Eskom	Policy	

Title: **Information Security Policy**

Document Identifier:	**32-85**
Alternative Reference Number:	
Area of Applicability:	**Eskom Holdings SOC Limited**
Functional Area:	**Group IT**
Revision:	**6**
Total Pages:	**32**
Next Review Date:	**November 2024**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Functional Responsibility	Authorised by
M Singo	**S Songo**	**F Burn**
Chief Advisor – IT Security Services	**Senior Manager – IT Security Services**	Chief Information Officer
Date: 10/12/2021	Date: 10-12-2021	Date: 10 December 2021

Contents

1. Introduction

The Information Security Policy is being implemented by Eskom to ensure that its employees utilise Eskom's information resources in a secure, responsible, and lawful manner and with respect for the rights and privacy of others as well as the integrity and security of the information resources.

This policy specifies the necessary requirements to ensure the confidentiality, integrity, and availability of Eskom information resources and aims to provide a comprehensive set of policies and procedures detailing acceptable practices for use of Eskom's information resources. While Eskom permits minimal personal use of its information resources, employees should be aware that such use is subject to the terms and conditions contained in this policy.

Information security is seen as the preservation of the following three characteristics of information:

- **Confidentiality** – that is, ensuring that information is accessible only to those authorised to have access.
- **Integrity** – that is, safeguarding the accuracy and completeness of information and its associated processing methods.
- **Availability** – that is, ensuring that authorised users will have access to information and associated processing systems when required.

2. Policy content

2.1 Policy statement

Information resources are Eskom's critical assets requiring a high level of protection. Sufficient measures commensurate with the risk shall be taken to protect these information resources against accidental or unauthorised modifications, disclosure, and/or destruction as well as to provide assurance regarding the confidentiality, integrity, and availability of Eskom's information resources. This policy has been updated to align it with the Protection of Personal Information Act (POPIA) and the Cybercrimes Act.

2.2 Policy principles or rules

2.2.1 Information security organisation

Group IT management shall ensure that there is clear direction and visible management support for effective implementation of security initiatives across the organisation. Management should actively support security in the organisation through clear direction, demonstrated commitment, and acknowledgment of information security responsibilities.

2.2.1.1. The committee responsible for information security management (including cybersecurity) shall meet to discuss the current status of information security in Eskom, approve and later review information security projects, approve the new or modified Information Security Policy, and perform other necessary high-level information security management activities.

2.2.1.2. Without specific written exceptions, all programs and documentation generated by, or provided by, any employee for the benefit of Eskom are the property of Eskom.

2.2.1.3. All employees shall personally sign an Eskom non-disclosure agreement before work begins.

2.2.1.4. Appropriate contacts with relevant authorities pertaining to Eskom incidents shall be maintained.

2.2.1.5. Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

2.2.1.6. A management authorisation process for new information processing facilities shall be defined and implemented.

2.2.2 Information classification

Information resources shall be classified, documented, and verified to ensure that they receive an appropriate level of protection.

2.2.2.1. All information resources shall be classified according to their level of confidentiality, sensitivity, and criticality.

2.2.2.2. The minimum security control requirements for each classification level shall be identified and implemented.

2.2.2.3. Where there is no indication of an information security classification, the information shall be deemed to be confidential.

2.2.2.4. The information owner shall classify and ensure adequate protection of his/her information.

2.2.2.5. All information resources classified as confidential and sensitive shall be encrypted during transmission and storage.

2.2.2.6. The information owner shall review and maintain all classified information on a regular basis.

2.2.2.7. Details of all critical information resources, as defined by Eskom, shall be documented in a central inventory register.

2.2.2.8. All information resources are to be clearly labelled, so that all users are aware of the classification and ownership.

2.2.2.9. All changes to the classification categories and the classification of information shall be in accordance with document revision control.

2.2.2.10. All critical information resources shall have a nominated owner.

2.2.2.11. All information resources shall have a responsible information owner or custodian.

2.2.2.12. A formal process shall exist to record critical information resources in the inventory and maintain the accuracy of the information resource inventory.

2.2.2.13. All critical information resources shall be sanitised during disposal or replacement.

2.2.3 Outsourcing

Outsourcing arrangements shall include minimum-security requirements based on a risk assessment.

2.2.3.1 Persons responsible for commissioning outsourced computer processing shall ensure that the services used are from reputable companies that operate in accordance with Eskom quality standards, which shall include a suitable service-level agreement that meets Eskom security requirements and a non-disclosure agreement.

2.2.3.2 A formal risk assessment shall be performed prior to considering the utilisation of outsourced services (financial and third-party assessment). Acceptance of tenders shall 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.

2.2.3.3 All security requirements shall be addressed in a contract agreement between the parties.

2.2.3.4 Eskom shall ensure that outsourced service providers comply with all applicable Eskom security policies and procedures and non-disclosure agreements.

2.2.3.5 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.

2.2.4 Personnel security

2.2.4.1 New employees' references shall be verified.

2.2.4.2 Employees' compliance with the Eskom Information Security Policy, Standard, and Procedures shall be monitored.

2.2.4.3 All employees shall sign a formal agreement undertaking to protect the confidentiality of information, both during and after contractual relations with Eskom.

2.2.4.4 Eskom management has the option of revoking the user's access on notification of resignation if the risk is deemed unacceptable.

2.2.4.5 Where Eskom has reasonable grounds to suspect that its security has been/is being compromised and/or the Information Security Policy has been breached, Eskom reserves the right:

2.2.4.5.1 to intercept and peruse any data sent, received, or stored by an employee (including any attachment to it) and to monitor the use of its information resources, including, but not limited to, Internet access, email use, hard drives, network drives, and other computing systems; and

2.2.4.5.2 to conduct inspections of the information resources without advance notice to the employees.

2.2.4.6 Eskom management shall determine the format in which documents and/or communication shall be transmitted electronically and all matters incidental to that. Every employee shall comply with this at all times.

2.2.4.7 Every change in the employment status of Eskom employees, including, but not limited to, permanent employees, consultants, contractors, and temporaries, shall be immediately reported by the individual's immediate manager to the HR Department. The HR Department shall then immediately update the individual's employment status on SAP.

2.2.5 End users and computing

2.2.5.1 End users shall not share or divulge their user identification and passwords.

2.2.5.2 End users shall access Eskom information resources in accordance with item *2.2.7 (Logical access control)*.

2.2.5.3 End users shall not make unauthorised copies of, or modifications to, the contents of any Eskom information resources. Records of copies shall be kept and be registered in the same way as the original document.

2.2.5.4 End users sharing a workstation shall always log out at the end of each session.

2.2.5.5 End users issued with mobile computing shall read information security awareness messages relating to mobile computing and implement the appropriate safeguards to minimise the risks.

2.2.5.6 End users shall familiarise themselves with item *2.2.2 (Information classification)* and ensure that the necessary controls are adhered to when dealing with sensitive information resources.

2.2.5.7 End users shall not forward or disclose and make copies of Eskom's information to parties external to Eskom without the explicit permission of the owner of the information.

