Sanlam Kenya PLC Policies and Procedure Guidelines v1.2

Index

User Policies

Sanlam Kenya Logical Access Policy

Document Type	User Policy
Owner	Head Of Innovation and Technology

Sanlam Kenya

PURPOSE:

To ensure that logical access controls are implemented appropriately to protect information technology resources in accordance with business' security requirements.

This policy is aligned to ISO 27001/27002 and COBIT 5 frameworks (DSS7.04)

RISKS:

Poorly managed access to systems and information assets could lead to users having anonymity or excessive system privileges which could be abused to cause financial and/or reputational damage.

POLICY STATEMENT:

Access control

- A formal approval process must be followed to grant standard and privileged user access to any system.
- Access must be granted on a "least privilege" basis according to individual user's role or profile requirements.
- A review of standard and privileged users' access rights must be conducted periodically by the system owner or the relevant business unit head.
- All activity initiated by system and application users, must be traceable to specific individuals using system logs and unique User Identifiers (User IDs).
- Both System(Service) and User account access must be managed according to the same principles.

User identity and password management

- User ID, password and access changes may only be communicated after positive identification of the user's identity is established, to ensure accountability.
- Interactive user sessions must be rendered inactive or suspended after 5 minutes of inactivity.
- Defined procedures and access control mechanisms (preferably automated) should be in place to ensure the timeous deactivation of terminated user accounts.

Remote access and connections

- User remote access must be approved and managed through a formal process.
- Remote Access privileges must be revoked as soon as the need for remote access has lapsed or user access has been terminated.
- Equipment used for remote access purposes must be compliant with the appropriate regulations for the country in which it will be used.
- A register of authorised remote access users and access levels must be maintained and reviewed regularly by Information Security Officer .

Elevated privilege access

- Privileged access may only be granted to accounts through a formal process, using a clear chain of authority and delegation.
- Authorised administrators are required to log in with their own user IDs first before switching to a generic administrator or root account for the performing of specific tasks.
- All tasks performed by administrators are required to be traceable to specific individuals via the use of comprehensive logs and unique User IDs. These logs must be reviewed on a regular basis and should be stored in such a way that the administrators cannot edit or change the logs of their activity.

Third party access

- Every third party, that has access to Sanlam Kenya resources must be contracted to secure their own connected systems in a manner consistent with Sanlam Kenya requirements.
- A register of authorised third party users, as well as the access levels provided, must be reviewed Every Quarter. . Access should be terminated if access in not required.
- Access by third parties to perform remote application support should be restricted, only to the systems that they support and only for limited times required to perform support actions.

Segregation of duties

- System Owners and administrators must define and implement user roles in such a way that appropriate segregation of duties is achieved, so that one person cannot abuse the system without collusion. Any system rights request must be reviewed and approved by the line manager.

Emergency access

- A formal process for granting emergency access must be followed; and this access must be revoked subsequent to the event. Activity performed during an emergency event must be traceable to a unique identity.
- Reports related to emergency access must be reviewed frequently.

APPLICABILITY:

This policy applies to all individuals who use, manage, provide and administer information and technology resources and services under the custodianship of Sanlam Kenya or those sourced via third party Service Providers which includes Sanlam Kenya employees, third parties, temporary staff, contractors, external service providers and consultants.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures.

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Sanlam Kenya Email Usage Policy

Document Type	User Policy
Owner	Head Of Innovation and Technology

Sanlam Kenya

PURPOSE:

To ensure that information transmitted via email and other electronic communications is appropriately protected and employees use these communication platforms in a responsible way.

This policy is aligned to ISO 27001/27002 and COBIT 5 frameworks (DSS7.02).

RISKS:

E-mail and other electronic communication platforms are not secure by design. The content transmitted could be sensitive in nature and un-authorised access or negligence in using the system could lead to legal issues, reputational or financial damage.

POLICY STATEMENT:

User Responsibility

- Email and other electronic communication facilities provided by Sanlam Kenya are business tools and information transmitted via these facilities will be considered business information, owned by Sanlam Kenya ,.
- Users of these communication facilities should limit all personal use to that which is coincidental. Even when using these facilities for personal purposes, the content transmitted must always be professional, lawful and in good taste.
- Employees are prohibited from creating, storing, downloading, forwarding or printing any form of communication that contravenes this policy, except where requested by or with approval from Management as evidence in a disciplinary or legal hearing.
- Employees will be accountable for all content transmitted under their user ID's.
- Sanlam Kenya respects employee privacy, but reserves it's right to access private and business electronic communication records given reasonable justification.
- Sanlam Kenya regards information relating to our customers, our business operations, our employees and our business partners as confidential property of Sanlam Kenya requiring formal management approval prior to distribution. This includes disbursement to other e-mail or cloud communication facilities used by the employee in his or her personal capacity (like personal webmail accounts)
- Employees may not take any part in the creation, download or forwarding of malicious or damaging code or content. This would include, but is not restricted to: viruses, worms, phishing, hoaxes, chain letters and abusive, in-appropriate or insulting content.
- Employees must familiarize themselves with security awareness content and report suspicious emails (including phishing and social engineering) to infosec@sanlam.co.ke.
- Email should never be considered a secure communication vehicle. If sensitive information has to be transmitted via e-mail or other electronic communications platforms, additional measures (like encryption) should be deployed to reduce the risk of information compromise. The additional measures used must either be according to a documented company standard or approved by the Information Security Officer
- Access to non-Corporate email will not be allowed within Sanlam Kenya network. Any exception will only be authorized through risk department.
- Employees are not allowed to communicate on behalf of Sanlam Kenya unless duly authorized to do so. In addition, Sanlam Kenya takes no responsibility for anything that the user does that is not in line with the Sanlam Kenya policies.

System Owner Responsibility

- System Owners for the email, and electronic communication systems must manage the storage of electronic communication in compliance with regulatory, legal and policy requirements.
- System Owners of the email, and electronic communications, systems must ensure that the appropriate company headers and disclaimers to electronic communication are attached to all outgoing email.
- The content of all incoming email must be filtered for malicious and unacceptable content, including but not limited to malware, spam and phishing

APPLICABILITY:

This policy applies to all individuals who use, manage, provide and administer information and technology resources and services under the custodianship of Sanlam Kenya or those sourced via third party Service Providers which includes Sanlam Kenya employees, third parties, temporary staff, contractors, external service providers and consultants.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures.

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Sanlam Kenya Use of Computing Assets

Document Type	User Policy
Owner	Head Of Innovation and Technology

Sanlam Kenya

PURPOSE:

To ensure that all assets, used to process Sanlam Kenya information are effectively and efficiently controlled, utilised, safeguarded, and managed.

