A8 - ACCEPTABLE USE POLICY V1.5

DOCUMENT CLASSIFICATION	Internal Use Only
VERSION	1.5
DATED	01 September 2024
DOCUMENT AUTHOR	Ameet Ranchod
DOCUMENT OWNER	Johan Kriel

Approval

NAME	POSISTION	SIGNATURE	DATE
Donald Fraser	IT Security & Compliance Manager		05.09.2024
Ameet Ranchod	IT Infrastructure Manager		30/09/2024
Johan Kriel	Group CIO		24/10/2024

This policy supersedes and replaces all previous versions of this policy.

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	10.11.2020	Ameet Ranchod	Document Creation
0.9	19.02.2021	Ameet Ranchod	Final Draft
1.0	23.02.2021	Ameet Ranchod	Version 1.0
1.1	28.05.2021	Ameet Ranchod	Updated to conform to POPIA
1.2	21.07.2021	Ameet Ranchod	Updated security
1.3	31.05.2022	Celeste Ramnarayan	Version 1.3 updated to cover cloud storage
1.4	01.07.2023	Donald Fraser	Updated personnel & roles, saving sensitive data
1.5	01.08.2024	Donald Fraser	2024 Revision, new template, added AI

Table of Contents

1 Policy Scope

This policy applies to all employees and contractors during the performance of company related business and duties. This policy covers all digital assets including, but not limited to: PCs, laptops, mobile phones, tablets, networks (including wireless), voice mail, email, Internet, and computer systems and files.

2 Policy Statement

The use and management of information technology is a vital component of our day-to-day operations. In addition to potential illegal activity, disclosure of our organisations' sensitive or personal information and the introduction of malware, misuse of these systems has a real cost in terms of lost productivity.

As such steps need to be taken to ensure that all users of information technology in the Digicall Group are aware of the rules pertaining to the use of electronic equipment in the Digicall environment. When using the Digicall Group's digital services, equipment, facilities, or networks, you must comply with all applicable laws, our policies, rules, and limits, including this Acceptable Use Policy (AUP).

Employees must remain aware that all our digital services, equipment, facilities, and networks are monitored for security and performance purposes and that monitoring data may be used to support any related enquiries or investigations.

All employees will be expected to read this AUP online and, by completing this task, signify their understanding and acceptance of this policy. If you do not agree to be bound by the terms of this Policy, then you must raise it with your line manager or HR.

3 Purpose

An acceptable use policy is a document stipulating constraints and practices that a user, contractor or customer must agree to for access to a set of computing resources, which could be a computer, a mobile device, a computer network, website, internet, large computer system or service. It restricts the ways in which the user may use these devices and services and sets guidelines as to how they must be used.

4 General

User responsibilities concerning electronic information resources.

4.1 General User Responsibilities

4.1.1 Access to information resources is granted with the expectation that resources shall be used in an ethical and lawful manner. It is each user's responsibility and obligation to ensure that all electronic information resources as well as company and client data are only used for its intended business purpose.

4.1.2 Authorized electronic information devices will be allocated, configured, and issued to users by the relevant regional IT Department.

4.1.3 Users that are leaving one department for another or leaving the company must consult the relevant regional IT Department to ensure that proper backups are in place for the information residing on their workstations before reallocation.

4.1.4 E-mail accounts, and the e-mail messages contained within these accounts, are important to the business functions of Digicall. As such, the messages and e-mail accounts are the property of Digicall Group and will be managed by the IT Department. In the event of any employee termination, the employee's e-mail account will remain with Digicall. All messages may be reviewed and redirected to the employee's successor or otherwise deleted, as may be deemed appropriate by the Digicall Group and guided by relevant legislation.

4.1.5 Users must ensure that their out-of-office reply is activated when they are away for a day or more.

4.1.6 The creation of business e-mail is equivalent to the creation of any other company document. Therefore, users must use the same degree of care and seriousness associated with the drafting of company documents when composing business e-mail messages.

4.1.7 E-mail must be retained for periods that would normally apply to written or facsimiled transactions; retention must be guided by relevant legislation or applicable client contracts.

4.1.8 All information developed by or for Digicall remains the property of Digicall.

4.1.9 Any third parties (such as vendors or service providers who provide goods and services to Digicall Group), and who provide server and computing technology along with such associated goods and services at Digicall Group premises must first consult the relevant regional Digicall IT Department before operating at any Digicall Group site.