2.2.5.8 End users shall transmit, receive, store, or archive electronic communication in accordance with item *2.2.12 (Electronic communication)*.

2.2.5.9 End users shall ensure that Eskom information resources are protected by not exposing them to security vulnerabilities and shall adhere to item *2.2.20 (Malicious code).*

2.2.5.10 End users shall report information security incidents in accordance with item *2.2.19 (Incident management).*

2.2.5.11 End users shall only connect remotely to the Eskom network in accordance with item *2.2.11 (Remote access security).*

2.2.5.12 Unauthorised software shall not be installed and/or used on Eskom equipment.

2.2.5.13 End users shall not disclose or use Eskom information for any purpose that contravenes Eskom, national, or international legislation.

2.2.5.14 End users shall be responsible for ensuring that data on their computers/notebooks and mobile equipment is backed up.

2.2.5.15 End users shall be aware of security requirements when developing spreadsheets, applications, databases, and ad hoc reports for operational purposes.

2.2.5.16 Actions shall be taken against end users who do not comply with any Eskom information security policy or supporting statements in accordance with the Eskom Disciplinary Code, Procedure, and Directives.

2.2.5.17 End users shall attend awareness programmes to familiarise themselves with the information security risks and their responsibilities for the protection of Eskom information resources.

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

2.2.5.19 Only Eskom-supplied information resources shall be used to perform Eskom business, unless an exception has been approved.

2.2.5.20 End users shall not use Eskom equipment and resources for malicious intent. An end user found to have abused Eskom equipment and resources shall be subjected to disciplinary action in accordance with the Eskom Disciplinary Code, Procedure, and Directives.

2.2.5.21 Employees who willingly and deliberately violate this policy will be subject to disciplinary action up to and including termination.

2.2.5.22 Unless an employee has been authorised by the information owner to make public disclosures, all requests for information about Eskom and its business must be referred to the Public Relations Department. Such requests include, but are not limited to, questionnaires, surveys, and newspaper interviews.

2.2.5.23 Unless it has specifically been designated as public, all Eskom internal information must be protected from disclosure to third parties. Third parties may be given access to Eskom internal information only when a demonstrable need to know exists, when a non-disclosure agreement has been signed, and when such a disclosure has been expressly authorised by the relevant Eskom information owner. If sensitive information is lost, is disclosed to unauthorised parties, or is suspected of being lost or disclosed to unauthorised parties, the information owner and the Information Security Department must be notified immediately. Employees who willingly and deliberately disclose or leak Eskom's internal information to third parties will be subject to disciplinary action up to and including termination.

2.2.5.24 End users must not publicly disclose internal Eskom information through the Internet that may adversely affect the business. Such information includes, but is not limited to, business prospects, research and development, human resources, procurement, and internal information systems problems.

2.2.5.25 Reporting and penalties

- Inappropriate use of the information resources is an ever-present threat to the viability of Eskom's networks and relationships with customers, vendors, and the general public. Participation in these activities is deemed an abuse of privilege and is subject to disciplinary action. It is a condition of use of the provided systems that the user actively prevents and reports any occurrence of this type of abuse to his/her head of department.
- Any employee using the Internet and email facilities inappropriately as described above may be subjected to disciplinary action, which, in serious cases, may result in dismissal.

2.2.6 Clear desk policy

2.2.6.1 A clear desk policy shall be followed. Sensitive information and reports in open office environments shall be safeguarded and secured.

2.2.6.2 Sensitive information shall be locked away (for example, portable computing devices such as laptops or PDA devices, CD-ROM, DVD, or USB, etc.).

2.2.6.3 End users shall prevent unauthorised access to their workstations when left unattended by using an appropriate locking mechanism such as password-protected screen savers.

2.2.6.4 The workstation shall always be logged out and/or switched off before being left overnight, unless it is running an overnight process, in which case an appropriate locking mechanism such as a password-protected screen saver shall be activated.

2.2.6.5 Incoming and outgoing mail collection points shall be protected or supervised, so that letters cannot be stolen or lost, and faxes and telexes shall be protected when not in use.

2.2.6.6 Photocopiers shall be switched off and locked outside working hours; this makes it difficult for unauthorised copying of sensitive information to occur.

2.2.6.7 All printers and fax machines shall be cleared of papers as soon as they have been printed; this helps ensure that sensitive documents are not left in printer trays for authorised users.

2.2.6.8 All documents containing sensitive information shall be locked in a secured place (lockable drawer) when not in use.

2.2.7 Logical access control

Logical access to information resources shall be forbidden, unless expressly authorised.

2.2.7.1 Logical access control standards for information resources shall be established and implemented.

2.2.7.2 The business requirements for the authorisation of logical access to information resources shall be defined and documented prior to logical access being granted, where appropriate.

2.2.7.3 Logical access to Eskom's information resources is protected through utilisation of unique user IDs and passwords. All users shall have their identity verified with a user ID and password (or by other means that provide equal or greater security, for example, biometrics or graded authentication) prior to being permitted to use Eskom's information resources.

2.2.7.4 Passwords are highly secret and confidential and shall be handled in the most secure way. Users are responsible for all activities performed on the network under their account. Passwords are set to expire after 30 days and shall be changed by the user. User IDs established for a non-employee/contractor shall have a specified expiration date, unless approved by the security advisor. If an expiration date is not provided, a default of 30 days shall be used.

2.2.7.5 Where supported by technology, the system shall display the last use of the individual's account, so that unauthorised use may be detected.

2.2.7.6 All user ID creation, deletion, and change activity performed by system administrators and others with privileged user IDs shall be secured.

2.2.7.7 Concurrent connections to the network are not permitted/not allowed.

2.2.7.8 All logical access rights shall be reviewed and managed in accordance with a formal procedure that shall be developed and implemented by Information Security and Investigations Department.

2.2.7.9 Critical logical access activities shall be logged to an audit trail and monitored to identify potential misuse of systems or information.

2.2.7.10 Logical access to source code shall be allowed only for authorised personnel.

2.2.7.11 There shall be segregation of duties for all users.

2.2.7.12 The use of operating system utilities or other powerful utilities that may result in failure of logical access controls shall be forbidden, unless authorised.

2.2.7.13 Logical access privileges shall be revoked when no longer required, or when a user's authorisation ceases, or as a result of inactivity by a user.

2.2.8 Third-party access

Third-party access to Eskom information resources shall be controlled.

2.2.8.1 A formal third-party access procedure shall be developed and implemented by Information Security and Investigations Department for authorising all third-party connections to Eskom information resources, and the approval shall comply with Eskom delegation of authority requirements.

2.2.8.2 Security considerations for each type of third-party connection shall be defined in the formal procedure and technical risk analysis performed and submitted for authorisation.

2.2.8.3 All third-party agreements shall be formalised in a contract. If the contract terminates, access by the third party to Eskom's information resources shall be terminated immediately.

2.2.8.4 All third-party connections will be reviewed regularly for applicability.

2.2.8.5 All third-party contractors are to sign a non-disclosure agreement regarding the confidentiality and non-disclosure of Eskom's information to which they may have access. Legal Department should be contacted for the non-disclosure agreement template.