This policy is aligned to ISO 27001/27002 and COBIT 5 frameworks (DSS7.03).

RISKS:

Poorly configured and managed computing assets could be a vehicle through which unauthorised access to systems and information assets could be obtained.

POLICY STATEMENT:

User Responsibility

- All devices (including privately owned devices) used for Sanlam Kenya business purposes, must
  - be registered with Sanlam Kenya technical support department,
  - have the password lock activated,
  - be configured in such a way that sensitive information stored on it is encrypted
  - Where possible the ability to 'remote wipe' Sanlam Kenya information from the device must be enabled.
- If Sanlam Kenya's IT division is unable to configure the necessary security and management software on the device, then an employee will not be allowed to use the device for business purposes.
- Sanlam Kenya has the right to scan the information on devices provided by Sanlam Kenya.
- Users must not jailbreak or root devices, or install illegal or pirated software on devices.

New Devices

- Before purchasing a device, employees must talk to their IT division to find out whether the device is supported or not.
- When migrating to a new device, employees must ensure that all relevant personal data on their old device is backed-up externally and Sanlam Kenya data on the previous device is deleted.

Information Security Controls

- When leaving Sanlam Kenya users must delete all Sanlam Kenya information on their personal device(s).
- Users must not remove, disable or bypass any security settings or software enabled on their devices.
- Users must enable the security, such as passcode lock protection, when they are not working on the device.
- Users must refrain from relying on "Password Vaults" to store device and application passwords; unless the vault has been approved and provided by Sanlam Kenya.
- Users will not be allowed to access portable USB devices. Any exception must be authorized by risk department.

Data Backup

- Data and Applications on the device as well as configuration settings will not be backed up by Sanlam Kenya .
- Users must backup any personal data, with the guidance of their IT Department, using a secure mechanism. Business data must be stored on network platforms provided by Sanlam Kenya.

Safe use of "apps"

- Only download "apps" that are provided by trusted sources.
- Regularly check for and apply security upgrades and patches.
- Don't override the base security of devices (e.g. "jailbreak" Apple devices, gain root access to Android devices, etc.).
- Don't break the security of "apps" and/or install pirate copies.
- Employees must familiarize themselves with how the "app" shares information to other services.
- Employees must understand how the "app" operates to enable them to stop its operation on a lost or stolen device.

Physical Security and Lost or Stolen Devices

- Employees are responsible for the physical security and safekeeping of devices (and the Sanlam Kenya information stored on them) whilst in their possession.
- Should the employees devices used to access Sanlam Kenya information and services be lost or stolen, employees must report the loss or theft of the device immediately and wipe the data on the device. They may be required to report the incident to the local police station.
- Employees must know what number to call if their devices are lost or stolen.
- Employees must change their e-mail passwords as soon as possible if stolen device used to access e-mail.
- A device must never be left unattended in a vehicle or public space unless it is out of sight and securely locked away.

APPLICABILITY:

This policy applies to all individuals that manage, provide and administer information technology resources and services under the custodianship of Sanlam Kenya or those sourced via third party Service Providers which includes Sanlam Kenya employees, third parties, temporary staff, contractors, external service providers and consultants.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures.

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Sanlam Kenya Internet Usage Policy

Document Type	User Policy
Owner	Head Of Innovation and technology

Sanlam Kenya

PURPOSE:

To ensure the appropriate and responsible use of corporate internet access by users.

This policy is aligned to ISO 27001/27002 and COBIT 5 frameworks (DSS7).

RISKS:

In-appropriate use of internet resources could have a negative impact on infrastructure capacity and availability. It could also expose internal resources when re-used credentials get compromised on external web platforms; and illegal activity by employees could expose Sanlam Kenya to legal and reputational risk

POLICY STATEMENT:

User Responsibility

- Internet access will be provided to users to support business activities, as needed to perform their jobs.
- Users must make reasonable efforts in conserving bandwidth when using the internet.
- Sanlam Kenya requires employees to use the privilege of internet access, allocated to them, sensibly, professionally, lawfully, consistent with their duties, with respect for their colleagues or any other party, with respect for Sanlam Kenya good name and in accordance with this policy.
- Employees may not establish a direct connection to the Internet from a device connected to the internal (or "trusted") network, unless through an authorised virtual private network (VPN) and personal firewall; as approved by the Information Security Officer .
- Employees may not establish any type of connection that bypasses firewall, proxy and web content filtering infrastructure provided by Sanlam Kenya unless approved by the Information Security Officer .
- Employees may not use Sanlam Kenya 's systems or network in any way that may damage, overload or negatively affect the performance of the system or the internal or external network.
- Employees may not create the impression that they are dealing on behalf of Sanlam Kenya when acquiring goods online or when using social media and other online platforms in their private capacity.
- Employees may not transfer personal information outside the borders of Kenya unless it is duly authorised by management and compliance authorities as part of standard business processes or as an ad hoc practice.
- Employees must not re-use their credentials (username, password or PIN) used to access Sanlam Kenya resources on other web or social media sites.

Social Media

- Employees should never establish a new relationship via the web when they can't sufficiently verify the other party's identity.
- Employees should understand the terms and conditions and privacy rules of social networking and other sites before accepting them.
- Employees are required to configure security and privacy settings (provided by social media sites and applications) to prevent unauthorized access of communication.
- Employees must be aware of the procedures they need to follow to add, change or delete content they post to social networking sites.
- Employees must familiarize themselves with the policies on each site or application they plan to enroll on as they may no longer have any control over their communication and the information contained therein.
- Employees must refrain from using their company e-mail address and other company contact details (telephone number, job title) when registering on social media sites or applications in their personal capacity.

APPLICABILITY:

This policy applies to all individuals who use, manage, provide and administer information and technology resources and services under the custodianship of Sanlam Kenya or those sourced via third party Service Providers which includes Sanlam Kenya employees, third parties, temporary staff, contractors, external service providers and consultants.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures.

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Infrastructure Policies

Sanlam Kenya Network Security Policy

Document Type	Infrastructure Policy
Owner	Head Of Innovation and Technology

Sanlam Kenya

PURPOSE:

To ensure that adequate network perimeter security measures are in place to protect information and information technology resources from potential loss, data tampering, unauthorised use/ viewing and denial of service.

This policy is aligned to ISO 27001/27002 and COBIT 5 frameworks (DSS01 and DSS7).

RISKS:

There may be a risk of vulnerabilities or threats (internal and external) left unattended, which may be exploited by malicious users or outside attackers and may lead to the disruption of organisational activities, sensitive information disclosure fraud and potential reputational damage.