4.1.10 Any changes to hardware and software in the Digicall IT production environment will be subject to the change control process that governs this action. No changes to software, hardware, databases, or any functionality that operates in the production

environment will be allowed until the change control process has been followed and the change has been approved. Please refer to the Change Management Policy for further details.

4.2 Usage

4.2.1 All users must use electronic information resources in a manner that does not in any way interfere with, compromise, or harm the performance, functionality, or integrity of Digicall's electronic information resources. This must include the adherence to company standards regarding software updates and protections, data handling, and other policies and procedures enacted by the company.

4.2.2 Users must respect network capacity as a shared resource and therefore may not perform operations that degrade network performance for other users.

4.2.3 Users must utilise corporate communication services for business purposes only, or for limited personal use that does not infringe on the rights or productivity of other users.

4.2.4 Users may not send inappropriate messages to groups or individuals. Only official company-specific information may be sent to all users, this may only be done by authorized personnel.

4.2.5 The downloading and printing of content is only permitted for business purposes.

4.2.6 Issued electronic information devices may not be used for personal purposes unless prior approval has been obtained from the relevant regional IT Manager.

4.2.7 No user, apart from duly authorised IT personnel, is allowed to install or remove any software on company issued devices. Users must request the installation or removal of software packages through logging a call with the IT Helpdesk.

4.2.8 No user, apart from duly authorised IT personnel, is allowed to change operating system configurations on company issued devices.

4.2.9 No user, apart from duly authorised IT personnel, is allowed to upgrade or downgrade existing operating systems or install new operating systems on company issued devices.

4.2.10 No user, apart from duly authorised IT personnel, is allowed to alter or add company issued devices in any way, including (but not limited to) upgrading processors, memory, or any other peripheral hardware.

4.2.11 No user, apart from duly authorised IT personnel, is allowed to access the workstations of other employees using remote access and/or administrator

capability/functionality including (but not limited to) administrator accounts, Remote Desktop, VNC, TeamViewer, or any other remote desktop solutions, file shares, etc.

4.2.12 The creation, transmission, receipt, or storage, of certain content may be in violation of regulatory and statutory requirements and are therefore prohibited within the Digicall Group. This content includes, but is not limited to the following:

- Threats.
- Pornographic or sexually explicit material.
- Material containing derogatory racial, gender, religious or hate-oriented comments.
- Libellous remarks about products or other companies.
- Defamatory remarks, including defamation of character.
- Discriminatory language or remarks that would constitute harassment of any type.
- Any other comment that offensively addresses someone's age, sexual orientation, political beliefs, national origin, or disability.

4.2.13 Users are strictly prohibited from uploading any company and/or client confidential or proprietary information to AI programs & sites, including but not limited to:

- Large language models such as ChatGPT, Google Gemini, Microsoft Copilot or similar.
- Deep learning models, text-to-image models such as Stable Diffusion, Dall-E, Midjourney or similar.
- Any other AI-driven platforms.

4.2.14 The direct use of AI to generate, modify, or complete documentation within the organization is not allowed unless the application has been reviewed and the use thereof has explicitly been authorized by senior management.

This policy aims to protect sensitive information, ensure the integrity and originality of Digicall documentation, comply with data privacy regulations, and protect our intellectual property.

4.3 Email Usage

4.3.1 Email is an important organisational communication tool made available by our organisation to employees to use as appropriate in performing their duties. Reasonable personal use is permitted provided it is with a sense of responsibility and fairness to our employees' job requirements. Keep in mind that emails serve as legal documents and hold the same weight as more formal communications like letters,

notices, or agreements. Emails must be drafted with care, having regard to the following:

- The content must not be objectionable.
- The message must be clear.
- Check the intended vs. the actual recipients.
- Check for personal, sensitive, confidential, or proprietary information.
- Confirm whether the email must be encrypted.

4.3.2 Corporate email accounts are intended solely for official business purposes and should not be used for subscribing to personal newsletters, websites, or any non-work-related communications. Utilizing corporate email for such activities can lead to increased risk of spam, security breaches, and potential misuse of company resources.

