DIGICALL

A10 - DATA ENCRYPTION POLICY V1.3

DOCUMENT CLASSIFICATION	Internal Use Only
VERSION	1.3
DATED	01 September 2024
DOCUMENT AUTHOR	Ameet Ranchod
DOCUMENT OWNER	Johan Kriel

Approval

NAME	POSISTION	SIGNATURE	DATE
Donald Fraser	IT Security & Compliance Manager		03/10/2024
Ameet Ranchod	IT Infrastructure Manager		04/10/2024
Johan Kriel	Group CIO		09/10/2024

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

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	17.02.2021	Ameet Ranchod	Document Creation
0.9	22.02.2021	Ameet Ranchod	Final Draft
1.0	02.03.2021	Ameet Ranchod	Version 1.0
1.1	31.10.2022	Celeste Ramnarayan	Version 1.1
1.2	01.07.2023	Donald Fraser	Updated personnel & roles
1.3	01.09.2024	Donald Fraser	2024 Revision, template change, added Key Exposure.

Table of Contents

1 Policy Scope

This policy applies to all Digicall Group staff that create, deploy, transmit, or support application and system software containing confidential information. It addresses encryption policy and controls for confidential information that is at rest (including portable devices and removable media), data in motion (transmission security), and encryption key standards and management.

2 Policy Statement

Digicall Group confidential information and employee, client, contractor personally identifiable information must be protected while stored at-rest and in-transit. Appropriate encryption technologies must be used to protect the Digicall Group. This document refers to confidential information, and in context of this policy the term “confidential information” will refer to both confidential information as well as personally identifiable information interchangeably.

3 Purpose

The purpose of this policy is to provide guidance on the use of encryption technologies to protect Digicall Group data, information resources, and other confidential information while stored at rest or transmitted between parties. This policy also provides direction to ensure that regulations are followed.

4 General

The Digicall IT Infrastructure Manager or their designee shall ensure:

1. Policies, procedures, scenarios, and processes must identify confidential information that must be encrypted to protect against persons or programs that have not been granted access.
2. The Digicall Group implements appropriate mechanisms to encrypt and decrypt confidential information whenever deemed appropriate. Internal processes and procedures shall specify how Digicall Group transmits sensitive information as well as how often the information is transmitted.
3. When encryption is needed based on data classification to protect confidential information during the transmission then procedures shall specify the methods of encryption used to protect the transmission of confidential information.
4. Logical user access is managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials) when disk encryption is used rather than file or column-level database encryption.

4.1 Encryption Key Length

1. Digicall Group uses software encryption technology to protect confidential information. To provide the highest level of security while balancing throughput and response times, encryption key lengths should use current industry-standard encryption algorithms for confidential information. As such, where RSA keys are used, the length should not be less than 2048 bits. Where elliptic curve cryptography (ECC) keys are used, key length should be a minimum of 256 bits. Elliptic curve cryptography shall be used in preference over RSA keys where possible.
2. The use of proprietary encryption algorithms is not allowed unless reviewed by qualified experts outside of the vendor in question and approved by Digicall Group management.

4.2 At-Rest Encryption

1. Hard drives that are not fully encrypted (e.g., disks that has one or more un-encrypted partitions, virtual disks, etc.) but connect to encrypted USB devices, may be vulnerable to a security breach from the encrypted region to the unencrypted region. Full disk encryption avoids this problem and shall be the method of choice for user devices containing confidential information. Currently, the Digicall Group employs BitLocker to protect these drives at risk.
2. Confidential information at rest on computer systems owned by and located within Digicall Group controlled spaces, devices, and networks should be protected by one or more of the following mechanisms:
    a. Disk/File System Encryption (e.g., Microsoft EFS technology)
    b. Use of Virtual Private Networks (VPN's) and Firewalls with strict access controls that authenticate the identity of those individuals accessing the confidential information.
    c. Sanitizing, redacting, and/or de-identifying the data requiring protection during storage to prevent unauthorized risk and exposure (e.g., masking or blurring confidential information).
    d. Supplemental compensating or complementary security controls including complex passwords, and physical isolation/access to the data.
    e. Strong cryptography on authentication credentials (i.e., passwords/phrases) shall be made unreadable during transmission and storage on all information systems.
    f. Password protection to be used in combination with all controls including encryption.
    g. File systems, disks, and tape drives in servers and Storage Area Network (SAN) environments are encrypted using industry-standard encryption technology.

h. Computer hard drives and other storage media that have been encrypted shall be sanitized to prevent unauthorized exposure upon return for redistribution or disposal.