2.2.8.6 Physical access to Eskom information resources by third parties shall be restricted.

2.2.8.7 Third-party users shall be made aware of all relevant Eskom information security policies, standards, and procedures and are required to comply with these.

2.2.8.8 The least-privileges principle shall be applied to any third-party connection.

2.2.8.9 Third-party access shall be granted only when a demonstrable business need exists. An approved non-disclosure agreement shall accompany the application before third-party access can be granted.

2.2.8.10 Third-party contractors shall comply with the Eskom Third-Party Standard, and the third-party connections shall be encrypted.

2.2.9 Network security

Information transported across networks, including wireless, shall be adequately safeguarded and the supporting infrastructure protected.

2.2.9.1 Network operational procedures shall be documented, kept up to date, stored in a secure environment, and be available to authorised personnel.

2.2.9.2 Access to network resources shall be managed in accordance with item *2.2.7 (Logical access control)* and item *2.2.21 (Physical and environmental security)*.

2.2.9.3 Formal change control procedures shall be followed in accordance with item *2.2.17 (Change control)* for any additions and/or changes to the network resources.

2.2.9.4 Network-related security incidents and malfunctions (of any nature) shall be reported, escalated, resolved, monitored, and communicated in accordance with item *2.2.19 (Incident management)*.

2.2.9.5 External facilities shall be managed with the same level of protection as on-site facilities.

2.2.9.6 Current and projected capacity levels of critical network resources shall be identified, monitored, and planned for in accordance with item *2.2.15 (Capacity planning)*.

2.2.9.7 Remote access to Eskom network resources shall only be granted as per an authorised remote access procedure via acceptable and authorised methods.

2.2.9.8 Eskom network resources shall be protected against the introduction of malicious program code.

2.2.9.9 Essential network resources shall be backed up and restored on a regular basis in accordance with item *2.2.13 (IT service continuity management)*.

2.2.9.10 All information travelling across network resources shall be appropriately safeguarded according to item *2.2.2 (Information classification)*.

2.2.9.11 A log of all critical operational network activities shall be maintained; this includes reviewing and reporting, on a regular basis.

2.2.9.12 Formal procedures shall be developed and implemented to approve any services requested through a network security perimeter device.

2.2.9.13 The internal network shall be segregated into zones of trust according to its level of criticality.

2.2.9.14 Security perimeter access points shall be configured by default to prohibit all those not explicitly permitted.

2.2.9.15 Security perimeter access points shall be monitored for policy violations.

2.2.9.16 Network access shall only be provided via facilities that are approved by Eskom.

2.2.10 Connectivity

2.2.10.1 Concurrent connections may not be made. Mobile computing shall be defined for certainty, for example, laptops, etc.

2.2.10.2 Only Eskom-approved methods of connectivity may be adopted and used by employees.

2.2.10.3 Great care shall be taken when connecting to a non-Eskom network using Eskom's information resources, and connectivity shall be appropriately monitored using approved safeguards.

2.2.11 Remote access security

Remote access to Eskom information resources shall be governed by a formal procedure and a standard supporting business needs.

2.2.11.1 Remote access shall only be granted for business purposes.

2.2.11.2 Remote access to Eskom's network and information resources is restricted, and it shall only be granted to users who have been identified and verified and have appropriate information security clearance as may be deemed appropriate by the relevant information manager.

2.2.11.3 Remote access shall only be provided via remote access facilities that are approved by Eskom.

2.2.11.4 Remote access privileges shall be revoked when no longer required or when a user's authorisation ceases.

2.2.11.5 All authorised remote-access users shall be reviewed regularly.

2.2.11.6 A register of all authorised remote-access users shall be maintained.

2.2.11.7 Remote-access users shall apply appropriate levels of security for the protection of equipment, software, and information, as detailed in item *2.2.5 (End users and computing)*.

2.2.11.8 Remote users shall not concurrently connect to the Eskom network and another unauthorised network.

2.2.11.9 All connections between Eskom internal networks and the Internet (or any other publicly accessible computer network) shall include an approved firewall.

2.2.11.10 Remote access shall be governed by a formal procedure.

2.2.12 Electronic communication

The use of electronic communication shall be subject to appropriate security controls.

Furthermore, the electronic communication facilities provided by Eskom shall be appropriately protected against misuse and malicious abuse to ensure their optimum functionality at all times.

2.2.12.1 Non-business use of electronic communication facilities

2.2.12.1.1 All emails and data are the property of Eskom, and Eskom has the right to retrieve, scan, and use all such emails in any investigation or in support of any Eskom investigations.

2.2.12.1.2 The electronic communication facilities exist for business purposes and shall not be used to engage in conduct contrary to Eskom's Conditions of Service Policy. Incidental, occasional non-business use is permissible (as may be mandated by Group IT) as long as:

- it does not consume communication resources in excess of those defined by Group IT;
- it does not interfere with the productivity of the user (both sender and receiver);
- it does not prevent a business activity taking place or delay or take precedence over normal business activities;
- the user does not originate or distribute monopolistic messages, such as chain letters;
- it does not damage Eskom's good name and reputation and does not cause any part of it to be damaged or undermined;

- it is not used to create or transmit any offensive, pornographic, obscene, or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material;
- it is not used to access, create, change, store, download, or transmit material that Eskom may deem to be threatening, defamatory, abusive, indecent, obscene, racist, or otherwise offensive; and
- it does not result in any contravention of this policy or any applicable law.

When Internet or email facilities are used for non-Eskom business, users shall be aware that they are using these facilities at their own risk, and Eskom shall not be held liable or responsible for any damage that may occur as a result of any such use.

2.2.12.2 **Email**

2.2.12.2.1 Email shall be used for business purposes, applying the same terms and levels of content that are consistent with other forms of business communication.

2.2.12.2.2 Minimal personal use is permitted, as long as it does not consume more than a trivial amount of resources, it does not interfere with the user's productivity, and it is not used for charitable or private business activities.

2.2.12.2.3 Users shall not forward or respond to any junk or unsolicited email.

2.2.12.2.4 Users shall be aware of malicious code and viruses when opening email attachments.

2.2.12.2.5 Automatic forwarding of email to external mail accounts is not permitted.

2.2.12.2.6 Users shall be aware that the successful delivery of email messages is not guaranteed.

2.2.12.2.7 Employees shall ensure that information sent by email (especially attachments) is correctly addressed and only being sent to appropriate persons.

2.2.12.2.8 Authorised users are responsible for all email sent from their email account.

2.2.12.2.9 Employees shall bear in mind that, when sending emails, they represent Eskom and shall follow basic courtesies in normal correspondence. Users shall also be cautious when expressing any views, particularly personal views that may be taken as the views of Eskom or may be potentially controversial.

2.2.12.2.10 It is strictly forbidden to intentionally transfer viruses or other destructive programs with the intent of causing damage to the recipient's programs, data, or systems.

2.2.12.2.11 The attachment of data files to an email is only permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code.

