National Bank of Rwanda
Banki Nkuru y'u Rwanda

KN 6 Av.4/P.O. Box 531 Kigali-Rwanda
Tel: (+250) 788199000 /
Website: www.bnr.rw /
E-mail: info@bnr.rw /
Swiftcode: BNRWRWRW /
Twitter: @CentralBankRw

The Governor

DIRECTIVE Nº 4230/2024-00037 [613] OF 17/01/2024 ON INCIDENTS MANAGEMENT AND RESPONSE FOR REGULATED INSTITUTIONS

The National Bank of Rwanda;

Pursuant to Law n° 48/2017 of 23/09/ 2017 governing the National Bank of Rwanda as amended to date, especially in Articles 6bis, 8, 9, 10, and 15;

Pursuant to Law nº 072/2021 of 05/11/2021 governing deposit-taking microfinance institutions, especially in Articles 23 and 24;

Pursuant to Law nº 47/2017 of 23/09/2017 governing the organization of banking, especially in Articles 37 and 117;

Pursuant to Law n° 061/2021 of 14/10/2021 governing payment system, especially in Article 6;

Pursuant to Law n° 030/2021 of 30/06/2021 governing the organization of insurance business, especially in Articles 56 and 58;
Pursuant to Law n° 05/2015 of 30/03/2015 governing the organization of pension schemes especially in Article 3;

Pursuant to the Law nº 73/2018 of 31/08/2018 governing credit reporting system, especially in Articles 11,12,18 and 23;

Pursuant to Regulation nº 43/2022 of 02/06/2022 governing business continuity management and operational resilience for regulated institutions, especially in articles 37 and 38;

Reference to also Regulation nº 50 /2022 of 02/062022 on cyber security in regulated institutions, especially in Articles 20 and 21

Considering that all regulated institutions should have systems enabling them to identify potential incidents that may pose risks to their infrastructure, systems, data, or customers, and establish a management framework;

ISSUES THE FOLLOWING DIRECTIVE:

CHAPTER ONE: GENERAL PROVISIONS

Article One: Purpose of this Directive

This Directive establishes the steps to be followed by regulated Institutions (RIs) to effectively monitor and report incidents and to ensure the safety and security of their systems, data, and customers.

Article 2: Interpretation

In this Directive:

(a) "Central Bank" means the National Bank of Rwanda

(b) "Regulated Institution(RI)" means an institution regulated and supervised by the Central Bank namely banks, insurers, deposit-taking microfinance institutions, payment system operators, payment service providers, credit reporting operators, and other institutions that the Central Bank may subject to this Directive

(c) "SLA" means Service Level Agreement

(d) An incident is defined as any unexpected event or series of events that has the potential to compromise the confidentiality, integrity, or availability of financial systems, data, or services. Incidents may include but are not limited to, cybersecurity breaches, data breaches, system failures, unauthorized access, fraud, natural disasters, and any other events that could negatively impact the stability, security, or resilience of an Institution.

(e) "Incident management" refers to the systematic process of identifying, responding to, and resolving incidents in a coordinated and effective manner. Incidents may be natural, technical, or man-made. Key aspects of incident management to be captured in the process are listed in the following Articles.

CHAPTER II: INCIDENT MANAGEMENT

Article 3: Categories of incidents

An RI shall categorize incidents based on their severity, and impact and consistent with their risk management framework. For example, incidents may be rated Minor, Medium, and Major

Here is an example of the rating of Incidents:

(a) Minor Incidents:

Minor incidents have a relatively low impact on operations, services, or individuals. They might cause inconvenience or minor disruptions, but they don't significantly affect the overall functioning of the organization.

(b) Medium Incidents:

Impact: Medium incidents have a noticeable impact on operations, services, or individuals. They can lead to partial disruptions or affect a larger portion of the organization's functions.

(c) Major Incidents:

Major incidents have a severe and widespread impact on the organization's operations, services, or individuals. They can cause significant disruptions, affecting critical systems, services, or infrastructure. Examples of Major incidents are highlighted in Annex III of this directive however the list is not exhaustive.