4.4 Social Media Usage

4.4.1 The use of social media is pervasive in both our organisational and social lives - and often there is a blurring between the two. With regards personal information there is the need to guard one's own privacy as well as the privacy of our organisation's data subjects.

4.4.2 Personal or anonymous social networking can impact our organisation's brand and reputation. In your personal capacity, never discuss or share our organisation's information on social media sites, including blogs, forums, wikis, micro-blogging sites, Facebook, or Twitter, unless you are specifically authorised to do so. Remember, any social media post from our organisation's computers may be traced back to its IP address.

4.4.3 Employees must ensure that they:

- Do not disclose information classified as Internal, Confidential or Client Confidential.
- Never offer opinions on behalf of our organisation without the prior approval of our organisation.
- Do not violate copyright, privacy, and intellectual property rights.
- Never cause offence or harass anyone.
- Do not breach anyone’s right to privacy or confidentiality.
- Never use our organisation's email address as an identifier.
- Always treat all social networking sites and activities as if they were publicly accessible.
- Always ensure that consent is received prior to adding external parties to social media groups (WhatsApp, Telegram, etc.)

4.4.4 Always be considerate of others privacy including that of the client, posting pictures taken at the workplace is strictly prohibited. Always be respectful of our company as well as its employees and clients when using social media, in so doing we must be mindful and ensure consent has been given before posting any pictures of people especially in the case of minors.

4.5 Data & Information

4.5.1 Users are strictly prohibited from accessing any information or data for which they have not been explicitly authorized. Any attempt to view, use, or disclose data without proper authorization is a violation of this policy.

4.5.2 Users may not use electronic information resources for commercial purposes, for personal financial gain, or to solicit support for outside organizations not otherwise authorized to use Digicall facilities.

4.5.3 No users are allowed to access the data of other users, without the express permission of such users or senior management. The exception to this rule applies where departments share information through common folders assigned by the IT Department that have shared usage rights. User data and information may be reviewed as part of monitoring and compliance activities undertaken by Digicall.

4.5.4 Users must not store any information locally; information must be stored in the locations and systems provided. Information stored on local machines will not be backed up by Digicall.

4.5.5 No personal, audio or video content would be allowed to be backed-up to the Digicall Group servers.

4.6 Sensitive Information

4.6.1 Users must not download or save sensitive information such as financial records, privileged company documents or intellectual property, or any other information that could be deemed as confidential or restricted, to any device that is not under the control of, or authorised by, the IT Department.

4.6.2 Additionally, no sensitive information is to be stored on any personal cloud storage system, such as, but not limited to, Google Drive or Drop Box, that is not under the control of, or authorised by, the IT Department.

4.6.3 Should sensitive information be saved to a user's hard drive or desktop for the purpose of completing a task outside of the primary storage location, such as printing a document or compiling a report, the document(s) must be deleted as soon as the task has been completed.

4.6.4 Databases containing sensitive or production data may not be installed on users' hard drives or desktops.

4.7 Security

4.7.1 Individuals must not give out, loan, share, or otherwise allow anyone else to use the access privileges granted to them. Access to secured information resources is provided only with proper authorization.

4.7.2 Users may not attempt to circumvent login procedures on any computer system or otherwise attempt to gain unauthorized access. This is not an acceptable use of information resources and may be a crime under local or international law.

4.7.3 No unauthorized or personal devices may be used to connect to the Digicall Group environment in any way without prior written approval from the relevant regional IT Manager responsible for that environment.

4.7.4 All users and departments have the responsibility to report any discovered unauthorized access attempts, unauthorized devices, or any other improper usage of Digicall Group information resources. If you observe, or have reported to you, a security or abuse problem with any Digicall Group information resource, including violations of this policy, notify the relevant regional IT Manager immediately.

Contact details are as follows:

- Email itsc@digicallgroup.co.za

4.7.5 Users who discover potential security vulnerabilities must not attempt to prove a suspected weakness, as testing weaknesses might be interpreted as a potential misuse of the system.

4.7.6 Users are not permitted to bring unauthorised devices and equipment into the Digicall Group network. Such devices must be disabled and removed immediately upon detection and disciplinary action must be taken.

4.7.7 Users must lock their workstation(s) and log out of any active applications when leaving their computers unattended.

4.7.8 Users must ensure that they have logged out of all systems, including the network, and power down workstations after hours.