2.2.12.2.12 Unsolicited email and computer files received from unknown senders shall be treated with caution and are to be deleted without being opened.

2.2.12.2.13 Should a user receive an email that has been wrongly delivered to his/her email address, he/she should notify the sender of the message. If the message contains confidential information, it shall not be disclosed or used, but rather deleted.

2.2.12.2.14 Care should be taken when opening email attachments. Any person receiving attachments or downloading files received via email should satisfy himself/herself regarding the contents and the sender before unzipping and/or executing any files.

2.2.12.3 Internet

2.2.12.3.1 Each Internet service (that is, FTP, HTTP) shall only be granted with prior written authorisation. Access shall be granted on the least-privileges principle (access granted for services required and not ALL services).

2.2.12.3.2 Sites and material available on the Internet will be filtered, and access to certain sites will be restricted. Users are not permitted to visit sites or download material that contravenes local law or presents documents about race and sexual content, pornography, terrorist activities, and obscene or defamatory content. To the extent that an employee contravenes this section, such employee indemnifies and holds Eskom harmless against any claims (including legal costs) howsoever that are brought against Eskom as a result of an employee's abuse of Eskom's information resources. In addition, Eskom will institute disciplinary actions against such an employee.

2.2.12.3.3 Great care must be taken when downloading information and files from the Internet to safeguard against both malicious code and inappropriate material. Information obtained from Internet sources should be verified before use for business purposes.

2.2.12.3.4 Persons responsible for setting up Internet access are to ensure that Eskom's network is safeguarded against malicious external intrusion by deploying, as a minimum, a configured firewall.

2.2.12.3.5 Access to the Internet must be provided only to those employees who have a legitimate business need for such access.

2.2.12.3.6 In addressing information risks, Eskom may, at its discretion, restrict or block Internet access for any employee.

2.2.12.3.7 Eskom may, at its discretion, restrict or block the downloading of certain file types that are likely to cause network service degradation and/or are deemed not to add value to the business. These file types include, but are not limited to, graphics and music files.

2.2.12.4 Electronic communication operations

2.2.12.4.1 Only Eskom-approved electronic communication facilities and software shall be used.

2.2.12.4.2 All electronic communication shall be scanned for malicious code at the first point of entry to the Eskom network in accordance with item *2.2.20 (Malicious code (antivirus))*.

2.2.12.4.3 Electronic communication facilities shall be configured to protect the availability of systems by limiting the size of messages/user facilities.

2.2.12.4.4 Usage of electronic communication facilities shall be monitored, controlled, and managed.

2.2.12.4.5 Electronic communication incidents shall be monitored, controlled, managed, and escalated in accordance with item *2.2.19 (Incident management)*.

2.2.12.4.6 The Eskom disclaimers (as relevant for the type of communication) shall be included automatically as a suffix to all messages to external addresses.

2.2.12.4.7 Only approved electronic communication service providers shall be used.

2.2.12.4.8 Users shall not use any electronic communication facilities provided by Eskom to create, send, forward, store, or display material that is fraudulent, sexually explicit, obscene,

defamatory, racially or sexually harassing, threatening, unlawful, contrary to the rules of Eskom or the regulations of the appropriate Eskom ethics body, or otherwise illegal.

2.2.12.4.9 All users shall, in all electronic communication, wherever appropriate, expressly indicate whether the communication is made on behalf of another Eskom user or that the communication is not related to Eskom's business.

2.2.12.4.10 Users shall not utilise non-Eskom-approved electronic communication facilities (specifically email and Internet) for Eskom business purposes.

2.2.12.4.11 Data and electronic communication shall be retained in line with legal and business requirements.

2.2.12.4.12 All electronic communication intended for an external recipient shall include the appropriate Eskom disclaimer.

2.2.12.4.13 Users may only publish information to the intranet or any external forum, newsroom, chat room, World Wide Web page, or other public communication mechanism in accordance with Eskom's publishing standards and procedures, as developed and implemented by the relevant information managers. Restricted information may only be published subject to adequate security controls and with the permission and approval of the person responsible for the information.

2.2.12.4.14 Users shall not probe or in any manner assist any other person in probing security mechanisms at either Eskom or other non-Eskom Internet sites, unless authorised.

2.2.12.4.15 Information resources may be ceased by the authorised personnel from users without prior notification for investigation purposes.

2.2.12.5 Monitoring of electronic communication

2.2.12.5.1 Eskom reserves the right to review, audit, intercept, access, monitor, and delete all messages created, received, sent, or stored on electronic communication facilities as part of systems performance monitoring, maintenance, investigating, forensic, auditing, or security activities.

2.2.12.5.2 Any user who unlawfully and intentionally intercepts data, including electromagnetic emissions from a computer system carrying such data within or which is transmitted to or from a computer system, is guilty of an offence.

2.2.12.5.3 Any user who is found in possession of data or the output of data in regard to which there is a reasonable suspicion that such data was intercepted and who is unable to give a satisfactory exculpatory account of such possession is guilty of an offence.

2.2.12.5.4 Where electronic communication is found to be contrary to Eskom's Conditions of Service and the provisions of this policy and warrants disciplinary action, such electronic communication shall only be disclosed for purposes related to the investigation and disciplinary or legal proceedings, of which Eskom shall be obliged to maintain the confidentiality.

2.2.12.5.5 Any user who unlawfully and with the intention to defraud makes a misrepresentation (a) by means of data or a computer program or (b) through any interference with data or a computer program or interference with a computer data storage medium or a computer system, which causes actual or potential prejudice to another person, is guilty of the offence of cyber fraud.

2.2.12.5.6 Any user who unlawfully and with the intention to defraud passes off false data or a false computer program, to the actual or potential prejudice of another person, is guilty of the offence of cyber uttering.

2.2.12.5.7 Any user who unlawfully and intentionally commits or threatens to commit any offence contemplated in the Act for the purpose of (a) obtaining any advantage from another person or (b) compelling another person to perform or to abstain from performing any act is guilty of the offence of cyber extortion.

2.2.12.6 **Waiver of right to privacy**

2.2.12.6.1 While Eskom will allow reasonable non-business use of the electronic communication facilities to users, users are not to have any expectation of privacy in any electronic communication of whatever nature, including any attachment to email, using the electronic communication facilities.

2.2.12.6.2 The electronic communication facilities provided by Eskom are the property of Eskom, and access to these facilities by users is intended for the purpose of facilitating business communication.

2.2.12.6.3 The use of Eskom's electronic communication facilities for non-business purposes amounts to an express authorisation that authorised personnel of Eskom can intercept, monitor, access, and review any communication for systems performance monitoring, maintenance, investigating, forensic, auditing, or security activities, including attachments to email, using either human or automated means, generated, created, sent, received, temporarily stored, archived, or deleted by the user, using Eskom's electronic communication facilities.

2.2.13 IT service continuity management

This policy supports Eskom's Business Continuity Management (BCM) by ensuring that all required IT infrastructure and IT services can be recovered within required and agreed timescales and to acceptable service levels after a decision to invoke recovery procedures has been made by the Crisis Management Team.