POLICY STATEMENT:

Network Security

- The principle of "Defence-in-Depth" for security must be followed in the design and implementation of the Sanlam Kenya perimeter network.
- Fault tolerance, backup and recovery must be considered as part of the risk assessment as stipulated in the Business Continuity Management Policy.
- Appropriate steps must be taken to mitigate any business risks identified in response to new or emerging network security threats.
- Different network segments (Trust Zones) must be appropriately segregated. Isolation must be enforced between different Trust Zones.
- Strong cryptography and security protocols must be utilised to safeguard sensitive data during transmission over untrusted networks. Non-standard and older (vulnerable) security protocols should not be used.
- All perimeter security devices are regarded as business critical and must comply with the relevant hardened configuration baseline standards.
- User-to-system connections from an Untrusted Network must not terminate directly within a Trusted Network.
- Split tunnelling will not be permitted.
- Where network perimeter services are provided by third party service providers, the contracts must provide for Sanlam Kenya "right to audit".
- Perimeter security logs must be reviewed periodically by Information Security Officer .
- All perimeter security devices must be configured to log security events.
- Suitable mechanisms must be implemented to ensure timeous alerting and notification of relevant network and security personnel of security incidents or malicious intent.
- Bi-annual security penetration tests must be performed by a trusted security partner..
- All network perimeter security devices must be physically secured, requiring authorised access.
- Firewalling systems must be used to prevent connections and network traffic originating from segments other than the Trusted Network.
- Firewalls Administration must take place over secure connections and be restricted to authorised users, IP addresses/ workstations and must be configured to validate the user and verify the source IP address.
- All connections must have business and system owners who carry the overall accountability for the risk management of their third party connections.

Trusted Network Access Security

- The Sanlam Kenya (internal) network is a private network, closed to the general public.
- Only users who have a valid business need will be granted access to the Sanlam Kenya (internal) network, governed by the principle of least privilege.
- All devices connected to the Sanlam Kenya Trusted network , including those of third parties, must be implemented according to Sanlam Kenya policy, governance, system standards and practises.
- All devices, including end-user and network, must be managed by internal resources or Sanlam Kenya approved service providers.

APPLICABILITY:

This policy applies to all individuals who use, manage, provide and administer information technology resources and services under the custodianship of Sanlam Kenya or those sourced via third party Service Providers which includes Sanlam Kenya employees, third parties, temporary staff, contractors, external service providers and consultants.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures.

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Sanlam Kenya Vulnerability and Patch Management Policy

Document Type	Infrastructure Policy
Owner	Head of Innovation and Technology

Sanlam Kenya

PURPOSE:

To ensure adequate and appropriate controls are in place and that information technology resources are protected in accordance with business' security requirements against the exploitation of known vulnerabilities.

This policy is aligned to ISO 27001/27002 and COBIT 5 frameworks (DSS3).

RISKS:

Unattended vulnerabilities or threats (internal and external) may be exploited by malicious users or outside attackers and may lead to the disruption of organisational activities, sensitive information disclosure fraud and potential reputational damage.

POLICY STATEMENT:

Vulnerability Management:

- Systems must be classified and prioritised by assigning a business impact rating.
- Business owners must be assigned for each asset.
- An asset database must be maintained via existing request and change management processes.
- Automated Vulnerability Scanning Tools must be maintained to ensure an up to date set of vulnerability scan tests are performed.
- All scan results rated as <Level 3,4 or 5> must be analysed and reported, accompanied by appropriate remedial actions.
- All exceptions or scan exclusions must be approved according to the Risk classification framework, documented and stored centrally for future reference.
- All remediation must be tested and verified before deployment to production systems.
- All remediation/mitigation must be subject to the existing change management process and verified by subsequent scans, with documented results kept for future use.
- Vulnerability Management MIS Reports must be made available and limited to the relevant stakeholders.

Security Patch Management:

- Vulnerability Assessment scans and Vendor notifications must be analyzed to determine the applicability of a security patch to remediate a vulnerability.
- Critical security patches must be applied as soon as possible or within 30 days of release.
- Non-critical security patches must be applied at least quarterly as part of the maintenance (change) slots.
- A patch register must be developed and maintained by the relevant platform Application manager and Infrastructure manager.
- All security patches must be subjected to User Acceptance Testing (UAT) and inter-operability testing.
- All security patches must be approved by the Application manger and, if required, the Business Owner of the application or system affected.
- The application of security patches must be subjected to the change control process and change approval board.
- All security patches applied must be verified after implementation.
- If a security patch cannot be applied to remediate a vulnerability, the formal exception process must be followed and exception documented for future reviews.
- System build images or build documents must be revised quarterly to include all approved patches.

APPLICABILITY:

This policy applies to all individuals who use, manage, provide and administer information and technology resources and services under the custodianship of Sanlam Kenya or those sourced via third party Service Providers which includes Sanlam Kenya employees, third parties, temporary staff, contractors, external service providers and consultants.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures.

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Sanlam Kenya Incident Management Policy

Document Type	Infrastructure Policy
Owner	Head Of Innovation And Technology

Sanlam Kenya

PURPOSE:

To reduce the impact of production incidents through the use of standardised methods and procedures for efficient and prompt handling of all incidents logged.

This policy is aligned to ISO 27001/27002 and COBIT 5 frameworks (DSS4 and DSS5).

RISKS:

Incidents not logged, prioritised, authorised or contained could lead to a disruption of the enterprise business activities and damage enterprise information assets. This could result in the extended unavailability of key business systems due to failure of addressing incidents and may result in reputational and financial damage.

POLICY STATEMENT:

- All incidents are to be logged at the Sanlam Kenya Sanlam IT service desk.
- The Service Delivery Manager is accountable for the entire Incident Management process and has the authority to develop policies and procedures pertaining to the process.
- All support issues and incidents must be assigned a valid incident reference number and the user, who logged the incident, must be given this number.
- Only incidents with valid incident reference numbers will be responded to.
- Incidents must be classified and prioritised according to the Sanlam Kenya incident severity rating scale.
- Incidents should be responded to within the defined timeframe for the assigned severity rating.
- Where an incident is deemed to be high priority; as outlined in the Sanlam Kenya incident management process document, the problem management process takes effect.
- As part of the problem management process, root cause analysis investigations must be conducted, and mitigating actions taken, to reduce the risk of high severity incidents re-occurring.
- Incidents are first attempted to be resolved by Service Desk Officer. Where they are unable to resolve the incident it is the agent's responsibility to assign the incident to Infrastructure Officer.
- Continual Service Improvement reviews must be conducted by the Service delivery manager on a regular basis based on the Process Owner's discretion. Reviews should focus on the process consistency and repeatability, and key performance indicators.
- Incident Management metrics and management reports should be provided to management in accordance to outlined procedures.
- The Service delivery manager is responsible to manage all assigned and escalated incidents within Sanlam Kenya's IT Department.
- Incidents should be closed when agreed to by all stakeholders.

