A. SCOPE OF WORK

The scope is for end-to-end assessment from the end user at Treasury back office to the servers and network to the SWIFT service Bureau, which is Trustlink. The assessment will be done based on the **SWIFT Customer Security Controls Framework (CSCF) V2021**. According to SWIFT CSCF, Eskom's architectural type is A4 and requires compliance with the following mandatory security controls:

a) **Operating System Privileged Account Control**

The service provider should assess built-in administrator account and members of groups with administrator privileges (for example, accounts with debug or file system privileges). Typically, Enterprise Admins group, Domain Admins group and Local Administrator group for the following:

- Access to administrator-level operating system accounts is restricted to the maximum extent possible unless needed to install, configure, maintain, operate and support emergency activities. The use of the administrator-level account is limited to the duration of the activity (for example, maintenance windows).
- Log-in with built-in administrator-level accounts is not permitted, except to perform activities where such accounts are specifically needed (for example, system configuration) or in emergency situations (break-glass account).
- Individual administrator-level account access and usage are logged so that activities can be reconstructed to determine the root-cause of incidents.
- Administrator-level passwords are tightly controlled with physical access controls when physically recorded.

b) **Virtualisation Platform Protection**

The service provider to assess the secure virtualisation platform, virtualised machines and supporting virtual infrastructure (such as Messaging interface, Communication interface, Firewalls and general-purpose operator PCs) to the same level as physical systems as follows:

- Vulnerability scanning is performed on SWIFT-related VM's and when technically possible on the virtualisation platform.
- The virtualisation platform hosts are subject to physical protection preventing unauthorised physical access.
- VM's isolation is ensured on the virtualisation platform to prevent a) lateral move out of a virtual machine to access or interact with other VM's or the

underlying hypervisor or b) bypassing normal network controls that filter and/or inspect connections to the SWIFT environment.

o Filtering and expected inspection of the network flows reaching the SWIFT-related VMs are performed preferably using resources (such as FW, packet inspections or content filtering) external to the virtualisation platform or must be enforced at the hypervisor level.

o Provided that isolation is ensured on the virtualisation platform, the hosted VM's can keep their (security) classification and be individually secured accordingly (as such, they would not inherit the classification of the SWIFT related VM's and be subject to all SWIFT related controls).

- If multi-factor authentication is implemented for interactive access to the SWIFT related VM's operating systems, preventing direct access to those VM's from the hypervisor layer, multi-factor authentication is not mandated at the virtualization platform management level.

c) **Restriction of Internet Access**

The service provider to assess the secure virtualisation platform, virtualised machines and supporting virtual infrastructure (such as Messaging interface, Communication interface, Firewalls and general-purpose operator PCs) to the same level as physical systems as follows:

i) Internet access from the secure zone

- General purpose internet browsing (including Web Mail activities) from systems within the SWIFT secure zone is not permitted.
- Internet access from systems within the secure zone (for example, dedicated operator PCs or other SWIFT-related components) is highly restricted and ideally blocked.
  - When possible, activities that require the internet are conducted outside of the secure zone. Example activities may include conducting daily business on swift.com or downloading security patches for secure transfer into the secure zone.
  - If internet access is needed from within the secure zone, access should be granted only to whitelisted URL destinations via a proxy with content inspection and adequate blocking/filtering controls. Connections are only permitted if initiated in the outbound direction.

- As the entry point into the secure zone, the jump server, located within the secure zone or another existing secure zone that has similar controls, does not have internet access.

ii) Internet access from general operator PCs

- Control internet access provided on the general-purpose operator PCs used to
  - connect to an application at the service provider (user-to-application) to process financial transactions.
  - access a messaging or communication interface through a browser-based GUI (for example, Alliance Web Platform) through one of the following options:
    - Internet access through a remote desktop or virtual machine solution
    - Internet access from the general-purpose operator PC to only whitelisted URL destinations via a proxy with content inspection, in combination with adequate blocking/filtering controls and permitting only outbound initiated connections.
    - Internet access from the general-purpose operator PC through a Web Gateway (with content inspection, in combination with blocking/filtering controls) using maintained blacklisted URL destinations
- Even if SWIFT strongly recommends controlling internet access, another way to meet the control objective on those PCs accessing the local SWIFT infrastructure is to enforce usage of a jump server that has no internet access combined with multi-factor authentication, in line with control 4.2, implemented on the individual SWIFT related applications/systems or at the jump server.