2.2.13.1 An IT service continuity management (ITSCM) standard shall be developed for ITSCM to document the standardised methods, processes, and approaches to support Business Continuity Management in a consistent manner.

2.2.13.2 IT service continuity capabilities shall be designed and implemented to meet the business requirements as agreed with Business Continuity. Where the requirements are unknown or have not been specified by the business, the business requirement will default to that of a mission-critical system.

2.2.13.3 IT service continuity plans shall be documented and aligned with the current IT continuity capabilities. Any identified risks will be presented to the business for acceptance or mitigation.

2.2.13.4 In conjunction with Audit, Governance, and Compliance, each IT service continuity plan shall be tested before a system goes live, at least twice a year, or after significant changes, unless BCM has specifically requested differently.

2.2.13.5 A minimum of two instances of recovery testing shall be performed annually. A pre-go-live test is a prerequisite for any new IT service/system.

2.2.13.6 ITSCM shall invoke disaster recovery (DR), following an informed decision to do so by the IT and Business Crisis Management Team and/or the Business Continuity Management Team.

2.2.13.7 Review of the plans shall take place at least once per year, after significant changes, during execution of the testing process, or following an invocation. Results of the review will provide input into a continual service improvement plan.

2.2.13.8 The ITSCM process shall integrate with other IT service management processes and relevant business processes to ensure that the continuity capabilities meet the agreed business requirements at all times.

2.2.13.9 In conjunction with Availability Management, a risk assessment shall be performed on all infrastructure components and recommendations made to reduce the impact and probability of threats that could affect the availability and reliability of identified critical applications.

2.2.13.10 Contracts with vendors that affect IT service continuity shall be monitored and reports produced showing the efficiency and effectiveness of vendor support (with the assistance of Supply Chain Management).

2.2.13.11 Outsourced IT services or systems or components of these are required to abide by this policy and the associated framework; however, if this is not applicable or feasible, then the service provider is required to align itself with British Standard 25777 at a minimum level.

2.2.13.12 At all times, management shall ensure that at least two capable staff members are trained to execute recovery on behalf of the responsible functional area, thereby eliminating single resource dependencies.

2.2.13.13 ITSCM infrastructure and plans shall be controlled configuration items and documents that are subject to both standard change management and document management. The ITSCM process manager shall be advised by the Change Management process of any changes to the live operational environment that potentially have an impact on any continuity plans.

2.2.13.14 For all critical systems, IT continuity capacity and functionality shall be equal to production.

2.2.14 Data retention

2.2.14.1 A formal information retention procedure shall be developed and maintained by each senior manager Information Management.

2.2.14.2 The information created and stored by Eskom's information systems shall be retained for a minimum period that meets both legal and business requirements, as prescribed in the formal procedure.

2.2.14.3 Day-to-day electronic information retention shall ensure that past and current business information is readily available to authorised users and that archives are both created and accessible in case of need.

2.2.15 Capacity planning

Current and projected capacity levels of Eskom critical information resources shall be identified, monitored, and planned for in order to ensure the availability of adequate capacity levels.

2.2.15.1 Formal capacity plans shall be in place.

2.2.15.2 Capacity plans shall be reviewed and updated.

2.2.15.3 All critical information resources requiring capacity planning shall be identified.

2.2.15.4 Critical information resources shall demonstrate a level of resilience that meets or exceeds the technical and business needs and requirements of the organisation.

2.2.15.5 Performance and capacity levels of critical information resources shall be monitored on a continuous basis.

2.2.15.6 Changes to capacity plans shall be reflected in disaster recovery plans.

2.2.16 System acquisition, development, and maintenance

The system acquisition, development, and maintenance procedure shall include appropriate information security processes.

2.2.16.1 All software developments shall always follow an approved system development methodology.

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

2.2.16.3 The development of software is only to be considered if warranted by a strong business case and supported by both management and adequate resources over the projected lifetime of the resultant software.

2.2.16.4 Documentation pertaining to system acquisition, development, and maintenance and security controls shall be retained and kept up to date.

2.2.16.5 The production, test, and development environment shall be segregated.

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

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

2.2.16.8 Formal change control procedures shall be utilised for all amendments to systems.

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

2.2.16.10 Necessary upgrades and patches to the systems shall have the associated risks identified and be carefully planned, incorporating tested fallback procedures.

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

2.2.16.12 Data used for testing purposes shall be protected and controlled in accordance with item *2.2.2 (Information classification).*

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

2.2.17 Change control

Changes to information resources shall be performed according to a formal change control procedure. The control procedure will ensure that proposed changes are reviewed for relevance and impact (business, technical, and financial).

2.2.17.1 The change control procedure and process shall be formally defined, documented, and adhered to.

2.2.17.2 All changes shall be assessed for business, technical, financial, and risk impact.

2.2.17.3 All changes and the results are to be formally planned, authorised, and documented.

2.2.17.4 Changes are to be fully tested in an isolated, controlled, and representative environment and approved before being implemented.

2.2.17.5 Any software change and/or update shall be controlled with version control.

2.2.17.6 All users significantly affected by a change shall be notified of the change.

2.2.17.7 Fallback procedures for aborting and recovering from unsuccessful changes shall be documented and tested.

2.2.17.8 Emergency changes shall be authorised and recorded.

2.2.17.9 Information resources documentation shall be updated on the completion of each change, and old documentation shall be archived or disposed of as per the Documentation and Data Retention Policies.

2.2.17.10 The disposal of software shall only take place when it is formally agreed that the system is no longer required and that its associated data files, which may be archived, will not require restoration at a future point in time.

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

2.2.17.12 Data is to be protected against unauthorised or accidental changes.

2.2.17.13 Disaster recovery plans shall be updated with relevant changes, managed through the change control process.

2.2.18 Cryptography

2.2.18.1 All confidential electronic transactions shall be protected by using digital certificates to ensure non-repudiation.

2.2.18.2 All sensitive information shall be encrypted.

2.2.19 Incident management

Information security incidents and malfunctions (of any nature) shall be reported, escalated, resolved, monitored, and communicated.

2.2.19.1 All types of incidents shall be defined and categorised in terms of their severity.

2.2.19.2 A formal incident management procedure shall be defined, documented, and implemented. This includes the approach to be adopted for investigations.

2.2.19.3 Users shall be made aware of what constitutes an incident and how to react to incidents.

2.2.19.4 Information security incidents shall be reported to outside authorities whenever this is required to comply with legal requirements or regulations. This may only be authorised by the chief information officer (CIO).

2.2.19.5 Information security incidents shall be properly investigated by suitably trained and qualified personnel.

2.2.19.6 Evidence relating to a suspected information security incident with a severity of 2 or lower shall be properly collected, formally recorded, and processed.

2.2.19.7 A database of information security threats and “remedies” shall be created, maintained, and used to reduce risk.

2.2.19.8 During the investigation of critical information security incidents, dual control and the segregation of duties are to be included in procedures to strengthen the integrity of information and data.