APPLICABILITY:

This policy applies to all individuals who use, manage, provide and administer information and technology resources and services under the custodianship of Sanlam Kenya or those sourced via third party Service Providers which includes Sanlam Kenya employees, third parties, temporary staff, contractors, external service providers and consultants.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures.

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Sanlam Kenya Change Management Policy

Document type	Infrastructure Policy
Owner	Head Of Innovation And Technology

Sanlam Kenya

PURPOSE:

To ensure that standardised methods and procedures are used for efficient and prompt handling of all changes, in order to minimise the impact of changes upon service quality and also to ensure that changes happen in a controlled environment and that the impact of changes on the IT Services are understood and all impacted parties are notified.

This policy is aligned to ISO 27001/27002 and COBIT 5 frameworks (BAI6 and BAI7).

RISKS:

Unauthorised, poorly tested and/or inadequately documented changes to IT systems, affecting Sanlam Kenya information, could cause disruption to production systems, increase the risk of system and information integrity being compromised; or create vulnerabilities in systems that can be abused by parties with malicious intent.

POLICY STATEMENT:

- All changes to IT Services must follow the Sanlam Kenya Change Management (CM) process.
- Changes should be logged on a Change management form, prioritised, categorised, assessed, authorised, planned and scheduled.
- The Change Advisory Board (CAB) will assess the risk associated with proposed changes in proposed timeslots. The CAB will approve or decline the proposed changes, based on risk.
- Changes submitted without the relevant information and/or documentation should be returned to the initiator and should only be submitted to the Change Advisory Board (CAB) after all requirements have been met.
- The CAB must be chaired by the Head Of Innovation And Technology or an authorised delegate, supported by the IT System Custodian, BU Representatives, Service Provider Representatives, ISO.
- The CAB will report to all relevant stakeholders on changes approved and declined after every CAB meeting.
- Requests for Change types that has been pre-approved in agreement with Business Risk Committee (standard changes) can be implemented without approval from the business.
- Any request for change requires successful completion of testing prior to authorisation for implementation into the production environment.
- Emergency Changes (or replacement of failed hardware components and Critical Maintenance changes) should follow an Emergency Change process.
- Unsuccessful changes, abandoned changes or changes that exceed the approved change window timeframe – must be escalated and resolved.
- Change implementations must be monitored for successes, trends and failures.
- The CM process must be included into the Sanlam Kenya IT Department's New Employee Induction process.
- Outsourcing contracts must specify predefined maintenance slots for environmental and maintenance changes per technical environment.
- Maintenance slots outside of the standard maintenance slot are subject to agreement with all stakeholders and the IT SYSTEM Custodian.

…es in business cycles in which only justified business critical changes should be allowed for implemented.

Roles and Responsibilities

•The Business system Owner must:
- be responsible for the change management process and is accountable for the release and deployment process
- conduct reviews on a regular basis
- focus on the effectiveness and efficiency of the process.

•The IT System Custodian is responsible for creating the release package for delivery.
•The CAB is responsible for the final communication to all impacted parties and/or clients after approval by the CAB.
•Deployment staff are responsible for the final physical delivery of the service and release implementation.
•Head of IT should coordinate with unit team leaders to have quarterly update from vendors regarding support staff for all key applications. This should capture, staff name, supporting role, mobile and email.

APPLICABILITY:

This policy applies to all individuals who use, manage, provide and administer information and technology resources and services under the custodianship of Sanlam Kenya or those sourced via third party Service Providers which includes Sanlam Kenya employees, third parties, temporary staff, contractors, external service providers and consultants.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures.

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Sanlam Kenya Backup Policy

Document Type	Infrastructure Policy
Owner	Head Of Innovation And Technology

Sanlam Kenya

PURPOSE:

To ensure that the right information is backed up at the right frequency, in line with business continuity requirements and that the process to restore this information is effective.

This policy is aligned to ISO 27001/27002 and COBIT 5 frameworks (DSS06).

RISKS:

A disaster, infrastructure failure or an attack, like Ransomware, could render business critical information un-available. If the business cannot restore the information from backups, it could lead to a breakdown of business processes leading to reputational damage, financial loss and even regulatory penalties.

POLICY STATEMENT:

- A formal backup schedule and inspection/testing procedure which supports and is aligned with the Sanlam Kenya Business Continuity Plans and requirements must be established.
- The necessary level, extent (e.g. full or differential backup) and frequency of back-up information should be defined in consultation with business owners;
- For disaster recovery purposes, a copy of the back-ups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;
- Back-up information should be given an appropriate level of physical, logical security and environmental protection consistent with the standards applied at the main site; the controls applied to media at the main site should be extended to cover the back-up site;
- Back-up media should be regularly tested to ensure that they can be relied upon for emergency use when necessary;
- Restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery;
- In situations where confidentiality is of importance, back-ups should be protected by means of encryption.
- Logs of daily backup processing must be reviewed to identify and rectify any failed backup before it creates an unacceptable risk to the business.
- End user devices will not be backed up. Information that has business importance must therefore be stored, by the user, on the file share or network storage platforms provided by Sanlam Kenya for this purpose.

APPLICABILITY:

This policy applies to all individuals who use, manage, provide and administer information and technology resources and services under the custodianship of Sanlam Kenya or those sourced via third party Service Providers which includes Sanlam Kenya employees, third parties, temporary staff, contractors, external service providers and consultants.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures.

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

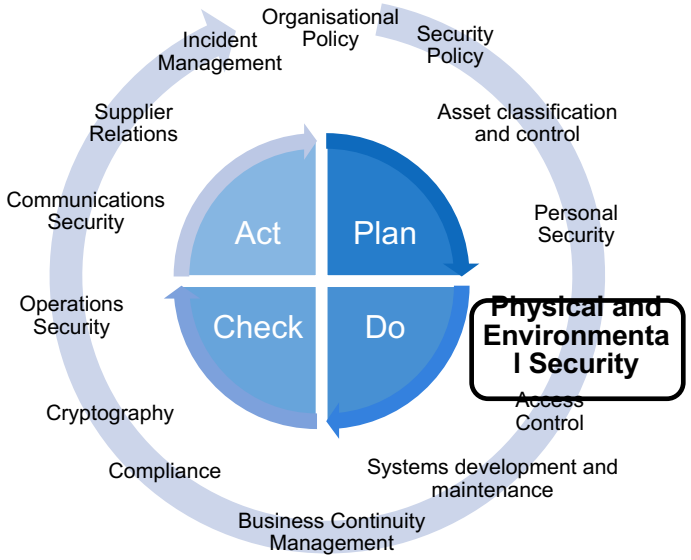
Sanlam Kenya Physical Security Policy

Document Type	Infrastructure Policy
Owner	Head Of Innovation And Technology

Sanlam Kenya

PURPOSE:

To ensure that physical security controls are implemented to ensure the confidentiality, integrity and availability of information at data processing facilities and environments where users handle sensitive information.



