CENTRAL BANK OF THE GAMBIA

Cybersecurity Guidelines for Financial Institutions

Version 1.0

January 2022

1 PART 1: PRELIMINARY

1.1 TITLE- Cybersecurity Guidelines for Financial Institutions

1.2 Authorisation

This Guideline is issued pursuant to section 79 of The Central Bank of The Gambia Act 2018.

1.3 Application

The Guideline applies to all financial institutions authorised under the Banking Act 2009, Non-Bank Financial Institutions Act 2016 and financial institutions authorised under section 66 (b) of the Central Bank of The Gambia Act.

1.4 Definitions

Terms used in this Guidelines are defined below:

Business Continuity
A state of continued and uninterrupted operation of the business.

Bank
Means the Central Bank of The Gambia.

Business Continuity Management
A holistic business approach that includes policies, standards, frameworks, and procedures for ensuring that specific operations can be maintained or recovered promptly in the event of a disruption. Its purpose is to minimise the operations, financial, legal, reputational, and other material consequences arising from disruption.

Business Continuity Plan
A comprehensive, documented plan of action that sets out procedures and establishes the processes and systems necessary to continue or restore the operation of an organisation in the event of a disruption.

Chief Information Security Officer (CISO)
He/ She is a senior-level staff within an institution responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

Cybercrime
According to the International Organisation of Securities Commissions (IOSCO), ‘cyber-crime’ refers to a harmful activity executed by an individual or a group, through computers, Information Technology (IT) systems and/or the internet and targeting the computers, IT infrastructure or internet presence of another entity.

Cybersecurity Incident
Any malicious act or suspicious event that compromises, or attempts to compromise, the electronic or physical security perimeter of an information infrastructure asset or disrupts or attempts to disrupt, the operation of an information infrastructure asset. Such malicious

act potentially compromises the Confidentially, Integrity and Availability of an information infrastructure asset.

Cybersecurity
An activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorised access or modification, or exploitation.

Cybersecurity Drill Exercise
Refers to an all-out attempt to gain access to a system by any means necessary, and usually includes cyber penetration testing, physical breach, testing all phone lines for modem access, testing all wireless and systems present for potential wireless access, and testing employees through several scripted social engineering and phishing tests. These are real-life exercises carried out by a dedicated team of trained professionals that are hired to test the physical, cybersecurity, and social defences and resilience of an information infrastructure.

Cyber Resilience
Is the ability to prepare for, respond to and recover from cyber-attacks.

Cyber Risk
Any risk arising from a failure of an institution's information technology systems resulting in financial loss, disruption of service, and/or interference with business as usual or damage to the reputation of an institution.

Cyberspace
A virtual space created by interconnected computers and computer networks on the internet.

Financial Institutions (FI)
For the purposes of the guideline, FI means a deposit-taking institution such as a commercial bank, savings and loans company, mutual savings company, and credit union. which carries on the business of, or part of whose business is any of the following activities:

a) taking of deposit of money from the public repayable on demand and withdrawals by cheques, draft, or by other means,
b) financing of any activity by way of creating financial assets such as loans and advances, securities, bank deposits or otherwise, other than its own,
c) dealing in shares, stocks, bonds, or other securities,
d) collecting of money or accepting employer contributions and paying it out for legitimate claims or retirement benefits.

Financial System
Refers to a network of deposit-taking and non-deposit-taking financial institutions and entities providing financial services to the public.

Intra-group
This refers to situations where a firm enters into an outsourcing arrangement with a separate legal entity within the same group (including cross-border outsourcings).

IT Infrastructure
Refers to the hardware, software, network resources and services required for the existence, operation, and management of an enterprise IT environment. It allows an organisation to deliver IT solutions and services to its employees, partners and or customers and is usually internal to an organisation and deployed within owned facilities.

Outsourcing
Refers to business practices of hiring a party outside a company to perform services and create goods that traditionally were performed in-house by the company's employees.

