NISR
NATIONAL INSTITUTE OF STATISTICS OF RWANDA

RISA
Rwanda Information Society Authority

DATA INCIDENT MANAGEMENT GUIDELINES

November 2025

Table of Contents

Acknowledgment

The development of the Data Incident Management Guidelines reinforces the National Data Sharing Policy and the National Data Governance Framework by establishing a clear, coordinated, and government-wide approach for identifying, reporting, managing, and resolving data-related incidents. These guidelines aim to safeguard the confidentiality, integrity, and availability of public-sector data and ensure that institutions can respond effectively to risks that may affect data security, service continuity, or public trust.

The National Institute of Statistics of Rwanda (NISR) coordinated the development of these guidelines in close partnership with the Rwanda Information Society Authority (RISA), the Ministry of ICT and Innovation (MINICT), and technical partners including Cenfri. Their expertise and collaboration were essential to ensuring alignment with national cybersecurity policies, the National Data Infrastructure, and Rwanda's broader Digital Transformation Agenda.

NISR extends its appreciation to sector institutions, members of the National Statistical System (NSS), and all stakeholders who contributed insights and feedback throughout the development process. Their engagement helped ensure that the guidelines are practical, relevant, and adaptable to the operational realities of government institutions.

The publication of the Data Incident Management Guidelines marks a significant step toward strengthening data governance, enhancing institutional readiness, and promoting responsible handling of data incidents. These guidelines affirm Rwanda's commitment to maintaining a secure, trusted, and resilient data ecosystem that supports innovation, accountability, and sustainable development.

1. Introduction

Information is a critical asset for the Government of Rwanda (GoR), essential for driving digital transformation, enabling service delivery, and supporting national development goals. The Government of Rwanda handles sensitive data that must be protected to maintain trust, ensure compliance, and safeguard national interests.

2. Purpose

This guideline provides a clear and practical framework for identifying, reporting, and responding to data security incidents in a timely and effective manner.

The key objectives of the data incident management guidelines are to:

- Ensure rapid detection and response to data incidents to reduce potential harm.
- Define clear roles and responsibilities for incident management across GoR.
- Maintain compliance with national data protection laws, regulations, and industry best practices.
- Protect the confidentiality, integrity, and availability of GoR data assets.
- Promote accountability and transparency in incident handling and reporting.
- Enhance organizational resilience through continuous improvement.

3. Scope

This guideline applies to all data assets managed, processed, or stored within any Government of Rwanda institution's data systems, including both on-premises and cloud-based environments; and all relevant stakeholders, including third parties.

4. Definitions

Data Incident	Event that compromises the integrity, confidentiality, or availability of data within any GoR data systems.
Data Breach	Specific type of data incident that involves unauthorized disclosure, access, or exposure of sensitive data.
Personally Identifiable Information (PII)	Data that can be used to directly or indirectly identify an individual, such as name, identification number, address, phone number, biometric data, or financial information.

5. Roles and responsibilities

Roles	Responsibilities
Data Protection Officer (DPO)	Ensures compliance with data protection regulations, oversees incident reporting and response procedures, and acts as a liaison with regulatory bodies in the event of a breach.
Data Owner	A leader (such as a divisional manager) responsible for ensuring the quality, security, and accessibility of data within their domain of oversight, collaborating with data stewards, data custodians and IT data governance teams.
Data Stewards	Continually ensure that data is properly defined, well-documented and governed, including ongoing improvement.
Data Custodians and System Administrators	Manage and safeguard datasets, ensure access control and encryption mechanisms are in place, and respond to potential data incidents. Implement technical security controls. Monitor system security to detect potential threats, implementing mitigation strategies. Maintain and configure IT infrastructure, implement backup and disaster recovery strategies, and assist in identifying and isolating affected systems.
Employees and Users	Responsible for following data security policies and guidelines, reporting suspicious activities, and cooperating with investigators during incident handling.

6. Data incident management process

STEP 1

IDENTIFY THE INCIDENT

The first step in incident management is to identify that an incident has occurred. Data Custodians and System Administrators should pay attention to the following indicators, among others:

- Unauthorized access attempts, such as multiple failed login attempts or unusual access from foreign locations.
- Unusual data modifications, including unexpected changes in datasets.
- Data unavailability or corruption, such as missing or unreadable files.
- System performance anomalies, including sudden slowdowns or unexplained crashes.
- Malware or ransomware detections, often flagged by protection tools.

STEP 2

CLASSIFY THE INCIDENT

Once an incident is identified, it should be classified by type and severity level.

Incident type

Identify the type of event:

- Unauthorized access
- Data corruption
- Data loss,
- Data Breach, or
- another category of incident.

Determine which systems, databases, and users have been affected by the incident.

Severity Level

- **Low:** The incident has minimal impact, and no sensitive data is involved.
- **Medium:** The incident has a noticeable impact, but operations remain functional and manageable.
- **High:** The incident significantly impacts data integrity, availability, or confidentiality, requiring immediate attention.
- **Critical:** The incident represents a severe breach affecting national data infrastructure or compromising sensitive information.

STEP 3

MITIGATE THE INCIDENT

Depending on the nature of the incident, consider the following containment and mitigation measures. If not competent to implement these measures themselves, staff members are advised to move on to the following step, reporting.