This policy is aligned to ISO 27001/27002 and COBIT 5 frameworks (DSS1).

RISKS:

Unauthorised access to areas, or infrastructure, where sensitive information is processed could create opportunity to disrupt processing, change or leak sensitive information.

POLICY STATEMENT:

Secure Areas

- Facilities must be designed to consider risks to data and infrastructure.
- Adequate measures must be implemented to ensure that critical or sensitive processing facilities are housed in secure areas.
- Data retained from access control systems must be adequately secured and backed-up.
- Access to facilities must be restricted to authorised individuals and monitored continuously.
- The sharing of physical access cards or security tokens must be prohibited, unless approved and monitored by Sanlam Kenya.
- Procedures must be developed and enforced to allow for the monitoring and control of access to visitors.
- Controls must be implemented to physically protect data transmission lines within Sanlam Kenya control.

Physical Security for Employees

- Employee access should be based on the principle of least privilege, including physical access.
- Employees should ensure that the Sanlam Kenya assets are not taken off site without prior authorisation.
- Laptops and desktops left unattended should be physically secured and locked.
- Employees have a general obligation to ensure that confidential, sensitive or personal information is adequately secured and not visible or accessible (to un-approved individuals) in their work environment.
- When disposing of physical documents containing confidential, sensitive and personal information, designated shredding machine(s) or waste bins should be used.

Equipment

- All network perimeter security devices must be located in physically secure locations with access to these locations restricted to authorised personnel.
- Access rights to the devices must be audited and verified on a regular basis.
- All equipment must be disposed off in a secure manner – appropriate to the type of device and the type of content processed by it.

Environment Safeguards

- Environmental safeguards to protect against hazards such as flooding, electromagnetic interference, fires, power failures and pests must be evaluated, implemented and maintained as appropriate.
- The ability must be established to monitor, detect and maintain variation in temperature and humidity associated with the use of Heating, Ventilation and Air Conditioning (HVAC) systems to manufacturer's specifications.
- Management interfaces to Environmental Systems (like HVAC and CCTV) must be appropriately secured and should be segmented from the data processing network.
- The design of the facility must be in such a manner so as to minimise the risk of visual disclosure of sensitive information to unauthorised individuals.

APPLICABILITY:

This policy applies to all individuals who use, manage, provide and administer information and technology resources and services under the custodianship of Sanlam Kenyaor those sourced via third party Service Providers which includes Sanlam Kenya employees, third parties, temporary staff, contractors, external service providers and consultants.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures.

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Sanlam Kenya Cloud and Technology Outsourcing Policy

Document Type	Infrastructure Policy
Owner	Head Of Innovation And technology

Sanlam Kenya

PURPOSE:

To specify sourcing guidelines, prescribe a cloud risk model and the governance for Cloud Computing and to provide the rules that will address known areas of risk in Cloud Sourcing and Technology sourcing.

This policy is aligned to ISO 27001/27002 and COBIT 5 frameworks (AP010 and BAI3).

RISKS:

Poor selection of outsourcing and cloud solutions, could create reputational, legal and compliance risk for Sanlam Kenya. Poor implementation could also create gaps in the security posture or weaken the effectiveness of Operational support procedures.

POLICY STATEMENT:

Responsible Sourcing:

- Sanlam Kenya must ensure that Service Level Agreements (SLAs), Contractual requirements, and availability of Cloud Service Provider (CSP) documentation is completed and maintained.
- All regulatory/compliance, support, architectural, integration, service termination and security requirements, and the total cost of ownership must be considered before approving the use of a cloud or outsourced solution.
- <Infrastructure Manager and Information Security Officer must sign-off on the solution before a contract can be signed with a CSP.
- The Sponsor or Owner of the outsourcing/cloud agreement is responsible to ensure that risks related to the use of the cloud solution are documented, communicated and appropriately managed.

Governance:

- Sanlam Kenya must have a Cloud strategy, compliant with this policy, which must:
  - state the geographies where data may physically reside.
  - State the minimum criteria that CSP's must satisfy
  - State under what circumstances cloud sourcing will not be allowed.
- An Information Security Due Diligence must be done on the CSP.
- A Risk assessment of the gaps identified must be used in the sourcing decision, and reviewed every 1 year.

Compliance and Audit

- Applicable regulatory and jurisdictional requirements must be identified and adequately contracted and provided for with the CSP.
- The right to audit must be negotiated with the CSP (where updated external audit reports are not available on an ongoing basis).

Information Ownership:

- CSPs who claim ownership of the Sanlam Kenya data may ***not*** be used.
- CSP's who only operate in geographies where Sanlam Kenya will lose ownership rights to information (due to legislation); may not be used.

Architecture

- Reliable and cost effective internet connectivity must be established to support the cloud solution.
- Systems Management functions, including the monitoring, logging, auditing, and the use of proprietary technology and nonstandard APIs should be identified before contracting with the CSP.

Business Continuity Management

- Business continuity and disaster recovery procedures must be rehearsed and practically tested in accordance with Business Continuity Planning.
- Where applicable, backups must be encrypted and stored at approved off-site locations, in accordance with the Backup Policy.

Incident Management

- Incident Management procedures must be developed and agreed upon with the CSP.
- Penalties for data breaches payable by the CSP must be specified in the contract.

Application Security

- Security of the CSP must be verified by a third party service provider (with suitable accreditation).
- It is imperative that either the Sanlam Kenya Business or the CSP must ensure that the necessary controls are in place to obscure data where required

APPLICABILITY:

This policy applies to all individuals who use, manage, provide and administer information and technology resources and services under the custodianship of Sanlam Kenya or those sourced via third party Service Providers which includes Sanlam Kenya employees, third parties, temporary staff, contractors, external service providers and consultants.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures.

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

IT Governance Policies

Sanlam Kenya IT Risk Management Policy

Document Type	Infrastructure Policy
Owner	Head Of Innovation And technology

Sanlam Kenya

PURPOSE:

The policy ensures that the organisations <Org Name> IT risk management capability supports the achievement of and aligns to the <Org Name> Group Risk Assurance Framework.