Article 4: Governance of Incidents

(1) A RI is required to put in place policies and procedures that enable the identification of incidents, assessment of incidents, resolution of incidents, and restoration plans of affected systems or services.

(2) A RI must have an updated incident management plan and procedures including the response plan, roles of individuals and necessary stakeholders such as police, health facilities, fire rescue, cyber security consultants, national cyber security Agencies, Institution groups, and subsidiaries, Integrated system third parties, Central Bank among others depending on the escalation matrix of the Incident.

(3) A RI is required to have an updated contact register at all times for individuals and third parties to be used at times of incident.

(4) A RI shall periodically test incident response plans and when major changes occur to ensure they are reliable and effective.

(5) A RI shall regularly review incident reports to identify trends and improve incident response procedures.

Article 5: Phases of incident management

A RI must follow the steps outlined in this Directive to effectively monitor and report incidents, protect their systems, data, and customers, and comply with regulatory requirements. The phases of the incident management life cycle are in Annex II of this Directive.

Article 6: Assessment of the incident

(1) A RI is required to delegate the function for Categorization of Incidents, escalation of Incidents, and ensuring resolution of Incidents.

(2) Depending on the type of incident, the incidents may be received from various channels and these may include, but are not limited to:

(a) Customer complaints;

(b) Intrusion prevention and detection systems; and

(c) Natural disaster.

(3) Incidents shall have an escalation matrix to the overall Incident Response Manager

Article 7: Incident response

(1) A RI is required to have an incident response plan for all types of Incidents as per the results of risk assessment in place to manage incidents effectively. The plan observes all phases of the incident management plan life-cycle as indicated in annex II of this Directive.

(2) A RI shall keep an updated Business continuity plan for all critical systems and their dependencies to ensure continuity and restoration of service in case of system failure.

Article 8: Incident response team

(1) A RI is required to form an Incident Response Team, comprising staff with the necessary technical and operational skills to handle incidents with an appropriate escalation matrix aligned to staff or entity responsibility and capacity.

(2) The team performs a root cause and impact analysis for all incidents and takes remediation actions and lays a strategy to prevent further damages and recurrence of incidents.

(3) A RI shall also have emergency response teams with the necessary skills to handle emergencies.

Article 9: Time-frame to address the incident

(1) A RI shall adequately address all incidents within corresponding resolution timeframes according to Impact and severity and the predefined incident response plan.

(2) A RI shall ensure that the recovery of systems/services does not exceed the identified recovery time objective.

(3) Where recovery of systems/services goes beyond the recovery time objective, The RI shall provide the justification to the Central Bank with immediate effect.

Article 10: Investigation of incidents

A RI is required to investigate incidents promptly to determine their cause, impact, and scope. Investigations shall be carried out by experienced and qualified personnel. The investigation team shall ensure that there is preservation of evidence.

Article 11: Escalation of Incidents

(1) A RI is required to establish corresponding escalation and resolution procedures where the resolution time-frame is proportionate to the severity level of the incident and the Business Impact assessment.

(2) An RI shall have an escalation matrix that considers staff or third-party roles and responsibilities to which the incident shall be assigned/escalated.

(3) A RI shall ensure that the handler of the Incident has the skills, qualifications, competence, and Decision-making authority.

(4) The incident escalation matrix shall include the business continuity coordinator to ensure that incidents exceed the defined recovery time objective and business continuity plan is activated.

(5) A RI is required to monitor all incidents to their resolution with a proactive escalation matrix that includes auto escalation once the resolution time is exceeded.

Article 12: Restoration of services

A RI is required to establish an incident management framework to restore all services as quickly as possible following the incident for a minimal impact on the business operations.

CHAPTER III: INCIDENT MONITORING AND REPORTING

Article 13: Identification of potential incidents

A RI is required to implement systems designed to identify potential incidents that may pose risks to their infrastructure, systems, data, or customers. This is done through the deployment of systems like inventory and event management, intrusion detection, and prevention systems among others.

A RI shall also regularly perform a risk assessment as per the institution's plan and each time major changes occur to identify potential incidents that may be faced.