2.2.19.9 Information relating to information security incidents may only be released by authorised persons.

2.2.19.10 Unresolved incidents shall be reviewed, escalated, and actioned.

2.2.19.11 Users shall not exploit any identified, unresolved, or reported incidents.

2.2.19.12 Critical incidents affecting Eskom shall receive immediate attention. If required, the necessary actions shall be taken to isolate the affected areas.

2.2.19.13 Incidents of Severity Level 1 shall be presented to the Group IT management meeting for evaluation.

2.2.20 Malicious code

Eskom information resources shall be protected against security risks that may be caused by the introduction of malicious program code.

2.2.20.1 All information resources shall be scanned for malicious code.

2.2.20.2 Only Eskom-approved antivirus software shall be installed and used.

2.2.20.3 Antivirus software shall be active at all times on all PCs, networks, servers, and laptops. Users shall not reconfigure the antivirus software.

2.2.20.4 New software, portable media, and information in electronic format from external sources shall be scanned for malicious program code before introduction into the Eskom network.

2.2.20.5 Malicious code incidents shall be reported and dealt with according to item *2.2.19 (Incident management).*

2.2.20.6 Users shall be made aware of the dangers posed by malicious program code and unauthorised software. Users shall be made aware of the detection and prevention measures and the procedures to be followed in the event of an incident.

2.2.20.7 Uncontaminated original software and operating system disks shall always be available for restoration purposes.

2.2.20.8 Users shall not forward/send email messages regarding virus incident notifications, with the exception of Eskom Information Security and Divisional Information Management.

2.2.20.9 The antivirus signature tables and software engines shall be up to date in terms of the latest releases per the antivirus software house and shall incorporate patch management.

2.2.21 Physical and environmental security

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

2.2.21.1 Computer premises shall be safeguarded against unlawful and unauthorised physical intrusion.

2.2.21.2 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.

2.2.21.3 All computer premises shall be protected against unauthorised access using an appropriate balance between simple ID cards and more complex technologies to identify, authenticate, and monitor all access attempts.

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

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

2.2.21.6 Photographic, video, audio, or other recording equipment shall not be allowed into an area housing critical information resources as categorised.

2.2.21.7 Procedures shall be developed to address secure disposal and sanitisation of information resources.

2.2.21.8 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.

2.2.22 Mobile computing and communication

Appropriate security measures shall be adopted to protect information resources against the risks of using mobile computing and communication facilities.

2.2.22.1 Mobile computing shall not be used for Eskom information, unless it has been configured with necessary controls and approved for such use by Group IT.

2.2.22.2 Employees possessing mobile computing containing confidential Eskom information shall not leave these devices unattended at any time, unless the information contained on them is exclusively stored in encrypted form.

2.2.22.3 When connecting personal devices to Eskom email, a security PIN shall be enforced on the device, and a user will be asked to define a PIN before completing the set-up process. If the PIN is not enabled on the device, Eskom email shall not be installed on the device.

2.2.22.4 Should a user lose the device, Group IT shall remotely wipe data from the device. It is the user's responsibility to report a lost personal device or any other mobile computing.

2.2.22.5 The architecture process shall be followed prior to Eskom applications being installed on mobile computing.

2.2.22.6 All user-owned devices shall not be supported by Eskom support staff and service providers, and they will not be included in the support contract.

2.2.22.7 All data stored on mobile computing equipment such as laptops, removable hard drives, and USBs shall be encrypted.

2.2.23 Logging and monitoring of IT systems

2.2.23.1 A security operation centre to detect, monitor, analyse, and respond to information security incidents shall be established and implemented.

2.2.23.2 Where possible, audit logs shall be enabled on critical IT systems.

2.2.23.3 A logging and monitoring standard and procedure shall be established and implemented.

2.2.23.4 Critical activities in the system shall be logged to an audit trail and monitored to identify potential misuse of systems or information.

2.2.23.5 Audit logs shall be retained to ensure that past and current system logs are readily available to authorised users and that archives are both created and accessible in case of need.

2.2.24 Compliance with legal requirements

2.2.24.1 Relevant statutory, regulatory, and contractual requirements and Eskom's approach to meet applicable legislation shall be explicitly defined, documented, and kept up to date.

2.2.24.2 For all production information system, all relevant statutory, regulatory, and contractual requirements shall be thoroughly researched, explicitly defined, and included in current system documentation.

2.2.24.3 Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

2.2.24.4 The Eskom environment will be regularly reviewed in order to determine whether the security policies and standards are adhered to.

2.2.24.5 Regular supervised vulnerability assessments will be performed for critical systems.

2.2.24.6 Internal Audit will periodically review the adequacy of information system controls and compliance with such controls.

2.2.24.7 Access to audit tools will be strictly controlled and restricted to authorised personnel.

2.2.25 Protection of personal information

2.2.25.1 All personal data shall be processed fairly and lawfully according to the laws and regulations of all jurisdictions where Eskom does business.

2.2.25.2 Personal data shall be collected for purposes communicated to the individual and not further processed in a way incompatible with those purposes.

2.2.25.3 Personal data shall be accurate and complete and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate or incomplete, keeping in mind the purposes for which it was collected or for which it is further processed, is definitively erased or corrected.

2.2.25.4 Personal data must not be kept in a form that permits identification of individuals for any longer than is necessary for the purposes for which the data was collected or for which it is further processed. Responsible parties of personal data are responsible for ensuring that items in the preceding points are complied with.

2.2.25.5 Personal data may be processed only if:

- the individual has given his/her consent unambiguously;
- processing is necessary for the performance of a contract to which the individual is party, such as completing an order for goods;
- processing is required to respond to a request made by the individual;
- processing is necessary for compliance with a legal obligation to which the responsible party is subject;
- processing is necessary in order to protect the vital interests of the individual; or
- processing is necessary to explore or provide new business products or services that may be of use to the responsible party, as long as these new products or services do not override the fundamental rights or freedoms of the individual.

2.2.25.6 Processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, criminal offences, health, or sex life is prohibited, unless:

- the individual has provided explicit consent to such processing;
- processing is necessary for the purposes of carrying out the obligations and specific rights of the responsible party in the field of employment law; or
- processing is necessary to protect the vital interests of the individual or of another person where the individual is physically or legally incapable of giving his/her consent. Operators of personal data are responsible for ensuring that this item and the items in the preceding two points are complied with.

3. Supporting clauses

3.1 Scope

3.1.1 Purpose

The purpose of this Information Security Policy is to specify the measures required to protect Eskom information resources against all types of threats, whether internal or external, deliberate or accidental.

This document focuses on Eskom's Policy for Information Security. Specific standards, procedures, and guidelines to facilitate the implementation of this high-level framework shall be established.

Lack of a security policy to govern system development or maintenance activity could lead to new systems and applications being developed or acquired and eventually put into production without appropriate security controls. This could lead to a breach in confidentiality, reliability, or availability of information or application systems.

