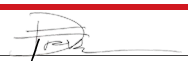
DIGICALL

A16 - INCIDENT MANAGEMENT POLICY V1.8

DOCUMENT CLASSIFICATION	Internal Use Only
VERSION	1.8
DATED	01 September 2024
DOCUMENT AUTHOR	Ameet Ranchod
DOCUMENT OWNER	Johan Kriel

Approval

NAME	POSISTION	SIGNATURE	DATE
Donald Fraser	IT Security & Compliance Manager		04/10/2024
Ameet Ranchod	IT Infrastructure Manager		07/10/2024
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	08.02.2019	Justus Boyens	Document Creation
0.9	11.02.2019	Justus Boyens	Final Draft
1.0	13.02.2019	Justus Boyens	Version 1.0
1.1	31.01.2020	Ameet Ranchod	Annual Review
1.2	24.02.2020	Ameet Ranchod	Added Information Classification Matrix and Handling Guide
1.3	19.03.2020	Ameet Ranchod	Amendments to Review, Added Policy Compliance Monitoring and Policy Governance
1.4	09.06.2020	Ameet Ranchod	Amendments after external review.
1.5	18.09.2020	Ameet Ranchod	Fix incorrect procedure reference
1.6	31.05.2022	Ameet Ranchod	Annual Review
1.7	01.07.2023	Donald Fraser	Updated personnel & roles, formatting
1.8	01.08.2024	Donald Fraser	2024 Revision, updated template

Table of Contents

1 Policy Scope

This policy applies to all employees and contractors during the performance of company related business and duties.

2 Policy Statement

Incidents are increasingly common occurrences whether caused through human error or malicious intent. Digicall Group operations rely on the proper use of confidential information and Personally Identifiable Information (PII) daily. Managing risk and responding in an organized way to incidents and breaches is key to operations and required by compliance standards.

3 Purpose

Digicall Group must have a robust and systematic process for responding to reported data security incidents and breaches. This policy is designed to standardize the Digicall Group-wide response to any reported breach or incident and ensure that they are appropriately logged and managed in accordance with best practice guidelines. Standardized processes and procedures help to ensure the Digicall Group can act responsibly, respond effectively, and protect its information assets to the best extent possible.

4 General

4.1 Incident

A “data security incident” or “incident” shall mean an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication or information resources of the Digicall Group. Common examples of data security Incidents include, but are not limited to, any of the following:

a. Successful attempts to gain unauthorized access to a Digicall Group system or client PII regardless of where such information is located.
b. Unwanted disruption or denial of service.
c. The unauthorized use of a Digicall Group system for the processing or storage of confidential information or PII.
d. Changes to Digicall Group system hardware, firmware, or software characteristics without the Digicall Group’s knowledge, instruction, or consent.
e. Loss or theft of equipment where confidential information or PII is stored.
f. Unforeseen circumstances such as a fire or flood that could lead to the loss or misuse of confidential information or PII.

g. Human error involving the loss or mistaken transmission of confidential information or PII.
h. Hacking, social engineering, phishing, or other subversive attacks where information is obtained by deceitful practice.
i. Information security weaknesses in systems or services.

A “data security breach” or “breach” is any incident where Digicall Group are not able to prevent the misuse of confidential information or PII. A breach is also an incident where data has been misused.

Adopting a standardized and consistent approach to incident management shall ensure that:

a. Incidents are reported in a timely manner and can be thoroughly investigated.
b. Incidents are handled by appropriately authorized and skilled personnel.
c. Appropriate levels of management are involved in response management.
d. Incidents are recorded and documented.
e. Organizational impacts are understood, and action is taken to prevent further damage.
f. Evidence is gathered, recorded, and maintained in a form that will withstand internal and external scrutiny.
g. External agencies, customers, and data users are informed as required.
h. Incidents are dealt with in a timely manner and normal operations are restored.
i. Incidents are reviewed to identify improvements in policies and procedures.

Incidents can occur locally, in the cloud, or through third party service providers. Reporting and management of Incidents shall occur similarly. Third party providers shall also be governed by contract terms and liability as defined in their operational agreements.