Incident Type	Containment Measures
Unauthorized Access	• Disable compromised accounts. Change passwords and enforce Multi-Factor Authentication (MFA). Block malicious IPs in firewalls.
Data Corruption	• Identify the last known good backup. Quarantine affected systems. Validate data integrity.
Data Loss	• Verify the extent of data loss or corruption. Identify last known good backups and validate their integrity. Ensure backups are scanned for malware or compromise before restoration. Restore data from backups. Verify data completeness and validity after restoration. Conduct data integrity checks using hashing or checksums. If possible, perform cross-validation against original data sources.
Data Breach	• Restrict access to exposed data. Determine leaked records. Notify affected stakeholders.
System Compromise (Malware, Ransomware)	• Isolate affected machines. Run antivirus/malware scans. Apply patches and security updates.

STEP 4

REPORT THE INCIDENT

Anyone can report an incident. Staff members are encouraged to report any unusual system behaviour. End-users can notify the Data Custodian if they encounter issues with data access or integrity.

All incidents must be reported according to the following timeline.

Timelines for Notification

Incident Severity	Internal Notification
Low (Minimal impact, no sensitive data exposed)	Within 24 hours, to the immediate supervisor or Data Custodian
Medium (PII exposure, but low risk)	Within 12 hours, to the Data Custodian
High (Significant data breach, affecting multiple users)	Immediately (within 1 hour) to the Data Team and Head of Institution
Critical (Major breach with legal, financial, or national security implications)	Immediately (within 1 hour) to the Data Team and Head of Institution

When reporting an incident, include as many of the below details as possible.

Reporting Template

Requirement	Details to Include
Nature of the Breach	Type of incident; type of data affected; severity level; how and when it occurred.
Scope and Impact	Number of affected individuals, systems impacted.
Mitigation Measures	Steps taken to contain and resolve the issue, if any.
Risk Assessment	Potential consequences for affected individuals.
Evidence	Any evidence of the incident, such as screenshots.

You may report the incident through any secure internal channels, such as:

- Emergency Email Alerts
- Incident Response Meetings (for high/critical breaches)
- GoR Secure Messaging Platform QTConnect

7. Notification protocols

In the case of High and Critical severity incidents, institutions may need to notify other stakeholders, including National Cyber Security Authority (NCSA) , affected individuals, and security organs. This should remain the sole responsibility of management.

Communication Restrictions

Only authorized public relations (PR) or legal representatives are permitted to communicate with the media. All public statements must be accurate, transparent, and compliant with legal requirements.

Under no circumstances may any staff member, unless authorized to do so by a legal representative, communicate reports of actual or suspected incidents via social media, email or telephone calls at any stage during or after the incident.

Reporting to NISR or NCSA

- Incidents can be escalated to NISR via email at info@statistics.gov.rw, through the NISR hotline at 4321, or by calling the NISR phone number 0788383103. You can also use the contact form at https://statistics.gov.rw/contact-us.
- For incidents related to Personal Information refer to the NCSA Incident Reporting Guidelines at www.cyber.gov.rw/report-incident/.

8. Investigation and continuous improvement

For High and Critical severity incidents, after containment, institutions should conduct an in-depth forensic investigation to identify the root cause and prevent future incidents. The objectives of the investigation are to determine how the incident occurred, identify the extent of data exposure, modification, or loss, and preserve evidence for regulatory compliance.

Investigation Report

The investigation should consider:

1. **Nature:** What happened? What systems or data were affected?
2. **Evidence:** System logs, network traffic data, compromised files, screenshots. If relevant, track IP addresses, login attempts, and timestamps of suspicious activity.
3. **Source:** Identify whether it was external hacking, insider threat, malware, or accidental data exposure.
4. **Recommendations:** Suggestions to prevent recurrence.

This report should be submitted to info@statistics.gov.rw within 15 days of the incident.

Lessons Learned

Furthermore, the report should be studied by the institution to identify lessons learned. A structured post-incident review helps organizations learn from incidents and enhance security policies, for example using Root Cause Analysis (RCA)**:**

1. **Identify the Problem**: Collect logs, system alerts, and forensic data.
2. **Analyse Contributing Factors**: Human error, technical failure, or external attack?
3. **Determine the Root Cause**: Use frameworks like 5 Whys Analysis, Fishbone Diagrams, or Fault Tree Analysis (FTA).
4. **Document Findings and Solutions**: Recommend actions to eliminate vulnerabilities and improve processes.

After RCA, a Lessons Learned Report should be developed to ensure that knowledge from the incident is used for future prevention. This should consider:

- *Response effectiveness* (What worked well and what didn't?)
- *Areas for improvement* (What security gaps need to be addressed?)

Lessons learned should be shared with internal teams and relevant stakeholders.

Improvement and Training

Relevant policies, processes, and any vendor security agreements should be revised to address recent chalenges and enhance security.

A well-informed workforce is the first line of defence against data incidents. Training and awareness programs ensure that employees and stakeholders understand their roles in incident prevention, detection, and response. Institutions are responsible for prioritizing training and ensuring staff are available to complete it. After High and Critical severity incidents, institutions may consider repeating relevant training.