The purpose of the policy is to minimise the following risks and exposure:

- Data integrity, availability, and confidentiality being compromised
- Breach of confidentiality
- Breach of legislation or non-compliance with regulatory or ethical standards
- Loss of, or damage to, equipment
- Connection of divisions' systems to uncontrolled environments
- Reputational risk
- Financial loss through loss of confidential Eskom information
- Excessive access levels, unsecured connections, and poorly secured third-party connections
- Security of Eskom systems being compromised
- Serious security weaknesses being introduced
- Human error
- Misuse of information resources
- Information resources availability being compromised
- Prolonged unavailability of critical business services
- Insufficient information to perform resumption of business activities
- Failure of critical information resources and services in the event of a disaster
- Computer performance being disrupted or degraded
- Poor or late delivery of service by outsourced contractors
- Productivity losses being incurred
- Loss of, or damage to, Eskom information resources

3.1.2 Applicability

This policy shall apply throughout Eskom Holdings SOC Limited, its divisions, subsidiaries, and entities in which Eskom has a controlling interest.

The provisions of this policy are applicable to all employees, temporary employees, contractors, subcontractors, vendors, and business partners of Eskom, all users of the information resources, and all service providers to Eskom, regardless of their status (contract, permanent, or otherwise), collectively referred to in this policy as “users or end users”.

If any provision of this policy is rendered invalid under law, such provision shall be deemed modified or omitted to the extent necessary, and the remainder of this policy shall continue in full force and effect.

No purported relaxation or waiver of this policy shall be valid, unless reduced to writing and signed by Eskom’s Executive Committee or its delegates. Unless specifically indicated to the contrary, any such relaxation or waiver shall relate only to the specific request received and employee concerned and shall not be of general application.

3.2 Normative/Informative references

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

3.2.1 Normative

[1] ISO CoBiT DS5 Process

[2] ISO 9001 Quality Management Systems – Requirements

[3] ISO 27001 Information Technology – Security Techniques – Information Security Management Systems – Requirements

[4] ITIL Information Technology Information Library 3.0

[5] British Standard 25777 Information and Communication Technology Continuity Management Code of Practice

[6] Protection of Personal Information Act 4 of 2013

[7] Cybercrimes Act 19 of 2020

3.2.2 Informative

[1] Interception and Monitoring Prohibition Act 127 of 1999

[2] Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

[3] Electronic Communications and Transactions Act 25 of 2002

[4] Minimum Information Security Standards

[5] EST 32-369: Information Security – Physical Asset Classification and Control

[6] EST 32-376: Eskom Third-Party Standard

3.3 Definitions

a. **Availability:** the reliability and accessibility of data and resources to authorised personnel in a timely manner.

b. **Audit trail:** a record or series of records that allows the processing carried out by a computer system to be accurately identified as well as verifying the authenticity of such amendments.

c. **Authorised personnel:** persons who are formally and properly empowered to perform specified duties associated with an office or an agreement or contract or in a system or building.

d. **Business continuity management:** a holistic management process that identifies potential threats to an organisation and the impacts on business operations that those threats, if realised, might cause and that provides a framework for building organisational resilience, with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.

e. **Business impact analysis (BIA):** the process of analysing business functions and the effect that a business disruption might have on them.

f. **Business resumption planning:** planning to ensure the continued availability of critical services, programs, and operations, including all information resources involved. Business resumption planning prepares an organisation for recovery from a contingency, defined as any event that may interrupt an operation or affect service delivery.

g. **Capacity planning:** the determination of the overall size, performance, and resilience of a computer system.

h. **Computer premises:** a building or part of a building, including its grounds, that houses information resources.

i. **Confidentiality:** a security principle that works to ensure that information is not disclosed to unauthorised subjects.

j. **Consent:** any freely-given informed indication of an individual's wishes by which he/she signifies his/her agreement to have his/her personal data processed, which may include disclosure.

k. **Contractor:** the individual or third party to whom responsibility for an activity has been delegated.

l. **Development environment:** a fixed area that is set aside for the development of software to avoid/minimise the possibility of conflict between an existing program and a new version.

m. **Disaster recovery:** recovery of components of IT services and/or systems such as databases, servers, etc.

n. **Emergency response planning:** a plan detailing the emergency actions to be taken after a disaster has occurred.

o. **Environment:** the physical and atmospheric surroundings of information resources.

p. **External networks:** all devices and services connected to one another that can be utilised by the organisation to carry data/traffic over a public carrier to its customers and clients outside the perimeters of the business. Service providers, third-party-access connections, and the Internet should be included in this infrastructure. External networks connect an organisation's computers to other organisations or computers situated outside the business perimeters via a security perimeter.

q. **Facility:** the place where the IT resources are housed.

r. **Inappropriate material:** information that contains, but is not limited to:

a. information or data unrelated to Eskom in all audio and video material and utilised for activities and/or reasons not relating to Eskom;

b. pornographic material in all formats, that is, images, audio, and video material; and

c. information or data that is considered illegal by law and must never be allowed to exist within the Eskom environment through downloading, uploading, dissemination, transmission, and/or sending, which includes, without being limited to, child pornographic images, bestiality, and violence.

s. **Information:** data that has meaning. It is the meaning of this data that has to be protected.

t. **Information classification:** the process of assigning a level of sensitivity and criticality to information as it is being created, amended, enhanced, stored, or transmitted.

u. **Information custodian:** a user or legal entity that is responsible for implementing the necessary safeguards and controls to protect the information resources as per the classification scheme by the information owner.

v. **Information owner:** a user or legal entity that creates or initiates the creation or storage of the information is the initial owner. The owner is responsible for assigning the classification to the information and dictating how the information should be protected.

w. **Information resources:** all data and information as well as the hardware, software, and procedures involved in the storage, processing, and output of such information. This includes data networks, servers, PCs, storage media, printers, photocopiers, fax machines, supporting equipment, fallback equipment, and backup media.

x. **Integrity:** a security mechanism that makes sure that information and systems are not modified maliciously or accidentally.

y. **Internal networks:** a collection of computer devices connected to one another located within the perimeters of the business, so that users can share information, programs, printers, and other computing resources and services. This includes the computers, servers, gateways, and all the components that make up the network within the perimeters of the business infrastructure. Internal networks can be connected to external networks.

z. **IT service continuity plan (ITSCP):** a plan that documents the IT services, the systems, and the components of the systems required to operate a service. The ITSCP also specifies how the recovery documents are organised to effect a recovery of the service or system.

aa. **Logical access:** the connection of one device or system to another through the use of software. The software may, for example, run as a result of a user powering a PC, which then executes the login sequence, or it may be the result of internal processing between systems.

bb. **Malicious code:** any code in any part of a software system or script that is intended to cause undesired effects, security breaches, or damage to a system.

cc. **Malicious program code:** such code includes all programs (including macros and scripts) that are deliberately coded in order to cause an unexpected (and unwanted) event. Malicious code includes viruses, worms, and Trojan horses (apparently useful and innocent programs containing additional hidden code that allows the unauthorised collection, exploitation, falsification, or destruction of data).

dd. **Mobile computing:** movable or transportable equipment, including notebooks, laptops, mobile phones, and PDAs.

ee. **Network resources:** any components or devices, physically or logically connected to another component or device that are used to receive and/or transmit data/traffic between these components or devices. Examples of network resources shall then be classified as user workstations, servers, hubs, routers, physical connection cables, etc.