4.7.9 Users must ensure that their laptops are appropriately physically secured.

4.8 Credentials

4.8.1 Users must create passwords that are a minimum of twelve (12) characters in length and comprise of upper and lowercase letters, numbers, and special characters.

4.8.2 Personal details such as spouse's name, license plate, ID number, and birthday must not be used.

4.8.3 Words in a dictionary, derivatives of user-IDs and common character sequences such as “123456” must not be employed.

4.8.4 Passwords must not be based upon month/year combinations such as “jan06” or “april2006”.

4.8.5 Users must not use cyclical passwords. For example, users must not add a numeric at the end of the password in sequence.

4.8.6 Passwords must not consist of identical all numeric or all alphabetic characters, for example “1111111” or “aaaaaaa”.

4.8.7 An ideal password is created from a pass phrase. For example, the phrase “security is vital to this company and me” might result in the password of “siv2tcam!” by using the first letter of each word in the phrase, substituting the number 2 for “to” and adding the exclamation mark.

4.8.8 Passwords must not be written down, e.g., diaries, post it stickers, desk calendars, etc.

4.8.9 Users must maintain exclusive control of their personal passwords, and they may not be shared with others.

4.8.10 Users must manually enter their password every time they log on and not choose the ”save password” option.

4.8.11 Users are responsible for all activity attributable to and/or recorded as originating from their authenticated user ID. Users must immediately report suspicious activity and/or suspected misuse of their user ID and password to the relevant regional IT Department.

4.8.12 To further safeguard user accounts from unauthorized access the relevant regional IT Department must ensure that user accounts must be locked-out after five (5) invalid login attempts.

4.9 Anti-virus

4.9.1 Externally supplied flash disks, CD-ROMs, and other removable storage media must not be used unless they have first been checked by internal IT staff for viruses.

4.9.2 Because viruses can be complex and sophisticated, users must not attempt to eradicate them without expert assistance. If users suspect infection by a virus, they must immediately stop using the involved computer, disconnect from all networks, and contact their relevant local IT Helpdesk.

4.9.3 Users must not open e-mail attachments or click on links from unknown sources.

4.9.4 Executable attachments (i.e. .exe, .com, .bat etc.) must not be launched and must be deleted immediately.

4.9.5 All e-mail attachments received from known sources must be scanned for viruses.

4.9.6 Users must not intentionally introduce any malicious computer code onto Digicall systems, such as viruses, worms, or malware.

4.10 Destruction of Information

Compliance with the Disposal of Media guidelines are required. Please refer to A8 - Asset Management Policy for guidance.

4.11 Intellectual Property Rights (Copyright Protection)

Digicall strongly supports strict adherence to software vendor's license agreements and copyright holder's notices. Users must therefore strictly adhere to the following conditions:

4.11.1 Making unauthorized copies of licensed and copyrighted software, even if only for "evaluation" purposes, is strictly forbidden.

4.11.2 Digicall allows reproduction of copyrighted materials only to the extent legally considered "fair use" or with the permission of the author/owner.

4.11.3 If users have any questions about the relevance of copyright laws, they must contact their relevant regional Digicall IT Department.

4.11.4 Users must assume that all software and other materials are copyrighted unless they have received information to the contrary.

4.12 Unauthorized Physical Access

4.12.1 Printers and copiers must not be left unattended when confidential data is being printed or copied.

4.12.2 Users must note that financial and other critical documents must be accepted as valid and accurate if they are maintained and controlled by the process owner/originator within the controlled and protective directories.

4.12.3 To ensure the integrity of critical documents relied upon for decision making which are emailed to various recipients, copied onto storage devices, or shared via file shares, the process owner must ensure that these documents are:

- Password-protected.
- Saved as read-only.
- Encrypted.
- Saved as an Adobe (PDF) document.
- The recipient(s) must not be able to make any changes to the document and must only be able to view the document contents.
- Document passwords must not be mailed with documents but rather sent via SMS/WhatsApp/Teams to the correct recipients.

4.12.4 If it is required that the document needs to be emailed without the document being password protected as read-only or saved as an Adobe (PDF), then the process owner needs to issue it with a notice/alert to the effect of:

"This document is issued as an uncontrolled copy. You are using the attached document for your own analytical purposes. Any changes made to the document by you are not valid. No reliance may be placed on the changed document for business decision, unless the new document fully complies to the protocols as contained in the Digicall Group User Acceptance Policy."