Social Engineering
The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

2 PART II STATEMENT OF POLICY

2.1 Purpose

The purpose of this Guideline is to:

1) Strengthen the regulatory framework for ensuring a secure environment within the cyberspace of the financial institutions.
2) Ensure that the financial systems operate in a safe and more secure cyber environment.
3) Establish a coordinated approach towards the prevention and response to cyber incidents.
4) Promote continuous cybersecurity awareness creation to all relevant stakeholders.
5) Promote compliance with appropriate technical and operational cybersecurity standards.
6) Maintain public trust and confidence in the financial system.

2.2 Scope

This Guideline sets the minimum standards that financial institutions should adopt to develop effective cybersecurity governance and risk management frameworks taking into account the increased digitisation, evolving cyber threat landscape, increase frequency of cybercrimes, sophistication of cyber incidents and the need to strengthen cyber resilience.

2.3 Responsibility

The Board of Directors of financial institutions shall formulate and direct the implementation of the cybersecurity strategies, policies, procedures, guidelines and set minimum standards for institutions.

3 PART III GOVERNANCE

The key stakeholders in the governance structure to be put in place for ensuring that the guideline is implemented and adapted across the financial institutions are as follows:

3.1 Board of Directors

The Board shall assume ultimate accountability for governing cyber risk and therefore must oversee the organisation’s strategy, policies, and activities in this area.

The Board of Directors of Financial Institutions will be responsible for:

1) The approval and timely review of strategies, policies and processes for the management of key IT operational risks including cybersecurity risks within the financial institution.
2) The approval of the ICT strategy aligned with the institution’s overall business strategy.
3) Ensure the effective implementation of the approved strategies and policies as well as the risk management framework.
4) Receive quarterly reports and updates as may be required concerning cyber and information security incidents.
5) The approval of outsourcing strategy and policies.
6) The approval of policies and procedures on backup, recovery from cyber incidents, attacks, and disaster events.
7) Ensure a fully functional cybersecurity response plan is implemented which clearly outlines escalation processes and authorities to contact for effective resolution.
8) The alignment of the cybersecurity guideline with the National Cybersecurity Plan in place.
9) The enforcement of mandatory reporting of high impact cybersecurity incidents as well as timely information sharing.
10) Shall determine the institution’s target cyber security posture in relation to its current posture.

3.2 Senior Management

Senior Management will be responsible for:

1) To oversee the effective implementation of the cybersecurity guidelines.
2) The revision or creation of internal policies on cyber and information security, outsourcing, business continuity, backup and recovery from cyber incidents and disasters.
3) Tasking the Chief/Information Security Officer (C/ISO) to take a lead role in the overall cybersecurity preparedness of the institution. She/he should be made responsible for handling all cybersecurity-related incidents and their resolution working closely with the Director of IT.
4) Ensure adequate cybersecurity certification training is given to all designated staff to enhance skills and expertise in the prevention of cyber-attacks on the various IT systems platforms.

5) Setting up a Cybersecurity Steering Committee subject to the approval of the Board.
6) Oversee the functions of The Cybersecurity Steering Committee to carry out its mandate.
7) Ensure adequate training and resources are allocated to the Chief /Information Security Officer and team to ensure effective monitoring is conducted and a thorough investigation is carried out to address any cyber incidents.
8) Frequent review of reports and updates on cyber threats and ensure they are adequately mitigated.
9) Frequent discussions on the implications of cyber risks in day-to-day operations and providing guidance and control on any required changes.
10) Clearly outlining the types of cybersecurity incidents to escalate directly to Board of Directors.
11) Outlining a clear escalation process and its effective communication to relevant authorities.
12) Promote inter-institutional collaboration on cyber and information security threats.

3.3 Cybersecurity Steering Committee

3.3.1 The Composition

Each financial institution shall establish a Cybersecurity Steering Committee that will be responsible for the governance of their cybersecurity programme. The steering committee shall consist of senior representatives of relevant departments within the FI.