ff. **Operator:** the Eskom manager, or third-party organisation manager if processing is outsourced, who processes personal data according to the instructions provided by the responsible party.

gg. **Outsourcing:** the transfer of responsibility for an activity to an external organisation or third party.

hh. **Personal data:** any information relating to an individual or existing juristic person. Such data includes name, address, telephone number, social security number, driver's licence number, and personal business transaction details. For example, such a person could be a purchaser of Eskom products.

ii. **Portable media:** portable data storage devices, for example, CDs, tapes, diskettes, and memory cards.

jj. **Processing of personal data or "processing":** any operation or set of operations performed on personal data, whether by automatic or non-automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, combination, blocking, erasure, or destruction.

kk. **Production environment:** the live environment.

ll. **Recovery time objective (RTO):** the target time set for resumption of product, service, or activity delivery after an incident. NOTE: in the context of IT continuity management, RTO is measured from invocation through to service resumption. IT RTO is generally less than the RTO for the resumption of business products, services, or activities.

mm. **Resilience:** the ability of information resources to both withstand a range of load fluctuations and remain stable under continuous load and/or adverse conditions.

nn. **Responsible party:** the Eskom manager or executive who determines the purposes of processing personal data and who makes decisions about the security mechanisms to be used to protect such personal data.

oo. **Security organisation:** the management framework in charge of initiating and controlling the implementation, follow-up, and correct application of the Information Security Policy statements and the security standards and procedures that support them.

pp. **Security perimeter:** a set of security systems, for example, firewalls, to control and restrict both network connectivity and services. Security perimeters establish a perimeter where access controls are enforced. In some instances, systems such as routers may be functioning as though they are perimeters. For the purposes of this policy, routers playing the role of firewalls will also be considered security perimeters and shall be managed according to the rules of this policy. In some instances, this will require that these systems be upgraded, so that they support the minimum functionality defined in this policy.

qq. **Server:** a dual (or better) processor computer that supplies (serves) a network of less powerful machines such as PCs.

rr. **Service-level agreement:** a contract between Eskom and an external party providing a service up to agreed minimum standards.

ss. **Services:** the way information flows through a firewall. Examples of services include File Transfer Protocol (FTP) and web browsing.

tt. **Signature tables:** tables defining virus characteristics. These tables are used by the antivirus software to identify and eradicate malicious program code.

uu. **Source code:** the actual program as written by the programmer, which is compiled into machine code that the computer can understand.

vv. **System:** a combination of computer components working together, that is, an application system or operating system. An application system is an IT implementation of a business system or process.

ww. **Third-party access:** the ability of an external organisation's staff or applications to access Eskom's information and information resources from a remote location, across an external telecommunication service, and while on site.

xx. **Unauthorised software:** software that is not standard to the Eskom environment. There is a classified list of all standard software.

yy. **Users or end users:** employees, temporary employees, contractors, consultants, subcontractors, vendors, and business partners of Eskom. In terms of logical access, users are employees, systems, and interfaces.

zz. **Viruses:** executable programs that have the ability to propagate themselves across a network, causing interruption and/or possible destruction of information resources. Viruses are a category of malicious program code.

aaa. **Workstation:** a type of computer used for desktop publishing, software development, and other types of applications that require a moderate amount of computing power and relatively high-quality graphics capabilities, that is, PCs.

3.4 Abbreviations

Abbreviation	Explanation
CD	Compact disc
CIO	Chief information officer
FTP	File Transfer Protocol
HR	Human resources
HTTP	Hypertext Transfer Protocol
ID	Identification
IT	Information technology
ITSCM	IT service continuity management
PC	Personal computer
PDA	Personal digital assistant
POPIA	Protection of Personal Information Act
RTO	Recovery time objective

3.5 Roles and responsibilities

Role	Responsibilities
Divisional executives	• Ensure that the necessary information security controls are implemented and complied with as per this policy.
Eskom Information Security manager	• Establish and revise the corporate Information Security Strategy, Policy, and Standards for personnel security, with input from divisions and subsidiaries. • Co-ordinate the overall communication and awareness strategy for personnel security. • Establish and co-ordinate appropriate working group forums to facilitate organisation-wide representation and feedback of personnel security. • Co-ordinate the implementation of new or additional security controls for personnel security.
Senior manager Information Management	• Ensure that all computer users are aware of the applicable policies, standards, procedures, and guidelines for personnel security. • Review the effectiveness of Eskom's personnel security strategy and implemented security controls. • Ensure compliance with this policy within the group, and report deviations to the Information Security manager.
Computer user	• Comply with all information security policies, standards, and procedures for personnel security. • Be aware of all updates made to information security policies, standards, and procedures for personnel security.
Corporate Legal Department	• Investigate special incidents that involve misconduct and ethical and any other form of incident as and when requested by the Information Security manager.
Human resources management	• Persons responsible for human resources management are to ensure that all employees are fully aware of the existence and contents of this policy and their legal responsibilities with respect to their use of the information resources. Such responsibilities are to be included in the employee documentation such as the Terms and Conditions of Employment.

3.6 Process for monitoring

- Development of supporting procedures and standards
- Regular reviews of policies, procedures, and standards, with divisional inputs
- Regular internal audits to ensure compliance with the policy
- Annual user surveys to verify that the policies, procedures, and standards are both applied and understood

4. Acceptance

This document has been seen and accepted by:

Name	Designation
Faith Burn	Chief Information Officer
Mmabatho Singo	Senior Manager – IT Security Services (Acting)
Tebogo Makhwelo	Senior Manager – Infrastructure Operations
Ian Marks	Senior Manager – Specialised Technical Services (Acting)
Anthenia Phuku	Senior Manager – IM Business Solutions and Development Services
Varsha Pillay	Senior Manager – Applications Operations
Leocardia Kamanga	Senior Manager – IT Governance Services
Grasswell Mabudusha	Senior Manager – Strategic Project Services

5. Revisions

Date	Rev.	Remarks
December 2005	0	The content of ESKPBAAX1 was revised in alignment with the new Eskom document criteria, with the following changes: a new unique number, 32-85, was allocated, and the policy was formatted accordingly.
July 2008	1	The content of EPL 32-85 was revised in alignment with South African statutory requirements.
August 2010	2	The content of the policy EPL 32-85 was reviewed and updated.
June 2013	3	The content of the policy EPL 32-85 was reviewed and updated.
February 2014	4	The content of the policy EPL 32-85 was reviewed and updated.
November 2017	5	Date changes and signatories' changes.
November 2021	6	The policy EPL 32-85 was reviewed and updated. Clause 2.2.23 and 2.2.25 were added.

6. Development team

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

- Mmabatho Singo Chief Advisor Information Security
- Ronald Netshishivhe Chief Advisor Information Security
- Mabongi Ngidi Senior Advisor Information Security
- Neo Lemao Senior Advisor Information Security
- Mmutle Kgampe Senior Advisor Information Security

7. Acknowledgements

- Eskom Legal and Compliance Department