMC	Change and Release Management Committee
LAN	Local Area Network
IAM	Identity Access Management
IM	Information Manager
InfoSec	Information Security
IP	Internet Protocol
IRSC	Information Risk and Security Compliance
IS	Information Security
IT	Information Technology (Enterprise Network)
OT	Operational Technology (SCADA Network)
RFS	Request For Service
SLA	Service Level Agreement
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network

2.5 Roles and Responsibilities

Roles	Functional Responsibilities
Connection Owner/System owner	• Takes responsibility for Third Party Application and ownership of access. • Renewal of access. • Shall take note of the duration from submission to implementation of their request. • Shall provide IAM/Network Security Governance teams with the required information as per the application form. • Shall follow this procedure to obtain approval and implementation access. • Shall log a Request for Service (RFS) for access creation. • Shall notify Information Security by sending an e mail to 'InfoSec Firewall Changes' when the access is no longer needed.
IAM	• Quality of information on the application form. • Creation of users on Active Directory (AD). • Communication with the user about the changes on their side.
Network Security Governance team	• Shall review the user request for access against the Information Security risks and ensure alignment to Eskom Information security policies and standards. • Perform quality control checks on the forms submitted. • Keep the user informed on the progress of their request. • Responsible for keeping records of approved forms for audit purposes and future enquiries. • Review of validity of access.
IRSC Change and Release Management Representative	• Review requests for changes or new features. • Facilitate approval for release of changes requested. • Provide feedback on approved/rejected changes.
Network Security Operations team	• Book a change request for the implementation of the user's request. • Implementation of access requested as per information security standards and change request form. • Communication with the user about the changes on their side. • Review of validity of access. • Provide information security trend reports in Eskom and propose solutions to address possible risks.

2.6 Process for Monitoring

The following reports shall be drawn and reviewed to assess compliance with this procedure:

a. A periodical (annual) report on all existing third party rules on the firewall.

b. Proof of approval for each third party connections.

Internal audit will conduct regular audits to ascertain compliance with this procedure.

2.7 Related/Supporting Documents

THIRD PARTY REMOTE NETWORK CONNECTION DOCUMENTATION – 240-51932451;

3. Third Party Access Procedure

Third Party Access Control procedure follows a 5 step lifecycle, *Application*, *Assessment*, *Approval, Implementation*, *Management and Revocation*. This section explains each step, the inputs and outputs, and duration of each step.

The entire process can take from one day (24 hours) to 12 weeks to complete, depending on the type of change, the urgency and user feedback. Information Security – Change Control Procedure documents the types of changes, and timelines for changes.

Change Control Procedure defines ‘Standard’, ‘Urgent’, ‘Emergency’ changes, etc., as a result, the Information Security governance team can fast track the process to cater for all these should there be such a need.