iii) Internet Access from other components (middleware servers or the virtualisation platform - Advisory)

- Internet access from, when used, the middleware system (such as IBM® MQ server) or the virtualisation platform underlying system (also referred as the hypervisor) is highly restricted and ideally blocked.
  - When possible, activities that require the internet are conducted from other systems. Example of such activities include conducting daily business or downloading security patches for secure transfer into the target system.
- If internet access is needed from those systems, access should be granted only to whitelisted URL destinations via a proxy with content inspection and adequate blocking/filtering controls. Connections are only permitted if initiated in the outbound direction.

d**) Security Updates**

- Vendor support
  - All software (including operating systems) and hardware (including network devices) are within the actively supported product lifecycle window of the vendor (including extended support), if applicable.
  - Maintenance or licensing contracts are in place for access to updates, minor upgrades, and other critical maintenance functions.
- Mandatory software updates: Mandatory releases or updates that are applicable to a local SWIFT component are installed within the deadline specified by the vendor.
- Application of security updates:
  - A risk assessment process is in place to determine the most appropriate treatment of vendor security updates/patches. Risk assessment considerations may include: the vendor-reported criticality of the patch, user exposure and vulnerability, mitigating controls, and operational impact.
  - User-defined deployment timelines are established for applying patches based on criticality, system type, and required patch testing.
  - In the absence of established internal processes and timelines, SWIFT recommends the use of Common Vulnerability Scoring System (CVSS) Version 3 as a guideline for criticality, with the following patch deployment targets:
    - Critical (9.0+ score): applied within 1 month of release
    - High (7.0 - 8.9 score): applied within 2 months of release
    - Low / Medium (< 7.0 score): user defined.
- Source and integrity validation of software and security updates
- Before applying the software and security updates, their legitimate source is validated and integrity checks (for example checksum validation) performed when technically possible.

e) **System Hardening**

Vendor to assess that Security hardening is conducted and maintained on all in-scope components (such as Messaging interface, Communication interface, Firewalls and general-purpose operator PCs). At a minimum, the hardening process should:

- Change default passwords,
- Disable or remove unnecessary user accounts,
- Disable or restrict unnecessary services, ports, and protocols,
- Remove unnecessary software,

- Restrict physical ports (for example, USB) as appropriate,
- Set, when technically possible, auto-lock options (such as activating an operator PC screen saver requiring to sign-in again after an inactivity time-out or once turned into sleep mode – a 15-minute inactivity time-out is recommended)
- Adjust any default configurations known to be vulnerable.

f) **Operator Session Confidentiality and Integrity**

Vendor to assess that the confidentiality and integrity of interactive operator sessions connecting to SWIFT-related applications (local or at the service provider) or into the secure zone is safeguarded as follows:

- All interactive sessions are protected by a cryptographic protocol (for example, ssh, https with one-way TLS).
- Protocols use a current, commonly accepted cryptographic algorithm (for example, AES31, ECDHE32), with key lengths in accordance with current best practices. More guidelines on cryptographic algorithms supporting secure protocols can be found in SWIFT Knowledge Base TIP 5021566.
- Operator sessions and other session types (for example, admin or maintenance) have an inactivity lock-out feature that limits the session to the minimal timeframe necessary to perform business-as-usual duties.
- If the inactivity lock-out is not implemented at the application level, it should be implemented at the operating system-level of the application, or on the jump server.

g) Vulnerability Scanning

Vendor to assess the following for the secure zone (Messaging interface, Communication interface, Firewalls and general-purpose operator PCs):

- Vulnerability scanning is performed at least annually or after any significant change to the environment (for example, introduction of new servers or components and network design change modifying/increasing the range of in-scope components).
    - Vulnerability scanning tools are from a reputable vendor and updated with scan profiles within one month prior to scanning.
    - The most appropriate type of vulnerability scanning (such as using credentials or black box) is selected for the environment. Any administrative credentials used for scanning are appropriately protected.

  - Sufficient risk-based safeguards are in place to minimise any operational impact (for example, running scans in safe mode, or omitting systems that may be negatively affected from the scan).
- Beyond vulnerability identification through scanning, all penetration tests or effective vulnerability tests on or through SWIFT-related services and products are consistent with the SWIFT Customer Testing Policy.
- The outcome of the vulnerability scanning is documented (with restricted access) and analysed for appropriate action and remediation (such as applying security updates in line with control 2.2).
- Once per quarter, month or ideally real-time scanning is recommended.

h) Physical Security

Vendor to assess that physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.