This policy is aligned to ISO 31000 and COBIT 5 (AP012).

RISKS:

Risks may be incorrectly identified and communicated within the enterprise. Appropriate risk responses need to be put in place.

POLICY STATEMENT:

Understanding the Context

It is important that the Sanlam Kenya Board, Sanlam Kenya management and the Sanlam Kenya Information Security Officer have a shared understanding of:

- the relationship between Sanlam Kenya and its operating environment.
- those factors that support or impair its ability to manage the risks it faces.
- the business capabilities and its goals, objectives, strategies and values and the drivers of these.

Risk Management Process

- Sanlam Kenya must establish and maintain an effective risk management process covering the full range of functional domains, including Information Technology, which must be adequately incorporated into risk management procedures.

Risk Identification

- Risks must be identified at all levels across all the Sanlam Kenya functional domains.

Risk Management Actions

- The risk response approach and supporting actions must be documented and monitored continuously for on-going relevance.

Responsibility

- The Sanlam Kenya Information Security Officer will determine the risk management framework appropriate for IT Department.

Ongoing Monitoring and Reporting

- Sanlam Kenya will customise reporting and monitoring to a level as to best fit and serve the defined Sanlam Kenya IT governance and management processes

Setting the IT Risk Appetite

- Key risk indicators for all categories of risks must be identified and measured regularly against agreed targets set by Sanlam Kenya Executive and IT Management.

Risk Categorisation Matrix

- The risk rating scale/matrix that is used for IT Risk Management must be aligned with enterprise risk rating models (example below)

Type of risk / loss event			Likelihood					
			1	2	3	4	5	6
			Rare <1%	Unlikely <5%	Possible-<20 %	Possible+ <50 %	Likely <80 %	Almost certain >80%
Impact	6	Extreme	M	H	H	VH	VH	VH
	5	Major	L	M	H	H	VH	VH
	4	Moderate+	L	M	M	H	VH	VH
	3	Moderate-	L	L	M	M	H	H
	2	Minor	L	L	L	M	M	M
	1	Insignificant	L	L	L	L	L	M

APPLICABILITY:

This policy applies to all individuals involved with IT Risk Management.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures. The policies can be found at the following link: https://sanlamem.sharepoint.com/sites/skplc/PolicesAndProcedures/

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Sanlam Kenya Business Continuity Management Policy

Document Type	Infrastructure Policy
Owner	Head Of Innovation And technology

Sanlam Kenya

PURPOSE:

To ensure plans and alternative service options are in place to meet BCM needs in the event of a significant business outage or disruption.

This policy is based on the ISO 27001 / 27002 and COBIT 5 frameworks (DSS6).

RISKS:

There may be a risk of that the organisation will not be able to continue its business operations for an extended time after a disaster. This could lead to reputational or financial damage.

POLICY STATEMENT:

- Business Continuity Management (BCM) Policy enables Sanlam Kenya business continuity in the event of various risks materializing.
- A risk assessment (RA) must be conducted to identify critical operational processes and key IT systems and their exposure to threats.
- A Business Impact Analysis (BIA) must be conducted to evaluate the impact over time of a disruption of the activities that support Sanlam Kenya key services, on a regular basis.
- BCM recovery strategies must be developed or updated based on the outputs of the BIA.
- Sanlam Kenya must develop and maintain Business Continuity Plans (BCP's) that include Crisis Management and Emergency Response.
- An Sanlam Kenya IT Department Recovery Plan (IT DRP) must be developed to provide a solution for the recovery and continuation.
- Managers or staff tasked with Business Continuity Management must receive appropriate training to enable them to fulfil their functions.
- BCM testing shall be regularly conducted according to a testing schedule.
- Organisational preparedness in responding to disruptive incidents must be established and validated on a regular basis.
- The Business Continuity Plans, Governance Structures and Policy must be reviewed and updated at least annually, or when significant relevant changes take place. These must be amended, if necessary, to take into account new legal or regulatory requirements, and implementation of relevant standards.
- Business Impact Analysis and Risk Assessments must be conducted at least annually, with business continuity plans updated quarterly.
- The Business Continuity and Disaster Recovery plan and processes will be updated as part of all major technology, system, application or business process changes, and any premises, personnel, branch structure or service changes that impact on resumption and recovery procedures.
- When a new project is identified, Business Continuity requirements will be identified and addressed as part of the non-functional requirements for the project.

APPLICABILITY:

This policy applies to all individuals involved with Business Continuity Planning, Senior and IT Management within Sanlam Kenya.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures. The policies can be found at the following link: : https://sanlamem.sharepoint.com/sites/skplc/PolicesAndProcedures/

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Sanlam Kenya IT Continuity Policy

Document Type	Infrastructure Policy
Owner	Head Of Innovation And technology

Sanlam Kenya

PURPOSE:

To ensure that business risks arising from disasters and loss of IT services will be managed to an acceptable level by planning for the recovery of IT services.

This policy is aligned to ISO 27001/27002 and COBIT 5 frameworks (AP013)

RISKS:

There may be a risk of that the organisation will not be able to continue its business operations for an extended time after a disaster. This could lead to reputational or financial damage.

POLICY STATEMENT:

- Each Business Unit in Sanlam Kenya must define and maintain its Business Continuity Plan (including Work Area Recovery(WAR) requirements), which will be used as input by IT Management to define the IT Continuity (ITC) Plan.
- IT Continuity documentation must be kept current and stored in the Sanlam Kenya battle-box in an off-site location which will be easily accessible in event of a disaster at the primary data centre.
- Sanlam Kenya Business Units must participate in Disaster Recovery tests, table top exercises and mock call-outs managed by IT.
- All Sanlam Kenya Business Units must create a list of their DR critical applications and maintain the information on risk register. These DR critical environments require standard battle-box information to be maintained by the respective Business entities and stored off-site by Sanlam Kenya
- Business entities must articulate the Disaster Recovery scenarios they need to guard themselves against in the form of a Disaster Recovery Plan.
- Business entities must state their down-time tolerance of critical processes and applications, and plan ITC with IT Department accordingly.
- ITC plans should be tested in accordance with the regulatory and business risk requirements, at a minimum of once per annum.
- Sanlam Kenya Business Units must agree a formal backup schedule and inspection procedure with IT.
- Management of ITC deliverables must be enforced through contracting and SLA's (Service Level Agreements), where services or components thereof is outsourced to third parties.
- IT Service providers used by Sanlam Kenya must include the practice of preparing for disasters by establishing, testing and implementing the strategies, processes and procedures imperative to minimise the impact of service unavailability on customers, according to formal service level agreements.
- The development of new IT Solutions must cater for the availability and restore requirements by design.
- The IT Department must maintain contact details for their key resources and must ensure contingency planning around these resources' skills.
- Testing should embrace practices and methods to authenticate the efficiency of the backup plans and to determine if the required data is backed up and if it can be retrieved and restored according to service level agreements from a Service Provider perspective, and if it can meet the Recovery Time Objectives and Recovery Point Objectives from a business perspective