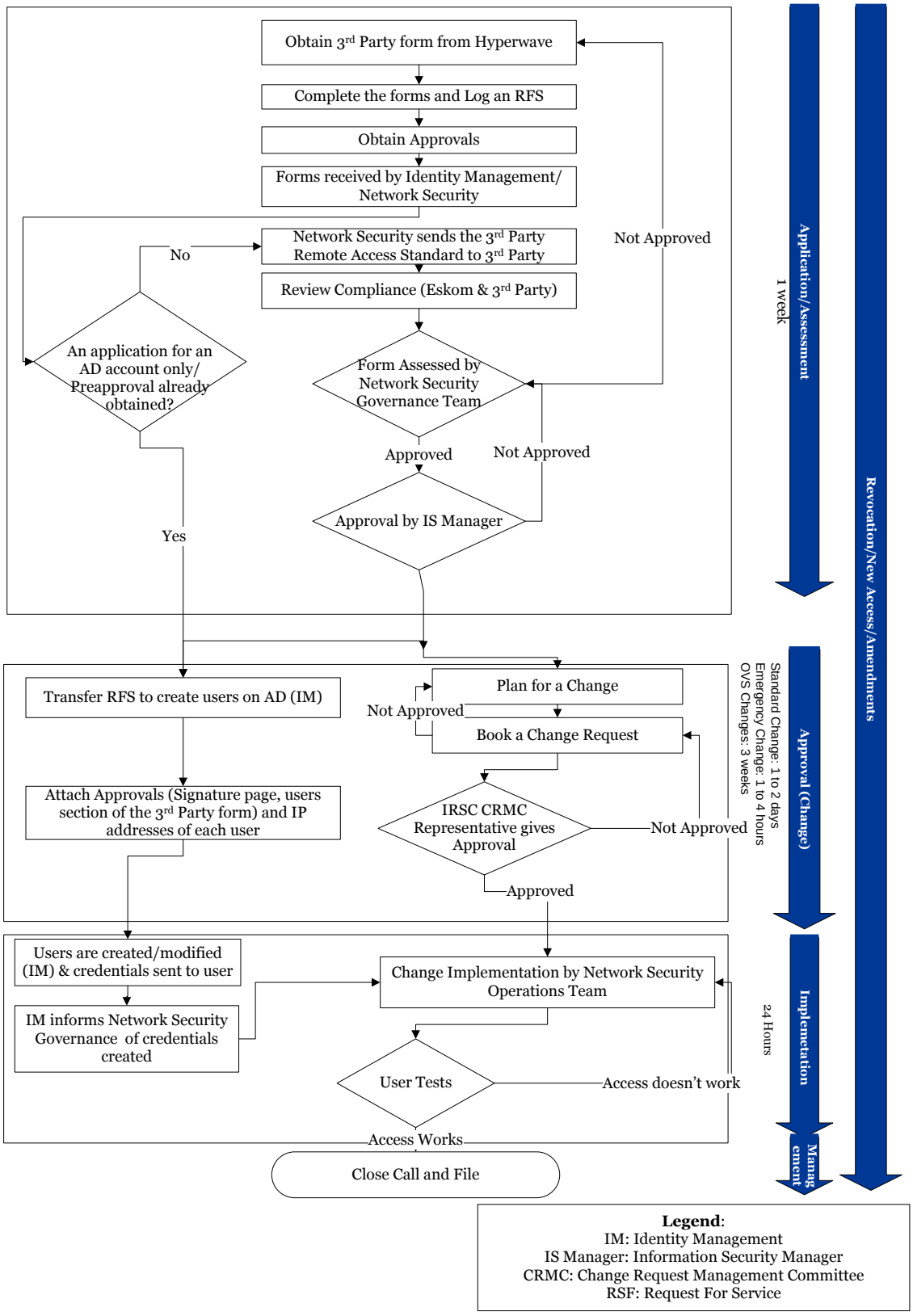

Figure 1: Process & Timelines

3.1 Third Party Access Application

a) The connection owner obtains the Third Party Access form or template from Eskom's Document Management System, 'THIRD PARTY REMOTE NETWORK CONNECTION DOCUMENTATION - Form Identifier: 240-51932451' (Link: http://hyperwave.eskom.co.za/240-51932451).

b) At the time of writing the procedure, there was a process to digitalize the application process, add the form to eForms. Should the process to add/migrate the form in eForms completed, that application form would take precedence and be used instead on the form on Hyperwave link in point 'a)' above.

c) With reference to 'b)', instead of signatures, approvals would instead be done on the eForm.

d) The application form is divided into sections, some users will only require identity store Accounts, and some will update, while others will require everything on the form (VPN access).

e) The form also allows users to quote the old Request for Service (RFS) which was used, to link to the new RFS for updates purpose.

f) The form will also allow users to apply for access without users on the form, and update the form with users later on as requested.

g) This is used to speed up some requests which users might not be known in advance, especially in OT/Generation.

h) In this case, the process will be much shorter than going through everything.

i) The connection owner & the third party members complete the form. The connection owner has to always be a permanent Eskom employee who takes full responsibility of the connection.

j) The connection owner also obtains 'Eskom Information Security Non-Disclosure Agreement – Form Identifier: 240-51932472' (Link: http://hyperwave.eskom.co.za/240-51932472), which is filled by Third Party users. All third party users requesting access, as per in the form, shall each fill in the Non-Disclosure Agreement.

k) A generic Non-Disclosure Agreement (NDA) between Eskom and the Third is also acceptable, i.e., if there's a Non-Disclosure Agreement already signed between Eskom and the Third Party, there's no need to fill in the NDA during this application.

l) The user should log an RFS on the Service Desk system, get an RFS number, and attach the completed forms (Third Party Access form and Non-Disclosure Agreement), along with a single page of the contract between Eskom and the Third Party company, which stipulates the termination date of the contract, to the RFS.

m) The RFS should be allocated to the IAM as per the form on the Service Desk system, either by the applicant, or Service Desk agents.

3.2 Assessment

a) If the users only require identity store credentials without the Remote Access/VPN ability, then the requests is processed by IAM only.

b) IAM then accesses the form from the Service Desk system, and then assesses the quality, and requirements of the application.

c) If Remote Access/VPN is requested, then the RFS is sent to Network Security Governance for assessment.

d) The team then obtains Vulnerability scans report, or something similar from Vulnerabilities Management team or from within, if there's a need.

e) Network Security Governance reviews the form, by assessing business requirements, technical feasibility and security risks.

n) Network Security Governance team makes recommendations and approves/rejects the form and communicates with the connection owner.

o) If the connection introduces/exposes security risks, and it's rejected by the Network Security Governance team, and the applicants cannot implement the recommendations by the team, but the business requirements compel the connection to go ahead, the applicants/connection owners will be given a Risk Letter to acknowledge and accept the risks.

p) Once the Risk letter has been signed by the applicants/connection owners, and CIO (optional), the Network Security Governance then also signs the letter, and proceeds by approving the connection, and attaches the letter to the Request.

q) Eskom (Network Security Governance) will decide the connection technology/type which will be used (Remote Access VPN, Site-to-site, VDI, etc.) for the remote access.

a) If an application had already obtained the preapproval, and there's a rule (which is disabled), the application will not have to go through a full assessment. The application can go straight for implementation, as details would already be known (see Figure 1).