3.3.2 The Functions of the Cybersecurity Steering Committee

The Cybersecurity Steering Committee shall be responsible for:

1) Implementation and management of cybersecurity guideline to ensure all cyber-related risks are fully addressed or mitigated.
2) Providing oversight of policies, procedures, plans, and execution intended to provide security, confidentiality and integrity of financial data.
3) Ensure all cybersecurity strategies, procedures and policies are updated and enforceable.
4) To oversee the quality and effectiveness of policies and procedures concerning its information technology systems, including privacy, network security and data security.
5) Ensure all outsourced platforms have adequate cybersecurity controls in place to avoid any systemic compromise.
6) Ensure all cybersecurity breaches or incidents are logged with the correct priority level and escalated to identified authorities.
7) Implement an effective incident response plan by reviewing and providing oversight on policies and procedures in responding to any cyber-attacks.
8) The committee shall meet at least once every quarter or as an when required to discuss and address cybersecurity issues or incidents.
9) Update Senior Management about all high priority cybersecurity incidents or potential threats.
10) Ensure all high priority cyber-attacks are fully investigated and a thorough root cause analysis conducted after the incident and reported to senior management.

3.4 Chief /Information Security Officer (C/ISO)

Each financial institution shall appoint a Chief/Information Security Officer who is to ensure that cybersecurity policies and procedures are adhered to, and incidents are dealt with on time.

3.4.1 Functions of Chief/Information Security Officer

The C/ISO shall:

1) Serve as chairperson of the Cybersecurity Steering Committee.
2) Put in place the necessary security controls and processes to minimize cybersecurity-related risks.
3) Communicate cybersecurity-related risks to the Chief Executive Officer/Board.
4) Monitor all IT platforms and enforce full adherence to strict cybersecurity standards.
5) Ensure any potential cyber threats detected are effectively communicated to the Chief Executive Officer/Board and all designated staff.
6) Create a cyber-incidence response plan.
7) Conduct frequent cybersecurity awareness training for all staff at least twice a year.
8) Conduct cybersecurity assessment every end of the year for all staff to be part of the end of year assessment.

3.4.2 Requirement of Chief/Information Security Officer

POSITION	QUALIFICATION	RELEVANT EXPERIENCE
Chief Information Security Officer (CISO)	Masters or Post Graduate Degree in Computer Science, Engineering, Mathematics, or relevant field. OR Professional Qualification such as CCNP Security, CISSP, CEH or equivalent	Minimum of five years relevant work experience.
Information Security Officer (ISO)	Bachelors or Undergraduate Degree in Computer Science, Engineering, Mathematics, or relevant field. OR Professional Qualification such as CCNA Security, CISA, CompTIA Security+ or equivalent field	Minimum of three years relevant work experience.

4 PART IV GENERAL RISK MANAGEMENT REQUIREMENTS

All financial institutions shall:

1) Establish a risk management framework which should clearly define the roles and responsibilities in addressing cyber risk.
2) Establish a robust operational risk management policy with appropriate systems, procedures, and controls to identify, protect, detect, monitor, and manage cyber risks.
3) Independently evaluate all the risk proactively relating to cybersecurity and report to Senior Management and Board.
4) Have comprehensive cyber/information security policies.
5) Identify, monitor, and manage the risks that end-users, contractors, participants, intermediaries and service and utility providers pose to its operations.
6) Identify, monitor, and manage risks its operations might pose to end-users, contractors, participants, intermediaries and service and utility providers.

4.1 Dependency Risk Management Strategies & Cyber Resilience

For financial institutions to manage risk effectively, the following must be observed:

All financial institutions shall:

1) Have effective capabilities to identify and manage cyber risks associated with its business by looking for deviations from normal operations and activities.
2) Be protected with a proper shield to restrict or contain the effect of a potential cyber-attack.
3) Detect events of a cyber-attack in their institutions.
4) Incorporate proper respond strategies with regards to identified cyber incidents.
5) Include a proper recovery plan for imminent cyber-attacks. This is achieved through the Disaster Recovery and Business Continuity Plan/Policy (DR/BCP).