3. Portable Device Encryption:
    a. Portable devices (e.g., smart-phones, flash drives, SD cards, USB storage) represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of confidential information are the result of stolen or lost portable computing or storage devices. The most reliable way to prevent exposure is to avoid storing confidential information on these devices.
    b. As a general practice, confidential information shall not be copied to or stored on a portable computing or storage device. However, in situations requiring confidential information to be stored on such devices, encryption reduces the risk of unauthorized disclosure if the device becomes lost or stolen. The following procedures shall be implemented when using portable storage:
        i. Hard drives (laptops, tablets, smartphones and personal digital assistants (PDAs)) shall be encrypted using products and/or methods approved by the Digicall IT Infrastructure Manager. Unless otherwise approved by management, such devices shall have full disk encryption with pre-boot authentication.
        ii. Devices shall not be used for the long-term storage of any confidential information.
        iii. All devices shall have proper and appropriate protection mechanisms installed including approved anti-malware/virus software, personal firewalls with unneeded services and ports turned off, and properly configured applications.
        iv. Removable media including CD's, DVD's, USB flash drives, etc. shall not be used to store confidential information.

4.3 In-Transit Encryption

1. In-transit encryption refers to the transmission of data between endpoints. The intent of these policies is to ensure that confidential information transmitted between companies, across physical networks, or wirelessly is secured and encrypted in a fashion that protects Digicall Group confidential information.
2. The Digicall IT Infrastructure Manager or their designee shall ensure:
    a. Formal transfer policies, protocols, procedures, and controls are implemented to protect the transfer of information using all types of communication and transmission facilities.

b. Users follow Digicall Group acceptable use policies when transmitting data and take particular care when transmitting or re-transmitting confidential information received from non-Digicall Group staff.

c. Strong cryptography and security protocols (e.g., TLS, IPSEC, SSH, etc.) are used to safeguard confidential information during transmission over open public networks. Such controls include:
    i. Only accepting trusted keys and certificates, protocols in use only support secure versions or configurations, and encryption strength is appropriate for the encryption methodology in use. Any use of outdated or insecure protocols (such as SSL v3, TLS 1.0, TLS 1.1, or outdated ciphers such as RC4, DES, and 3DES) must be approved on a case-by-case basis by the IT Security and Compliance manager and documented before they can be implemented.
    ii. Public networks include but are not limited to the internet, wireless technologies, including 802.11 (Wi-Fi), Bluetooth, and cellular technologies.
    iii. Confidential Information transmitted in e-mail messages is encrypted. Any confidential information transmitted through a public network (e.g., internet) to and from vendors, customers, or entities doing business with Digicall Group must be encrypted or transmitted through an encrypted tunnel (VPN) or point-to-point tunnelling protocols (PPTP) that include current transport layer security (TLS) implementations.
    iv. Wireless (Wi-Fi) transmissions used to access Digicall Group computing devices or internal networks must be encrypted using current wireless security standard protocols (e.g., RADIUS, WPS private/public keys or other industry-standard mechanisms).
    v. Encryption or an encrypted/secured channel is required when users access Digicall Group confidential information remotely from a shared network, including connections from a Bluetooth device to a Digicall Group PDA or cell phone.
    vi. Secure encrypted transfer of documents and confidential information over the internet uses current secure file transfer programs such as “SFTP” (Secure FTP) and secure copy command (SCP).
    vii. All non-console administrative access such as browser/web-based management tools are encrypted using SSL based browser technologies using the most current security algorithm.