Article 14: Records of incidents

A RI must document all incidents, including their causes, impact, and remedial actions. This should be done using a system to make tracking, documentation, and reference possible.

Article 15: Incident reporting

(1) A RI is required to put in place procedures for internal and external reporting of incidents, including the reporting channel, the information required for reporting, and the escalation procedures.

(2) A RI shall consider all regulatory reporting requirements including the Regulation governing business continuity management and operational resilience. the regulation on cybersecurity as well as the Directive of the Central Bank Implementing the Regulation On Reporting Requirements

(3) In reference to the above regulations the initial incident report shall therefore be submitted to the Central Bank within 2 hours of the incident and the final incident report within 24 hours.

(4) A RI shall use the Annex I template for major Incident reporting to the Central Bank.

(5) A RI shall keep customers informed of any major incident to maintain customer confidence throughout a crisis or an emergency situation. However, Incidents must be communicated professionally to avoid any potential reputational risk.

(6) A RI is required to comply with the SLAs while reporting Incidents to third parties and stakeholders to avoid any penalties, further damage, or loss of potential evidence.

(7) An RI also shall demand critical third parties to report Incidents that impact an interconnected system or shared service and monitor SLA in the occurrence of incidents.

CHAPTER IV: FINAL PROVISION

Article 16: Entry into force

This Directive comes into force on the date of its signature.

Done at Kigali on 22nd January 2024

Digitally signed by BNR(GOVERNOR)

RWANGOMBWA John
Governor

ANNEX ONE OF DIRECTIVE № 4230/2024-00037 [613] OF 17/01/2024 ON INCIDENTS MANAGEMENT AND RESPONSE FOR REGULATED INSTITUTIONS

REPORTING TEMPLATE

A. Initial incident report format

1. Major incident Initial report		
I. General Information		
Date of the report:		
Reporting institution:		
Contact person addresses:		
II. Detection and general information on the incident		
Date and time of the incident		
Date and time for detection of incident		
Reference number of incident/ID and Incident Name		
Summary Description of incident (Please, provide a brief description of the incident. e.g. information on: - What is the specific issue? - How did it happen? - How did it evolve? - Was it related to a previous incident? - Background of the incident detection - Service providers/ third parties affected or involved		
III. Incident classification		
Incident title and ID		
Overall Impact	Confidentiality/Integrity/Availability	
Transactions affected	% in volume	% in amount
High level of internal escalation so far/Business level		

III. Incident description	
Type of incident	
Cause/origin of the incident	
The root cause (If it is already known)	
Estimated completion time/date	
IV. Impact of incident	
Systems and components affected	
Noted Third parties affected	
other affected systems/dependencies	
Service downtime	
Estimated impacts/Noted impacts	
Action taken	

B. Final incident report format

2. Major incident final report	
I. General Information	
Date of the report:	
Reporting institution:	
Contact person addresses:	
II. Detection and general information on the incident	
Reference number of incident/ID and Name of the incident	
Date and time of the incident	
Date and time for detection of incident	
Date of accounting	
Summary Description of incident (Please, provide a brief description of the incident. e.g. information on: - What is the specific issue? - How did it happen?	

- How did it evolve? - Was it related to a previous incident? - Background of the incident detection; - Service providers/ third party affected or involved; - Crisis management started (internal and/or external (Central Bank crisis management); - internal classification of the incident and reason behind it)		
III. Incident classification		
Incident Tittle and ID		
IV. Incident description		
Type of incident		
Cause/origin of the incident		
Third parties/stake holders involved		
High level of internal and external escalation/Business level		
The root cause (If it is already known)		
V. Impact of incident	Confidentiality/Integrity/Availability	
Impact quantification	% in volume	% in amount
Systems and components affected		
Insurance claim		
Other recoveries		
Reputational impact		
Other affected systems/dependencies		
Service downtime		
Transactions affected		
Net loss		

Third parties affected	
Total recoveries	
Total claims	
VI. Resolution	
Justification of breach of Recovery Time Objective (if it was breached)	
Mitigations to prevent future occurrence	
Lessons learned	