- Security of Removable Equipment:
  - Sensitive removable equipment (for example, PIN Entry Device (PED), PED keys, SWIFT-related smart cards, USB Tokens, TOTP Devices) is supervised or securely stored when not in use.
  - Sensitive removable equipment required for normal continuous operations (for example, hot swappable disks, HSM devices) are hosted in a data centre or, at a minimum, in a locked room.
  - Back-up media (for example, tapes) is physically secured.
- Security of the Workplace Environment
  - Operator PCs are located in a secured workplace environment where access is controlled and granted only to employees and other authorised workers and visitors. A separate physical area for operator PCs accessing SWIFT systems is not required.
  - Printers used for SWIFT transactions are located in a secured workplace environment and their access is restricted.
  - USB and other external access points on operator PCs are disabled to the maximum extent possible, while still supporting operations (for example, when tokens are required to authenticate users or message operations).
- Security for Remote Workers (for example, teleworkers, "on call" operations staff)
  - A security policy is established to support expected use cases for remote workers. The following items are considered when establishing the policy:
    - Physical security of the expected teleworking environment,

        - Rules for personal equipment used for SWIFT business purposes (for example, personal PCs cannot be used to access the SWIFT infrastructure, however personal mobile devices can be used as a second authentication factor),
        - Security during use in public environments,
        - Security during public and private transport,
        - Equipment storage,
    - Unauthorised access to equipment (for example, from family or friends),
    - Remote access requirements (recommended VPN with multi-factor authentication),
    - Protection of mobile devices used for authentication, such as OTP (recommend enabling password and auto-lock features),
    - Compensating controls (for example, virtual desktop preventing local storage; full-disk encryption),
    - Reporting of security incidents (for example, theft) while working remotely.
- Security of the Server Environment
    - Servers are hosted in a data centre or, at a minimum, in a locked room with limited and controlled access (for example, using access control cards or biometrics).
    - Ideally, servers are rack mounted. A risk assessment is conducted to determine if a separate and exclusive rack, or the locking of the rack, is appropriate based on the existing data centre physical access controls.
        - The server environment has video surveillance with movement detection and recording equipment. The implementation of video surveillance recording, and retention of images comply with applicable laws and regulations. Ideally, images are retained for at least three months.
        - No physical reference to SWIFT on servers (for example, labels).
        - External ports (for example, USB, serial bus) on servers are disabled to the maximum extent possible while still supporting operations.
- Physical Access Logging and Review
    - Physical access to sensitive equipment areas (for example, data centre, secured storage) is logged.
    - Physical access logs are available for audit and investigations and are retained for a minimum of 12 months and in compliance with applicable laws and regulations.
    - Physical access is promptly revoked (or modified) when an employee changes roles or leaves the organisation.
    - Physical access control lists are reviewed at least annually.

i) Password Policy

Vendor to assess that all application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed log-in attempts. Similarly, personal tokens and mobile devices enforce passwords or Personal Identification Number (PIN) with appropriate parameters.

- A password policy also covering PIN settings is established, aligned to current industry standards or industry best practices, and defines the following criteria:
  - Password expiration,
  - Password length, composition, complexity, and other restrictions,
  - Password reuse,
  - Lockout after failed authentication attempts, and remedy.
  - Password requirements may be modified as necessary for specific use cases:
    - In combination with a second factor (for example, one-time password),
    - Authentication target (for example, operating system, application, mobile device, token),
    - Type of account (general operator, privileged operator, application-to-application account or local authentication keys).

More good practice guidelines on password and PIN parameter settings can be found in SWIFT Knowledge Base TIP 5021567 and 5022038.

- The password policy is developed in consideration of known password-based vulnerabilities in the computing environment. For example, requiring a 15+ character password for Windows systems prevents Windows from computing the highly vulnerable LM (LAN Manager) password hash.
- The established password policy is enforced through technical means (for example, through Active Directory group policy, or within application settings) where possible.
- Effectiveness of the password policy is reviewed regularly (recommended annually).
- System settings related to password management and storage are aligned to industry and vendor best practices (for example, enabling the "NoLMHash" registry setting in Windows).
- Passwords used for secure zone systems are significantly more exposed if the passwords are stored in authentication systems outside of the secure zone (for example, an enterprise Active Directory). Instead, passwords for secure zone

systems are, to the fullest extent possible, stored only within the zone (for example, in an Active Directory for production systems) as described in the guidance for the design of the secure zone or another existing secure zone that has similar controls.

j) Multi-factor Authentication

Vendor to assess that Multi-factor authentication is used for interactive user access to SWIFT-related applications and operating system accounts.