4.2 Data Classification

a. Incidents vary in impact and risk depending on several mitigating factors including the content and quantity of the data involved. It is critically important that Digicall Group management respond quickly and identify the data classification of the incident. This allows staff to respond accordingly in a timely and thorough manner.
b. Managers or information ‘owners’ shall be responsible for assigning classifications to information assets according to the standard information classification system presented below. (‘Owners” have approved management responsibility. ‘Owners’ do not have property rights.)

c. Where practicable, the information category shall be embedded in the information itself.
d. All Digicall Group associates shall be guided by the information category in their security-related handling of Digicall Group information.
e. All Digicall Group information and all information entrusted to Digicall Group from third parties falls into one of four classifications in the table below, presented in order of increasing sensitivity:

Information	Description	Examples
Unclassified / Public	Information is not confidential and can be made public without any implications for Digicall Group. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	• Product brochures widely distributed. • Information widely available in the public domain, including publicly available Digicall Group web site areas. • Sample downloads of Digicall Group software that is for sale. • Financial reports required by regulatory authorities. • Newsletters for external transmission.
Proprietary	Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence Digicall Group's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	• Passwords and information on corporate security procedures. • Knowledge used to process client information. • Standard Operating Procedures used in all parts of Digicall Group business. • All Digicall Group developed software code, whether used internally or sold to clients.
Client Confidential Data	Information received from clients in any form for processing in production by Digicall Group. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Client media. • Electronic transmissions from clients. • Product information generated for the client by Digicall Group production activities as specified by the client.
Company Confidential Data	Information collected and used by Digicall Group in the conduct of its business to employ people, to log and fulfil client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the Digicall Group. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Client media. • Salaries and other personnel data. • Accounting data and internal financial reports. • Confidential customer business data and confidential contracts. • Non-disclosure agreements with clients\vendors. • Digicall Group business plans.

4.3 Incident Reporting

The following process shall be followed when responding to a suspected incident:

1. Confirmed or suspected incidents shall be reported promptly to the relevant regional Digicall Infrastructure Manager. A formal report shall be filed that includes full and accurate details of the incident including who is reporting the incident and what classification of data is involved.
2. Once an incident is reported, the relevant regional Digicall Infrastructure Manager shall conduct an assessment to establish the severity of the incident, next steps in response, and potential remedies and solutions. Based on this assessment, the relevant regional Digicall Infrastructure Manager shall determine if this incident remains an incident or if it needs to be categorized as a breach.
3. All incidents and breaches will be centrally logged and documented to ensure appropriate documentation, oversight, and consistency in response, management, and reporting.
4. Refer to Incident Management & Escalation Procedure for further guidance.

4.4 Classification

Data breaches or incidents shall be classified as follows:

a. Critical/Major breach or incident – Incidents or breaches in this category deal with confidential information or PII and are on a large scale (Digicall Group-wide). All incidents or breaches involving client PII will be classified as Critical or Major. They typically have the following attributes:
    i. Any incident that has been determined to be a breach.
    ii. Significant confidential information or PII loss, potential for lack of business continuity, Digicall Group exposure, or irreversible consequences are imminent.
    iii. Negative media coverage is likely, and exposure is high.
    iv. Legal or contractual remedies may be required.
    v. Requires significant reporting beyond normal operating procedures.
    vi. Any breach of contract that involves the misuse or unauthorized access to client PII by a Digicall Service Contract Provider.

b. Moderately Critical/Serious Incident – Breaches or incidents in this category typically deal with confidential information and are on a medium scale (e.g., <100 users on the internal network, application or database related, limited exposure). Incidents in this category typically have the following attributes:
    i. Risk to the Digicall Group is moderate.

ii. Third party service provider and subcontractors may be involved.
iii. Data loss is possible but localized/compartmentalized, potential for limited business continuity losses, and minimized Digicall Group exposure.
iv. Significant user inconvenience is likely.
v. Service outages are likely while the breach is addressed.
vi. Negative media coverage is possible, but exposure is limited.
vii. Disclosure of client employee PII is contained and manageable.

c. Low Criticality/Minor Incident – Incidents in this category typically deal with personal or internal data and are on a small or individualized scale (e.g., <10 users on the internal network, personal or mobile device related). Incidents in this category typically have the following attributes:
    i. Risk to the Digicall Group is low.
    ii. User inconvenience is likely, but not Digicall Group damaging.
    iii. Internal data released but data is not client, employee, or confidential in nature.
    iv. Loss of data is totally contained on encrypted hardware.
    v. Incident can be addressed through normal support channels.