APPLICABILITY:

This policy applies to all individuals involved with Business Continuity Planning, Senior and IT Management within Sanlam Kenya.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures. The policies can be found at the following link: : https://sanlamem.sharepoint.com/sites/skplc/PolicesAndProcedures/

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Process and Guidelines

Sanlam Kenya Firewall Rule Management

Document Type	Infrastructure Policy
Owner	Head Of Innovation And technology

Sanlam Kenya

PURPOSE:

To provide high level principles and guidelines to set-up and manage firewall rules.

This guideline is aligned to ISO 27001/27002 and COBIT 5 frameworks (DSS07).

Guideline Statements

- Separation of duties must exist between individuals who approve rule changes and the individual who implement them.
- The firewall infrastructure must be clearly documented with graphical, logical network diagrams containing detailed information about all the components of the infrastructure, which is updated regularly.
- All firewall components must be backed up according to the **Backup Policy**.
- All changes to the firewalls must be documented using the change management process.
- Firewall rule base must be configured with a “default deny” posture. Traffic that is not explicitly needed for business reasons must be blocked by default.
- The firewall rule base must be reviewed at least every 6 months
    - During this review all dormant rules must be identified and removed or disabled.
    - Ownership of rules and third party connections must be confirmed and documented
    - Deviations from security principles (least privilege) and standards (like rule descriptions) should be identified and rectified.
- Firewall rules must be written from the perspective of “least privilege”. This means that additional objects are not permitted in a rule if there is no explicit business need and approval for connectivity.

Basic Network Segments:

- The ***Un-Trusted Segment*** denotes the direct Internet facing segment(s). Direct connectivity with the ISP’s are housed here.
- The ***Semi-Trusted Segment*** demarcates the point of hand-off or proxy through which all connections must traverse (unless otherwise required). This includes hosting of websites and third party connectivity. It also includes devices to facilitate remote access to the Trusted Segment. Separate DMZs must be used to host the different services.
- The ***Trusted Segment*** denotes the internal/ private network access through either wired or wireless connectivity. This includes the Off-Site Trusted segment.

Firewall Rules Types:

The following guidelines apply to implementing firewall rules.

Type A Firewall rules

- Specified source IP address is allowed to connect to specific destination IP address for specifically permitted protocols.

Type B Firewall rules:

- From Trusted Segment destined for Un-Trusted Segment.
    - Source IP or subnet will be allowed to connect to a proxy device in Semi-Trusted Segment (for traffic destined to the Un-Trusted Segment).
- From Semi-Trusted Segment destined for Un-Trusted Segment
    - Proxy external interface IP or NAT IP will be allowed to connect IP addresses in the Un-Trusted Segment.
- From Un-Trusted Segment destined for Trusted Segment.
    - Any IP address allowed to connect to a reverse proxy or VPN segment in Semi-Trusted Segment.
- From Semi-trusted segment destined for Internal segment.
    - Source IP address allowed to connect to specific destination IP for specific and approved protocols.

Type C Firewall rules:

- System-to-System firewall rules are allowed where specific and approved IP addresses and protocols are specified.
- This applies to Trusted Segment system’s access to Un-Trusted Segment resources and vice versa.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures. The policies can be found at the following link: : https://sanlamem.sharepoint.com/sites/skplc/PolicesAndProcedures/

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Sanlam Kenya Vulnerability Management Process - Example

Document Type	Infrastructure Policy
Owner	Head Of Innovation And technology

Sanlam Kenya

PURPOSE:

To demonstrate the steps involved in Vulnerability Management to ensure pre-emptive and pro-active remediation of vulnerabilities to minimize security related incidents.

This process is aligned to ISO 27001/27002 and COBIT 5 frameworks (DSS2 and DSS3)

Overview:

The process of Vulnerability Management requires a number of activities to ensure that vulnerabilities on the <Org Name> network are timeously identified and remediated

Step 1: Detection → Step 2: Assessment → Step 3: Testing → Step 4: Remediation → Step 5: Reporting

Process Steps

- **Step 1:**
  - The scope of vulnerability scans are agreed with business and IT stakeholders and is based on the asset list in the CMDB/Asset Register
  - Vulnerability scans are performed for all security vulnerabilities on operating systems and technologies used in Sanlam Kenya
  - The scan is run on all Sanlam Kenya assets agreed within scope.
  - The scan results are saved in a central location.
- **Step 2:**
  - Once the scan is run the vulnerabilities are assessed by the Information Security Officer
  - The Information Security Officer creates a record of identified but un-remediated vulnerabilities and communicate it with the Information Security Officer and relevant technology asset owners.
  - The Information Security Officer and technology asset owner agree to an action plan based on the risk posed by the vulnerability and the criticality of the asset that it applies to.
- **Step 3:**
  - Information Security Officer invokes the Security Patch Management process for the testing of the relevant patches to address the identified vulnerabilities.
  - The Information Security Officer requests the testing of the identified remediation/s (other than patches) and requests feedback regarding the results from the relevant Internal/External Service Provider (where applicable)
- **Step 4:**
  - The Information Security Officer evaluates the testing results and makes a decision regarding implementation of remediation
- **Step 5:**
  - The ITISS Information Security Consultant re-scans the affected technologies, generates monthly vulnerability reports and distributes it to the Information Security Officer .
  - These reports indicate progress (in remediating vulnerabilities) and current status of vulnerabilities. This information must be made available to IT Executive Management and Risk Management forums to ensure that high risk issues receive the right level of attention.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures. The policies can be found at the following link: : https://sanlamem.sharepoint.com/sites/skplc/PolicesAndProcedures/

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Sanlam Kenya Patch Management Process Example

Document Type	Infrastructure Policy
Owner	Head Of Innovation And technology

Sanlam Kenya

PURPOSE:

To provide the steps required to allow <Org Name> to install vendor supplied software or bespoke software/application patches to correct deficiencies that exist in the vendor's or bespoke software/application products

Overview:

A patch is a piece of software designed to fix problems, update a computer program or its supporting data or improve the usability or performance the program. Though meant to fix problems, poorly designed patches can sometimes introduce new problems hence the need to test systems once patches have been installed