- The following principles apply:
  - When based on a knowledge factor (typically a password) combined with a possession factor (a mobile device), the device used for the second factor must not be the same as the device used to enter the first factor. As such, using an app to generate the second factor on the same device/PC used to enter the first factor (password) is not deemed sufficient to access the local SWIFT systems.
- Second factor solutions based on a possession factor include (not exhaustive list): TOTP, RSA SecurID, Digipass, Mobile App, Transaction Authentication Number (TAN) Table, personal USB token. Solution to be selected as per user's own risk management.
  - An inherence factor is more safely combined with a possession factor than with a knowledge factor.
- Multi-factor authentication is implemented at least on one authentication stage/step faced by the system administrator or the end user when accessing a SWIFT application or its hosting system:
  - For operating system administrators when accessing the hosting system:
    - At the secure zone boundary (jump server),
    - At the dedicated operator PC log-in (within the secure zone).
  - For end users in descending order of security robustness when accessing the SWIFT application:
    - On the individual SWIFT applications (on the browser-based GUI, on the messaging interface, or on the communication interface),
    - At the secure zone boundary (jump server)
- Multi-factor authentication is implemented for remote user administrative access, generally for VPN authentication.
- Multi-factor authentication systems are significantly more exposed if the authentication credentials are stored outside of the secure zone (for example, within an enterprise Active Directory). If feasible, the authentication system supporting the multi-factor solution is located within the secure zone.

- The authentication factors presented are individually assigned and support individual accountability of access to services, operating system, and applications.
- If single sign-on (for example, SAML) is implemented, then a second factor is still required at the single sign-on, or at a later stage.
- MFA is also to be presented when accessing, at least for transaction processing36, a SWIFT related service, application or component operated by a service provider (such as a service bureau, an L2BA provider or intermediate actor).

k) Logical Access Control

Vendor to assess that accounts are defined according to the security principles of need-to-know access, least privilege, and segregation of duties.

A logical access control policy is documented and enforced to consider the following principles:

- Need-to-know.
  - Only operators (end users and administrators) who have a continuing requirement to access the secure zone are permitted to have accounts within the secure zone.
  - Privileges are only assigned to an operator with a validated need-to-know (for example, system setup ensures that operators only have access to the information, files, and system resources necessary for their defined tasks). Access to other system functions is disabled.
- Least Privilege.
  - The system setup ensures that user and administrator privileges are controlled in a way that allows all privileges to be tailored to individual needs.
  - Accounts are granted only the privileges that are required for normal, routine operation. Additional privileges are only granted on a temporary basis.
- Segregation of Duties and 4-Eyes.
  - Vendor documented guidance on role separation is followed in vendor-specific documentation.
  - Sensitive duties are separated. This means that some roles cannot be represented by the same individual, such as:
    - Transaction submission and transaction approval
    - Application Administrator and security officer roles
    - Network and operating system administrators.
  - Sensitive permissions are separated to prevent by-passing of the 4-Eyes principle. At a minimum, this requirement applies to access control and

security configuration operations on the following components: Messaging and Communication Interface, HSMs, SWIFTNet Online Operations Manager, and Secure Channel.

- Account Review and Revocation
  - Privileges are promptly revoked when an employee changes roles or leaves the organisation.
  - Accounts are reviewed at least annually (ideally more frequently) and adjusted as required to enforce access security principles.
- An emergency procedure to access privileged accounts is documented for use when authorised persons are unavailable due to unexpected circumstances:
  - Any operational use of the procedure is logged.
  - Access to the emergency privileged accounts is controlled. The usage is logged and the password is changed after emergency use.

l) Token Management

Vendor to confirm and report that this is not applicable

m) Physical and Logical Password Storage

Vendor to assess that recorded passwords are stored in a protected physical or logical location, with access restricted on a need-to-know basis.