4.12.5 Documents, for the purposes of Digicall Group business are proprietary in nature. As such, the necessary password controls are required to be in place to safeguard any information deemed to be confidential as related to Digicall Group business. All Documents that are used to compile monthly data for financial reporting and strategic decision-making purposes must adhere to change control and access control processes as specified in the relevant procedures adhered to within Digicall IT for the specific purposes of such control.

4.13 Cloud Storage

4.13.1 If employed in a work context, cloud services also introduce risks to the security, privacy, copyright, and retention of Digicall & Client data. Before using cloud storage for work, Digicall employees must consider if the usage is appropriate and follow the policy guidance in this document to limit the risk imposed on Digicall & Client data. The main risks when files are stored in public cloud storage are that:

- Digicall can no longer guarantee the quality of access controls protecting the data.
- The location where the data is stored may not be guaranteed and therefore protection of its sovereignty is questionable and so may not meet the various Data Protection Act's we are required to comply with for the protection of personal data, etc.
- In many cases, public cloud storage requires that files be associated with an individual's personal account. Should that individual be absent for whatever reason, Digicall may lose access to the data.
- Cloud services limit their liability for negligence, resulting in little or no recourse should the provider misuse, lose or damage information stored in the cloud.
- Few cloud providers guarantee they must not access the information stored within their service, leading to concerns over privacy and intellectual property rights.
- Some if not all providers do not guarantee that the user's ownership of the data stored in the cloud must be retained. This is primarily to enable the providers to move data around to their different server locations without your prior approval but opens further questions about intellectual property rights.
- Using cloud storage client software to synchronise files between work and personal devices could result in sensitive information being held inappropriately on personal equipment.
- If they have financial difficulties a cloud storage provider may end the service with little or no notice, leaving users with no access to files.

4.13.2 Digicall has provided all employees with access to Microsoft Office 365. As part of this, employees have access to an individual Microsoft OneDrive for Business and Group OneDrive for Business via Microsoft Teams using accounts based on their Digicall login ID. Microsoft will store data uploaded by employee accounts in agreed locations to protect sovereignty. Using OneDrive for Business via a staff login ID is therefore the only approved Cloud Storage solution for use by Digicall employees.

There may be some situations when access to other services and providers may be needed - for example when collaborating with clients or suppliers who make use of a different service, such as Apple iCloud, Box.com, Dropbox or Google Drive. Access to

these services will be considered on a case-by-case basis and restricted to the individuals involved with the client or supplier for the duration of the requirement, after which access will be revoked.

4.14 Enforcement

4.14.1 Users must employ electronic information resources consistent with the requirements of local regional law and Digicall Group policies.

4.14.2 Users are responsible for using resources appropriately to maintain the integrity of the electronic information resources, and where appropriate, the privacy, confidentiality, and/or security of the electronic information.

4.14.3 Users are responsible for all activities that occur while using information resources assigned to them.

4.14.4 Users will be held responsible for all activity conducted under his/her user ID and password.

4.14.5 Any Digicall Group business information or records in personal or private email accounts or electronic devices must be disclosed in the event of a request for public records as defined by local regional laws.

4.14.6 Incidental personal use of electronic information resources, including email, is permitted provided that this use does not interfere with Digicall operations, violate Digicall policies, create an inappropriate atmosphere for employees in violation of law or Digicall policy, generate incremental identifiable costs to the company, and/or negatively impact the user's job performance.

4.14.7 Representing oneself as someone else, without previous written authorization, is not considered responsible use of electronic information resources (impersonation).

4.14.8 Users are prohibited from impersonating another user or sending a message from another user's account.

4.14.9 Electronic resources may not be used to engage in any illegal, threatening, harassing, or bullying conduct, including cyber-harassment or cyber-bullying, nor may they be used in a deliberately destructive manner.

4.14.10 Users are expected to take precautions to ensure that company issued devices are not stolen, lost, or damaged. If devices are lost, stolen, or otherwise damaged such that they cannot be restored to normal working order, the employee may be responsible for the prorated cost of the laptop. In case of theft or loss, the user must

file a report with the relevant regional IT Manager. Users are encouraged to check their home insurance policies regarding coverage.