Seen to be annexed to the directive № 4230/2024-00037 [613] of 17/01/2024 on incidents management and response for regulated institutions

Done at Kigali on 22nd January 2024

Digitally signed by BNR(GOVERNOR)

RWANGOMBWA John
Governor

ANNEX II OF DIRECTIVE № 4230/2024-00037 [613] OF 17/01/2024 ON INCIDENTS MANAGEMENT AND RESPONSE FOR REGULATED INSTITUTIONS

Phases of incident management life cycle

	Phase	Activities
	Planning and preparation	(a) creating policies, acquiring management support, developing user awareness, and building a response capability; (b) conducting research and development; (c) building checklists and acquiring necessary tools; (d) developing a communication plan and awareness training.
	Detection, triage, and investigation	(a) defining events *vs.* incidents and notification process; (b) detecting and validating incidents; (c) prioritizing and rating incidents; (d) implementing intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and security information events monitoring (SIEM); (e) utilizing anti-malware and vulnerability management systems; (f) conducting and participating in global incident awareness, e.g., CERT; (g) conducting log and audit analysis.
	Containment, analysis, tracking and recovery	(a) executing containment strategy for various incidents; (b) performing forensic analysis according to evidence-handling processes; (c) executing recovery procedures in line with the enterprise Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs); (d) determining the source of the incident.
	Post-incident assessment	(a) conducting post-mortem: (i) Exactly what happened, and at what times? (ii) how well did staff and management perform in dealing with the incident?

		(iii) were the documented procedures followed? Were they adequate? (iv) What corrective actions can prevent similar incidents in the future? (b) reporting on incident management-related metrics, e.g., mean-time-to-incident-discovery, cost of recovery; (c) providing feedback on lessons learned.
	Incident closure	(a) conducting incident response post-mortem analysis; (b) submitting reports to management, and stakeholders.

Seen to be annexed to the directive № 4230/2024-00037 [613] of 17/01/2024 on incidents management and response for regulated institutions

Done at Kigali on 22nd January 2024

Digitally signed by BNR(GOVERNOR)

RWANGOMBWA John
Governor

ANNEX III OF DIRECTIVE Nº 4230/2024-00037 [613] OF 17/01/2024 ON INCIDENTS MANAGEMENT AND RESPONSE FOR REGULATED INSTITUTIONS

Brief examples of major Incidents

- **Cybersecurity Breaches**: Major security breaches involving unauthorized access to sensitive customer data, financial fraud, or disruption of critical banking systems and system Outages: Prolonged and widespread system outages affecting online banking, ATMs, mobile apps, or other essential banking services;

- **Data Loss or Corruption:** Significant data loss or corruption, leading to the potential compromise of customer information or critical financial records and Fraud and Identity Theft: Major incidents involving widespread fraud or identity theft affecting a large number of customers;

- **Payment Processing Failures:** Failures in processing payment transactions, resulting in delayed or failed transactions for customers and businesses and Rogue Trading: Significant financial losses caused by unauthorized and risky trading activities by bank employees.

- **Regulatory Non-Compliance**: Serious violations of banking regulations that can lead to substantial fines or penalties and Money Laundering and Terrorism Financing: Incidents involving ML/TF activities within the Bank's systems that could attract regulatory actions and damage the bank's reputation.

- **Credit Card Breaches**: Large-scale breaches of credit card information leading to potential misuse and financial losses for customers and the Bank;

- **Operational Errors:** Major operational errors resulting in incorrect financial transactions, customer account mismanagement, or significant errors in financial reporting.

- **Corporate Governance Issues**: Serious governance issues that lead to internal conflicts, lack of transparency, or potential misuse of power within the bank's management and Incidents affecting critical systems: critical systems are considered to be the systems the institution uses for the core business for which the incident may pose a significant loss of funds, delays and breach of SLA, and failure to deliver services to customers or critical third parties.

Seen to be annexed to Directive Nº 4230/2024-00037 [613] of 17/01/2024 on Incidents Management and Response for Regulated Institutions

Done at Kigali on 22nd January 2024

Digitally signed by BNR(GOVERNOR)

RWANGOMBWA John
Governor