4.5 Incident Response

1. Management response to any reported Incident shall involve the following activities:
    a. Assess, Contain and Recover Data - All security Incidents shall have immediate analysis of the incident, and an incident report completed by the relevant regional Digicall Infrastructure Manager or their designee. This analysis shall include a determination of whether this incident should be characterized as a breach. This analysis shall be documented and shared with the Digicall Group Infrastructure Manager, the Digicall Group CIO, the Digicall Group Board, the affected parties, and any other relevant stakeholders. At a minimum, the relevant regional Digicall Infrastructure Manager shall:

Step	Action	Notes
A	Containment and Recovery:	Contain the breach, limit further organizational damage, seek to recover/restore data.
1	Breach Determination	Determine if the incident needs to be classified as a breach.
2	Ascertain the severity of the incident or breach and determine the level of data involved.	See Incident Classification.

3	Investigate the breach or incident and forward a copy of the incident report to the Digicall Group Infrastructure Manager.	Ensure investigator has appropriate resources including sufficient time and authority. If PII or confidential data has been breached, also contact the Digicall Group CIO. If the incident or breach is severe, Digicall Group executive management and general counsel shall be contacted.
4	Identify the cause of the incident or breach and whether the situation has been contained. Ensure that any possibility of further data loss is removed or mitigated as far as possible. If this loss cannot be mitigated, then any incident will be characterized as a breach.	Compartmentalize and eliminate exposure. Establish what steps can or need to be taken to contain the threat from further data loss. Contact all relevant departments who may be able to assist in this process. This may involve actions such as taking systems offline or restricting access to systems to a small number of staff members until more is known about the incident.
5	Determine depth and breadth of losses and limit exposure/damages.	Can data be physically recovered if damaged through use of backups, restoration, or other means?
6	Notify authorities as appropriate.	For criminal activities where property was stolen, or fraudulent activity occurred, contact the appropriate authorities and general counsel. Should the Breach involve client PII that involves a Digicall Group Service Contract Provider, notify the Digicall Group Board members.
7	Ensure all actions and decisions are logged and recorded as part of incident documentation and reporting.	Complete incident report and file with the Digicall Group Infrastructure Manager.

2. Assess Risk and Incident Scope – All incidents or breaches shall have a risk and scope analysis completed by the relevant regional Digicall Infrastructure Manager or their designee. This analysis shall be documented and shared with Digicall Group Infrastructure Manager, the Digicall Group CIO, the Digicall Group Board, the affected parties, and any other relevant stakeholders. At a minimum, the relevant regional Digicall Infrastructure Manager shall:

Step	Action	Notes
B	Risk Assessment	Identify and assess ongoing risks that may be associated with the incident or breach.
1	Determine the type and breadth of the incident or breach.	Classify incident or breach type, data compromised, and extent of breach.
2	Review data sensitivity.	Determine the confidentiality, scope and extent of the incident or breach.
3	Understand the status of the compromised data.	If data has been stolen, could it be used for purposes that harm the individuals whose identity has been compromised; if identity theft is involved, this poses a different type and level of risk.

4	Document risk limiting processes or technology components that contain and manage the incident.	Does encryption of data/device help to limit risk of exposure?
5	Determine what technologies or processes will mitigate the loss and restore service.	Are there backups of the compromised data? Can they be restored to a ready state?
6	Identify and document the scope, number of users affected, and depth of incident or breach.	How was many individuals' personally identifiable information affected?
7	Define individuals and roles whose data was compromised.	Identify all students, staff, districts, customers, or vendors involved in the incident or breach.
8	If exploited, what will the compromised data tell a third party about the individual? Could it be misused?	Confidential information or PII could mean little to an opportunistic laptop thief while the loss of trivial snippets of information could help a criminal build up a detailed picture associated with identity theft or fraud.
9	Determine actual or potential harm that could come to any individuals.	Identify risks to individuals: • Physical Safety. • Emotional Wellbeing. • Personal or Business Reputation. • Financial Implications. • Identity Concerns.
10	Are there wider consequences to consider?	Is there risk to another Digicall Group Business, the state, or loss of public confidence?
11	Are there others who might provide support or advise on risks/courses of action?	Contact all clients, local providers, agencies, or companies impacted by the breached data, notify them about the incident, and ask for assistance in limiting the scope of the incident.
12	Has the appropriate data been collected, reported, and maintained appropriately to be used as evidence?	Ensure processes for identification, collection, acquisition, and preservation of evidence are followed.