Step 1: Identify Security Patches to be applied → Step 2: Test/ Certify Security Patches → Step 3: Decide whether to apply security patch. If not Determine Risk and register security patch exception → Step 4: Log Change and apply security patch → Ste 5: Audit applied Security Patches → Step 6: Update device configuration with security patch attribute/s

This process is aligned to ISO 27001/27002 and COBIT 5 frameworks (DSS3)

Process Steps

- **Step 1:**
  - The process is triggered by the Vulnerability Management Process, Risk reports, Audit reports, Penetration tests, Vendor published information or Security Announcements.
  - Patches are identified that will rectify vulnerabilities in technologies currently used by Sanlam Kenya.
  - These patches are captured in the Security patch register
- **Step 2:**
  - The applicable IT service and support providers are requested to determine (test) if a patch will disrupt existing IT systems, and must update the Security patch register with their recommendations.
- **Step 3:**
  - The Information Security Officer evaluate the recommendations of the service providers and application support providers and update the Security patch register with the decisions to apply or not.
    - If the decision is to apply the patch then the Information Security Officer will inform the application or asset owner of the decision and request them to inform their service provider to apply the patch.
    - If the decision is to not apply the patch then the ISO will inform the application or asset owner of the decision and invoke Sanlam Kenya IT Security Exception/Risk Acceptance process.
- **Step 4:**
  - When the service providers are tasked with applying the patches they are responsible to log the change request.
- **Step 5:**
  - Once the security patch has been applied the IT infrastructure is audited (scanned) to determine if the vulnerability has been remediated
- **Step 6:**
  - The last action in this process is to update the configuration information of the applicable devices with the security patch attributes.

Process Statements

- Security patches will be applied quarterly, but Critical Patches will be applied as soon as possible but no later than 30days

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures. The policies can be found at the following link: : https://sanlamem.sharepoint.com/sites/skplc/PolicesAndProcedures/

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Sanlam Kenya Incident Management Process

Document Type	Infrastructure Policy
Owner	Head Of Innovation And technology

Sanlam Kenya

PURPOSE:

To detail the processes and procedures crucial in the prompt handling of all incidents logged.

This process is aligned to ISO 27001/27002 and COBIT 5 frameworks (DSS04).

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Overview:

The process of Incident Management requires a number of processes and interactions between Sanlam Kenya users, agents and Service Provider/s. The diagram, below, illustrates the processes through which incidents are handled:

Step 1: Users log and update incidents based on some standardized template → Step 2: Incidents are either resolved by agents or escalated according to predetermined guidelines on priority, skill and responsibility → Step 3: Based on criticality of incident and assets affected, escalated incident is either resolved or dealt with as a problem (Problem management) → Step 4: Issues that are flagged as problems are analysed and root cause analysis is performed. Once issue is resolved, mitigation actions to address the root cause get documented and actioned → Step 5: Incidents are resolved (closed) upon confirmation that the user is satisfied that the incident has been resolved

Process Steps

- **Step 1:**
  - Incidents may be logged by either users or technical/service desk resources (on behalf of users).
  - Incidents may only be actioned upon once sufficient information has been provided. Templates or process documents detail information needed are predetermined, these may vary based on users, rights, infrastructure and software in place or business cases.
  - Incidents are checked against some master file of open logged incidents to screen for duplicates made by users or groups of users.
  - The person who logged the incident receives an incident number which will be used for reference and query purposes.
- **Step 2:**
  - The incident responder resolves the issue, if it is simple and well known type of incident for which a solution has already been created and documented.
  - More complex and new types of incidents are escalated to the second line support (more technical resources) for investigation and resolution.
  - Escalations like this is always according to a pre-agreed priority guideline and to a pre-agreed second-line support role.
  - Assignee record comments on the state and status of work being actioned on an incident.
  - Users are informed as incidents are received, assigned and updated on progress to prevent the re-logging of incidents.
- **Step 3:**
  - High criticality incidents without known solutions are flagged as problems.
  - Problems are assigned to an expert or team of experts, who will investigate the problem as a top priority.
- **Step 4**
  - The root cause of the problem will be identified and documented.
  - Action plans to reduce the immediate impact, as well as, to address the root cause of the problem in the long term will be agreed, documented and actioned.
  - First and second line responder documentation (process and knowledge base) is updated with relevant information generated by the problem management process.
- **Step 5**
  - Once the incident has been resolved the client is contacted and informed that the incident has been resolved.
  - Once the client confirms that their issues were resolved, the incident will be closed.

STANDARDS AND GUIDELINES:

To be read in conjunction with other Sanlam Kenya policies, standards and procedures. The policies can be found at the following link: : https://sanlamem.sharepoint.com/sites/skplc/PolicesAndProcedures/

Standards

Sanlam Kenya Password Standard

Document Type	Infrastructure Policy
Owner	Head Of Innovation And technology

Sanlam Kenya

PURPOSE:

To ensure that the password related mechanisms are adequately configured to facilitate adherence to the <Org Name> <Logical Access Management Policies> .

This policy is aligned to ISO 27001/27002 and COBIT 5 frameworks .(DSS7)

Password Standard

- Passwords must meet complexity requirements. Passwords must:
  - contain a minimum of one numeric value (i.e.1234567890).
  - not be easy to guess.
  - contain a special character (e.g. ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/ etc.).
- The Password History must be configured to enforce the previous 24 passwords to be remembered.
- Where applicable, passwords must not be stored using reversible encryption.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- The “remember password” feature must always be declined (disabled).
- Password changes should be communicated through ‘out-of-band’ methods.
- Accounts must be configured to lockout after 4(four) consecutive, unsuccessful passwords attempts and remain locked until unlocked by a ICT team.
- Any deviation from the above must be logged on the IT risk register
- Summary of account password and lock out attributes:

NON-COMPLIANCE

Failure to comply with Sanlam Kenya IT policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.
Requests for exceptions to Sanlam Kenya IT policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form and submitted to the Risk Department.

Description	End user account	Privileged Account	Service accounts	Mainframe accounts
Minimum password length (characters)	8	10	14	6
Maximum password length (characters)	-	-	-	8
Minimum password age (days)	1	1	3	0
Maximum password age (days)	40	40	Not expire	31
Password complexity enforced	Yes	Yes	Yes	No
Number of numeric characters	1	1	1	0
Number of special characters	1	2	3	0
Password history	24	24	24	15
Store using reverse encryption	No	No	No	-
Account lock	7	7	Not required	4
Account lockout duration	30	30	Not required	Indefinitely
Account lockout threshold	30	30	Not required	Indefinitely