- Passwords written on physical media are protected via:
  - Placement inside a sealed, tamper-evident security envelope,
  - Storage in a safe,
  - Logging of access to the storage location and which account's password was accessed.
- Passwords stored logically (digitally) are protected via:
  - Encryption-at-rest or obfuscation (that is, no plain-text storage),
  - Authenticated access to the storage location, ideally with logging of access.
- Passwords are not recorded in user manuals or other operational material unless the password is stored in accordance with the guidance above.
- If emergency access is granted to an operator who under normal conditions would not have access, the password is changed immediately thereafter, and optionally also the combination to the storage safe.
- Passwords are not hardcoded in scripts or other software code.

n) Malware Protection

Vendor to assess that Malware is a general term that includes many types of intrusive and unwanted software, including viruses. Anti-malware technology (a broader term for anti-virus) is effective in protecting against malicious code that has a known digital or behaviour profile.

- On-access anti-malware scanning (also known as real-time or background scanning) is performed on all in-scope systems. On-demand full scanning is scheduled at least on a weekly basis for operator PCs (ideally on a daily basis). On-demand full scanning should be scheduled regularly for servers in line with business and operational constraints. For performance reasons, full scans are performed at times of low usage and/or outside of business hours.
- The scope of the scanning should include all files of the systems in scope. Exclusion of elements or directory from scanning is subject to risk assessment considering user's infrastructure setup, internal security requirements and policies, the product capabilities and the following principles:
  - Software (such as exe, libraries, scripts) and static data (such as configuration files) are expected to be scanned on-access or at installation, and regularly thereafter, when complemented with a run time integrity mechanism (in line with the software integrity check depicted in control 6.2) allowing the identification of file changes or unexpected additions.
  - Database server content (data files) can be excluded from the scanning when the data has been checked, validated and scanned at least once before being stored.
- Anti-malware software from a reputable vendor is installed on all computing platforms and updated in line with the scanning frequency.
- Systems that fail to update their profiles or run scheduled scans are detected and corrected.
- Anti-malware software is tested for compatibility with the operational environment.
- Anti-malware software is configured in prevent mode if possible, after assessing for operational impact. It is recommended to configure the anti-malware software to quarantine suspicious files and raising an alarm to user's security department instead of immediately deleting them. This allows the user's security department to investigate the alert and possibly prevent future 'false positives' while allowing the recovery of files in case it is confirmed they are legitimate.
- Files to be sent should be scanned at least once at any stage/step of their internal processing and ideally as close as possible to their transfer into the

SWIFT network. This is to ensure that such files do not contain viruses or malware that may create risks for the sender, for SWIFT, or for the receiver.

- Endpoint Protection Platform (EPP) solution combined or not with Endpoint Detection and Response (EDR) offering similar control on the infrastructure can be considered as a valid implementation.

o) Logging and Monitoring

Vendor to assess that Capabilities to detect anomalous activity are implemented, and a process or tool is in place to frequently store and review logs.

- Overall goals for logging and monitoring:
  - Implement a plan for logging of security-relevant activities and configure alarms for suspicious security events (when supported by the application).
  - Implement a plan for monitoring of security events in logs and for monitoring of other data (for example, real-time business activities through the GUI), and establish a plan to treat reported alarms.
- All logging and monitoring activity complies with applicable laws and regulations, and employment contracts which supersede any implementation guidance.
- Logging:
  - Logging capabilities are implemented to detect abnormal usage within the secure zone as well as any attempts to undermine the effectiveness of controls within the secure zone.
  - Logs provide traceability of account usage to the appropriate individual.
  - Messaging and communication interface application audit logs are retained for no less than 12 months and are sufficiently protected from an enterprise administrator-level compromise (for example, log files are transferred to a separate system with different system administrator credentials).
  - Operator PC, firewall and database audit logs are retained for no less than 31 days.
  - Minimum logs to be recorded include:
    - Command line history for privileged operating system accounts on servers,
    - Messaging and communication interface application and operating system logs which detail abnormal system behaviour (for example, activity outside normal business hours, multiple failed log-in attempts, authentication errors, changes to user groups),
    - Firewall logs,
    - Database logs (if available, and as a minimum in the case of hosted database solutions).