4.14.11 Company resources may not be used in external activities unless written approval has been received in advance from the Group Chief Executive Officer or their designee. Such permission must be granted only when the use of company resources is determined to further the mission of the company.

4.14.12 Users may be held liable for any losses suffered by Digicall Group due to user disregard of any policy or procedure as set out in the relevant Digicall Group policy or procedure document.

4.14.13 Users who are found to be responsible for causing damage or destruction to Digicall Group information resources including (but not limited to) infrastructure, data or intellectual property may be held liable for disciplinary or legal action.

5 Training and Awareness

Users are required to read and acknowledge understanding this policy by signature, during the onboarding process.

6 Responsibilities

Digicall Group electronic information resources are company owned and maintained, thus giving Digicall Group the responsibility to monitor, audit, and assure the proper use of those resources. Although the Digicall Group supports a climate of trust and respect and does not ordinarily read, monitor, or screen individual user's routine use of electronic information resources, it must monitor systems for misuse. The Digicall Group, therefore, cannot guarantee the confidentiality, privacy, or security of data, email, or other personal information transmitted or stored by employees or contractors on its electronic information systems.

When Digicall Group officials believe a user may be using electronic information resources in a way that may violate company policies or regional local law, or the user is engaged in activities inconsistent with the user's business responsibilities, then system administrators may monitor the activities and inspect and record the files of such users(s) on their computers and networks, including word processing equipment, personal computers, workstations, mainframes, minicomputers, and associated peripherals and software.

Reports of all apparent IT policy violations must be forwarded to the relevant regional IT Manager and the IT Infrastructure Manager for disposition according to standard procedures and company policies on violation of policy.

The necessary disciplinary procedures in terms of the relevant Digicall Group code pertaining to asset abuse must also be followed up through the relevant Human Resources and Industrial Relations channels.

Digicall is not responsible for material viewed or downloaded by users from the internet or other public communications networks. Users are cautioned that web pages may include offensive, sexually explicit, and/or other inappropriate material. Users accessing the internet and other public communications networks do so at their own risk.

The IT Security and Compliance Manager is responsible for maintaining this policy and providing support and advice during its implementation in line with the IT Risk Management Policy

All Managers are directly responsible for implementing the policy and ensuring staff compliance.

Compliance with this Information Security and all subsequent policies is mandatory.

7 Policy Compliance Monitoring

7.1 Compliance

Group IT must verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

If any user is found to have breached this policy, they may be subject to the Digicall Group's disciplinary procedures. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

7.2 Exceptions

Any exception to this policy must be approved by the Group Chief Information Officer in advance.

7.3 Non-compliance

All users (employees, contractors, vendors) are required to adhere to this Policy. Failure to comply may result in disciplinary action up to and including termination from employment, termination of contract, and civil penalties and/or criminal sanctions, depending on the circumstances.

7.4 Remediation of Non-compliance

Where non-compliance has been identified, dependent on the severity and criticality and impact, opportunities may be provided to correct identified non-compliance. This corrective action will be evaluated on a case-by-case basis and timelines will be imposed and strictly enforced to ensure timeous remediation.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Human Resources Department or the IT Security and Compliance Officer.

8 Policy Governance

The following table identifies who within the Digicall Group is **Accountable, Responsible, Informed** or **Consulted** with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	IT Security and Compliance Manager
Accountable	Group Chief Information Officer
Consulted	IT Infrastructure Manager, Regional IT Infrastructure Managers
Informed	All Employees, All Temporary Staff, All Contractors, All Vendors and All Suppliers

9 Audit and Review Process

This policy and compliance there to, will be audited and reviewed internally at least once every 12 months depending on the changes or requirements within the group which will be reviewed by Management, or as required by significant changes in business operations or regulatory requirements.

For Group companies' pursuing certification, policies are required to be audited externally at least once in a 36-month cycle or sooner depending on changes or requirements within the group. Any employees or contractors with suggestions should refer these to their line manager in the first instance so they can be considered for implementation. Whenever changes are made to this policy the final draft will be shared with the Group CIO, IT

Infrastructure Manager and the IT Security & Compliance Manager for review and approval before publication.

The IT Security and Compliance Manager will undertake annual policy reviews.

10 Appendices

None included with this policy.