4.4 Encryption Key Management

a. Effective enterprise public and private key management is a crucial element in ensuring encryption system security. Key management procedures must ensure that authorized users can access, and decrypt all encrypted confidential information using controls that meet operational needs. Digicall Group key management systems are characterized by following security precautions and attributes:
    i. The Digicall Group uses procedural controls to enforce the concepts of least privilege and separation of duties for staff. These controls apply to persons involved in encryption key management or who have access to security-relevant encryption key facilities and processes, including Certificate Authority (CA) and Registration Authority (RA), and/or contractor staff.
    ii. The relevant regional IT Manager shall verify backup storage for key passwords, files, and confidential information to avoid a single point of failure and ensure access to encrypted confidential information.
    iii. Key management should be fully automated. Digicall Group IT Administrators should not have the opportunity to expose a key or influence the key creation.
    iv. Keys in storage and transit must be encrypted and password protected.
    v. Private keys must be kept confidential.
    vi. Application and system resource owners should be responsible for establishing data encryption policies that grant exceptions based on demonstration of a business need and an assessment of the risk of unauthorized access to or loss of confidential information.
    vii. Keys shall be rotated annually wherever possible. Any deviation to this policy where keys cannot be rotated, should be documented.
    viii. The relevant regional Digicall Group IT Manager or their designee shall ensure:
        - Decryption keys are not associated with user accounts.
        - Documentation and procedures exist to protect keys used to secure stored confidential information against disclosure and misuse.
        - Restrict access to cryptographic keys to the fewest number of custodians necessary.
        - Cryptographic keys are stored in the fewest possible locations.
        - Key management processes and procedures for cryptographic keys are fully documented.
        - Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened or keys are suspected of being compromised.

- Note: If retired or replaced, cryptographic keys need to be retained, these keys must be securely archived. Archived cryptographic keys should only be used for decryption/verification purposes.

- Cryptographic key custodians shall formally acknowledge that they understand and accept their key-custodian responsibilities.

4.5 Audit Controls and Management

a. On-demand documented procedures and evidence of practice should be in place for this operational policy as part of Digicall Group operational methodology.
b. Digicall Group shall inventory encrypted devices and validate the implementation of encryption products at least annually.
c. Documentation shall exist for key management procedures.
d. At-Rest encryption procedures exist and can be demonstrated.
e. In-Transit encryption procedures exist and can be demonstrated.
f. Exception logs exist and can be produced for those resources that are excluded from this policy.

4.6 Encryption key exposure

If an encryption key is stolen or exposed, the following steps should be taken to mitigate the risk and ensure the security of the encrypted data:

i. Revoke the compromised key immediately to prevent further unauthorized access. This should be done by updating the key management system to mark the key as invalid.
ii. Generate a new key to replace the compromised key. Update all systems, applications, and devices that used the compromised key with the new key.
iii. Activate the incident response plan specific to key compromise events. This plan should include notifying relevant stakeholders, including IT security teams, management, and any affected parties.
iv. Inform all users and administrators who use the affected key about the compromise and provide them with instructions on how to update to the new key.
v. Re-encrypt any data that was encrypted with the compromised key using the new key. This is critical to ensure that the data remains secure.
vi. Conduct a thorough investigation to determine how the key was compromised. Identify the root cause and any potential vulnerabilities that need to be addressed.
vii. Audit all systems and logs to detect any unauthorized access or data exfiltration that may have occurred using the compromised key. Implement enhanced monitoring to detect any further suspicious activities.

viii. Based on the findings from the investigation, implement additional security measures to prevent future key compromises. This may include strengthening access controls, improving key management procedures, and enhancing network security.

ix. Review and update the key management and data encryption policies to incorporate lessons learned from the incident. Ensure that the policies are aligned with best practices and regulatory requirements.

x. Document the incident, including the actions taken, findings from the investigation, and any changes made to the security practices. This documentation will be useful for future reference and for compliance purposes.

xi. Provide additional training and awareness sessions for staff to reinforce the importance of key management and the procedures to follow in the event of a key compromise.

5 Enforcement

1. Staff members found in policy violation may be subject to disciplinary action, up to and including termination.
2. Vendors and contracted employees found in policy violation may be subject to legal action being taken against them.

6 Distribution

This policy is to be distributed to all Digicall Group staff and contractors using Digicall Group confidential information resources.

7 Responsibilities

1. 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
2. All Managers are directly responsible for implementing the policy and ensuring staff compliance.
3. Compliance with this Information Security and all subsequent policies is mandatory.

8 Policy Compliance Monitoring

8.1 Compliance

Group IT will 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).

8.2 Exceptions

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

8.3 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.

8.4 Remediation of Non-compliance

Where non-compliance has been identified, dependent on the severity, 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 Manager.

9 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

10 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.

11 Appendices

None included with this policy.