3. Notification and Incident Communications - Each security incident or breach determined to be "moderately critical" or "critical" shall have communication plans documented by the Digicall Group senior leadership, and their designees to appropriately manage the incident and communicate progress on its resolution to all effected stakeholders. At a minimum, the Digicall Group CIO shall:

Step	Action	Notes
C	Notification and Communications	Notification enables affected stakeholders to take precautionary steps and allow regulatory bodies to act on the incident or breach.

1	Are there legal, contractual, or regulatory notification requirements associated with the incident or breach?	Review vendor contracts and compliance terms, assure governmental reporting and notifications are understood. Contact Digicall Group legal representation as necessary to begin contractual adherence. Should the breach include client PII, initiate the Digicall Group Board hearing process.
2	Notify impacted individuals of the incident or breach remedies.	Provide individuals involved in the incident or breach with mitigation strategies to re-secure data (e.g., change user id and/or passwords etc.)
3	Determine internal communication plans.	Work with senior leadership and provide regular internal updates on status of the incident or breach, remedies underway, current exposure and containment strategies. This messaging should be provided to all internal stakeholders and management. Messaging shall be coordinated through relevant regional Digicall Group IT office.
4	Determine public messaging.	Prepare and execute a communication and follow-up plan with the Digicall Group CIO and senior leadership. Communication strategies need to define audience(s), frequency, messaging, and content.
5	Execute messaging plan.	Working through the Digicall Group CIO and appropriate leadership, execute the public and internal communication plans. Depending on the nature and scope of the incident or breach, multiple messages may need to be delivered as well as press and public communiques. Minimally notifications should include: • A description of the incident or breach (how and when it occurred). • What data was involved and whose data was compromised. • Details of what has been done to respond to the incident or breach and any associated risks posed. • Next steps for stakeholders. • Digicall Group contacts for the incident or breach, any follow-, and other pertinent information. • When notifying individuals, provide specific and clear advice on the steps they can take to protect themselves and what the Digicall Group and/or third-party vendor will do to help minimize their exposure. • Provide a way in which they can contact Digicall Group for further information or to ask questions about what has occurred (e.g., a contact name, helpline number or a web page).

4. Postmortem Evaluation and Response – Each incident or breach determined to be "moderately critical" or "critical" shall have a postmortem analysis completed by

the relevant regional Digicall Infrastructure Manager and their designees to appropriately document, analyse, and make recommendations on ways to limit risk and exposure in the future. At a minimum, the relevant regional Digicall Infrastructure Manager shall:

Step	Action	Notes
D	Evaluation and Response	To evaluate the effectiveness of the Digicall Group's response to the incident or breach.
1	Establish where any present or future risks lie.	Assess and evaluate the root causes of the incident or breach and any ways to mitigate and/or prevent a similar occurrence.
2	Consider the data and security measures employed.	Evaluate, analyse, and document the use cases and technical components of the incident or breach. Document areas for improvement in environment, technology, or approach that limit future security exposures. Make recommendations as appropriate.
3	Evaluate and identify areas of weakness in existing security measures and procedures.	Document lapses in process, procedure, or policy that may have caused the incident or breach. Analyse and document solutions and remedies to reduce future risks.
4	Evaluate and identify areas of weakness related to employee skills.	Assess employee readiness, education, and training. Document and plan for updates in education or procedural changes to eliminate potential for future incidents.
5	Report on findings and implement recommendations.	Prepare report and presentation to Digicall Group for major incidents or breaches.

Each of these four elements shall be conducted as appropriate for all qualifying incidents or breaches. An activity log recording the timeline of incident management shall also be completed. Reporting and documentation shall be filed and managed through the office of the relevant regional Digicall Infrastructure Manager.

5 Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy. Appropriate audit controls and management practice examples are as follows:

1. Archival completed incident reports demonstrating compliance with reporting, communication, and follow-through.
2. Executed communication plans for incident management.
3. Evidence of cross-departmental communication throughout the analysis, response, and post-mortem processes.

6 Responsibilities

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 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).

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, 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.

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.