- Monitoring:
  - Procedures are in place to identify suspicious log-in activities into any privileged operating system or application accounts within the secure zone.
  - Monitoring processes are in place to review server, application and database monitoring data of the secure zone either daily via human reviews or via automated monitoring with alerting.
  - Monitoring processes are in place to review network monitoring data on a regular basis.
  - Unusual or suspicious activity is reported for further investigation to the appropriate security team.

p) Cyber Incident Response Planning

Vendor to assess that the user has a defined and tested cyber incident response plan.

- The user has developed and annually updates a cyber incident response plan. A formal backup and recovery plan exists for all critical business lines to support incident response activities.
  - The cyber incident response plan includes up-to-date contact details (internal and external when using third parties or service providers) and escalation timers. Such a plan has to incorporate:
    - The Cyber Security Incident - Recovery roadmap that provides a non-exhaustive list of steps or actions that a customer must follow in case of a cyber security breach and refer to SWIFT Support. Details are outlined in SWIFT-ISAC Bulletin #10047.
    - Internal security policies, laws, and regulations within a user's jurisdiction must be adhered to and considered in the cyber incident response planning.
- As a minimum, the plan is reviewed on an annual basis, and tested at least every two years ensuring safe recovery of critical business operations with minimised outage time after a cybersecurity incident.
- The cyber incident response plan includes steps to:
  - Promptly notify the appropriate internal stakeholders and leadership,
  - Promptly notify the relevant external organisational stakeholders (typically, regulator(s), supervisor(s), law enforcement authorities),
  - Promptly notify the SWIFT Customer Support Centre through the default channel and to comply with other obligations applicable to users in case of a security incident including the obligation to cooperate and provide forensic materials as may be required by SWIFT,
  - Promptly contain or isolate the impacted system to limit the exposure of the attack whilst still be able to identify rogue activities,

  - Involve skilled cybersecurity professionals to identify and address the cyber incident. It is the user's responsibility to take prompt corrective action to investigate, clean the full infrastructure and resume secure operations as soon as possible,
  - Review the correctness of the user current attestation(s) and, as applicable under the SWIFT Security Controls Policy, invalidate such attestation(s) and submit new attestation(s),
  - Conduct post-incident problem analysis to identify and remediate vulnerabilities,
  - Fully document the incident.
- The user has a documented plan for the timely sharing of threat information to intelligence-sharing organisations, law enforcement/local regulators (as required in each users' jurisdiction) and to SWIFT. Sharing of threat information may potentially support root cause analysis and sharing of anonymised Indicators of Compromises (IOC) with the community.
- Information to be shared is first evaluated to ensure compliance with applicable laws and regulations (for example, privacy of personal data, confidentiality of investigations) and protects against the unintended sharing of sensitive data or data beyond the relevance of the incident.
- The user has the capability to consume threat intelligence shared by SWIFT, for example in the form of IOCs. The user has procedures in place to:
  - Ensure the information is distributed to the correct contacts within the organisation,
  - Block traffic to/from IP-addresses/URLs mentioned in the IOCs.

q) Security Training and Awareness

Vendor to assess that annual security awareness sessions are conducted for all staff members including role-specific training for SWIFT roles with privileged access.

- Staff complete annual security awareness and training. Topics may include:
  - SWIFT-related products and services training (for example, via SWIFTSmart which is available to all users),
  - Cybersecurity threat awareness within the financial services industry or relevant to staff's role and responsibilities,
  - Risks related to internet usage or deployment in the cloud
  - Password security and management,
  - Device security,
  - Safe operating habits (for example, spam and phishing, including "spear39" phishing identification, downloading files, browsing practices),
  - Reporting of suspicious events and activities,
  - Detection and response to cyber incidents in line with the organisation's response plan,
  - Internal or external programme that optionally allows staff to obtain and maintain certifications.

- Training is delivered through the most appropriate channel, including computer-based training, classroom training, webinars.
- Persons who have access to SWIFT applications, data, certificates, network, etc. have an adequate knowledge level and are aware of the pertinent cyber risks (for example, through IOCs published by SWIFT), best practice behaviours, and processes.

DOCUMENT ACKNOWLEDGEMENT

By signing this document, the people listed record their agreement on the contents of this document.

	Name:	Tshilidzi Catlyn
Information System Support Manager	**Signature:**	Catlyn
	Date:	10 February 2022
	Name:	Mugeshen Covenden
Solution Support Manager	**Signature:**	
	Date:	10/02/2022
	Name:	Rebecca Shabalala
Senior Advisor Info Systems	**Signature:**	
	Date:	2022/02/10