3.3 Approval

a) If the form is approved by Network Security Governance, the next step is for an Information Security Manager approval.

b) The Network Security Governance team then hands over the approved form to the Network Security Operations team for implementation.

3.4 Implementation

a) IT Network Security Operations team plans for the implementation of the change.

b) Simultaneously the Identity and Access Management (IAM) team logs an RFS, or updates and transfers the same RFS logged by the user, for creation of an Identity store account.

c) The Network Security Operations team books a change for the implementation.

d) If only an identity store account was requested without the VPN, Network Security Team will not have to book/implement any changes.

e) Network Security Operations team sends the form to IRSC CRMC representative for a Change approval.

f) Network Security Operations shall implement firewall changes as per Information Security Standards and change request form.

g) Once implemented, Network Security Operations shall communicate with the user to test access as per the form submitted and confirm.

h) If there are issues, Network Security Operations shall engage with the user until the issue is resolved.

i) In cases where, the users/applicants applied for access without users, the Network Security Operations will be required to implement the rules without the user, and add the rule to the firewall, but disable it immediately. The rule added should be commented appropriately.

This is to speed up the process of when the applicants want to add users in the future more quickly than normal process takes.

j) This process is to accommodate OT, as they don't always know their users on time and by the time they know the users, things are already urgent.

k) The rule to grant a user access will only be enabled when the users are known, for the time requested.

l) The support will also be required to be 24 hours. A list of people who can be contacted after hours will be distributed.

3.5 Management

a) Network Security Governance keeps records of approved forms for audit purposes and future enquiries.

b) Third Party access shall be reviewed on an annual basis for applicability.

c) Unused ports shall be disabled.

d) Any changes to Third Party access after the form has been approved shall follow the same process as a new application.

e) Access removal will have to be automated, add dates to access. For long term access, a week should be added to the dates required to help the users sort out the extension of access. For short term access, the access should expire on the date and time requested.

f) The expiry of access should preferably be on both identity store and the firewalls.

3.6 Third Party Access Revocation/Extension

a. IT Network Security Governance shall revoke unused ports by logging a change request.

b. The connection owner shall notify Network Security Governance when access is no longer in use.

c. The access expires on the date agreed upon on the third party access application form. It is the connection owner's responsibility to reapply following the termination of access should this be needed.

d. Expired access shall be removed, either automatically (if the equipment allows) or a change will be logged.

e. Users can request access extension by resending the application form with new/extended dates.

4. Acceptance

This document has been seen and accepted by:

Name	Designation
Nondumiso Zibi	Acting General Manager - Application Management
Dika Modise	Acting Senior Manager – Analytics Centre of Excellence
Sham Dhrampal	Corporate Specialist (SSE) - Enterprise Architecture
Maureen Mokone	Senior Manager – Business Process Management
Nico Harris	Senior Manager – IM Operations
Grasswell Mabudusha	Senior Manager – IM Business Relationship Management
Bhavesh Reddy	Acting Senior Manager - ITSO Business Solutions
Tebogo Makhwelo	Senior Manager – ITSO Shared Services
Andrea Fortune	Senior Manager – ITSO Technical Governance
Shaheen Osman	Senior Manager – Office of the Chief Information Officer
Fanele Mondi	Senior Manager – Portfolio Management
Oliva Muwanga-Zake	Senior Manager - Strategy Execution, Architecture and Risk
Maletsema Phofu	Manager Information Security Manager
Reshin Moodley	OT Cyber Security Care Group Chair
Mmabatho Motshoane	Chief Advisor IM Security
Xolani Lukhele	Senior Advisor IM Security
Mmutle Kgampe	Chief Advisor (Acting) IM Security
Beresford Jelliman	Chief Advisor IM Security
Charles Kungwane	Senior Advisor IM Security
Ronald Netshishivhe	Chief Advisor IM Security
Nyameka Mxosa	Middle Manager Infrastructure
Erika Human	Middle Manager Infrastructure
Sizwe Dlamini	Middle Manager Infrastructure
Mahendra Balipursad	Middle Manager Service Delivery
Goodman Sithole	Manager Contracts Management
Khathu Muvenda	Snr Advisor IM Application

5. Revisions

Date	Rev.	Compiler	Remarks
January 2006	1	Kgomotso Sekgaphane	Developed and published the document
January 2008	2	MOK Motshoane	Review and Update the document
August 2010	3	N Mokumo	Review, update and published the document
May 2017	4	Kenneth Matau	Review, update and publish.

6. Development Team

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

- Nombuso Hlela
- Michelle Govender

7. Acknowledgements

N/A