4.1.1 IT Disaster Recovery and Business Continuity Plan/Policy

For effective and efficient incident response, all financial institutions shall:

1) Have a business continuity plan/policy that addresses events posing a significant risk of disrupting operations and return to normal operations through traffic diversion to disaster recovery site should the main site become unavailable.
2) Review its Disaster Recovery and Business Continuity Plan/Policy (DR/BCP) with the business stakeholders to ensure they are adequate and effective to support cybersecurity resilience.
3) Create a DR/BCP test calendar to ascertain the effectiveness and efficiency of the Disaster Recovery and Business Continuity plans.
4) Establish processes for secure offline storage of critical records, including financial records of the institution using defined data standards to allow for the restoration of records after a disruption.
5) Test the DR/BCP that addresses a disruptive, destructive, corruptive or any other cyber event that could affect the ability to service customers and avoid incurring significant downtime that would affect the business operations of customers. Lessons learned shall be incorporated into the DR/BCP documents as an improvement.

4.1.2 IT Change Management Policy

All financial institutions shall:

1) Have a well-defined change management policy outlining the roles of internal parties (technical/operations).
2) Have a change management form in APPENDIX I signed by the respective authorities highlighting every change within the IT Systems.
3) Conduct a thorough impact analysis of all changes that should be carried out to avoid any negative adverse effect on systems and customers.
4) Have a test system where all required testing is conducted and confirmed before any deployment to live systems.
5) A review and test on all systems, operational policies, procedures, and controls should be conducted periodically and after any significant changes.

4.1.2.1 Roles and Responsibilities

Several categories of participants will assume responsibility regarding change management:

1) Change Manager – This person leads the change process and is accountable for ensuring the change plan is implemented. He/she should have the ability to make decisions relative to the goals and objectives of the said change cognisant of the resource implications such as the budget. He/she must have the rights to authorise change request.
2) Change Advisory Board- This constitutes stakeholders from different domains with requisite knowledge serving as advisers on change. They shall review and evaluate the implementation of critical change processes and validate before any high-risk changes are approved.
3) Change Owner/Implementor- Is responsible for defining, supporting, and documenting the overall change request life cycle. He/she shall facilitate the cross-departmental collaboration necessary for change management. He/she shall ensure that the necessary tests have been performed so that the request is followed with appropriate urgency.
4) Change Requestor- Responsible for initiating, preparing, and submitting a change request. He/she will support the collection of necessary business information and engaging with the concerned stakeholders.

4.1.3 Incident Response and Cyber Resilience

Financial institutions shall develop an incident response policy to plan for, respond to, contain and be able to rapidly recover from disruptions caused by cyber incidents, thereby strengthening their cyber resilience. This policy should stipulate the following:

1) The creation of a cyber-incident response plan with clearly defined escalation channels for effective resolution; approved by the Board of Directors.
2) Definitions of an Acceptable Interruption Window (AIW) for all categories of cyber-incidents; and performance metric at each stage of the incident response process.

3) The establishment of a dedicated team whose focus shall be on detecting and responding to cyber-incident.
4) Adequate and continuous training of the incident response team on how to respond, report cyber-incidents, and conduct trend analysis to thwart future occurrence.
5) Conducting cybersecurity drills based on the approved cyber-incident response plan and test schedule to ascertain its viability, effectiveness, and efficiency.
6) The adoption of automated detection tool such as network and system (endpoint) scanners; and alerts from Log Management solutions, Firewall, Intrusion Detection/Intrusion Prevention Systems (ID/IPS) etc. for effective early detection of cyber-incidents.
7) Appropriate chain of custody when collecting, analysing, and reporting cyber-incident in a legally admissible manner; and
8) How crisis information shall be communicated and shared with stakeholders including the CBG, law enforcement agencies and the public
9) Financial institutions should have the capability of operating critical business functions in the face of attacks while continuously enhancing cyber resilience.
10) Establish processes designed to maintain effective situational awareness capabilities to reliably predict analyse and respond to changes in the operating environment and to maintain effective incident response and cyber resilience governance.
11) FIs shall develop adequate management processes and plans for IT incident detection, notification, and escalation.

4.2 Cyber Resilience Assessment

Financial institutions shall carry out cyber resilience assessment to determine their current cybersecurity posture.

4.2.1 Determining the Current Cybersecurity Posture ("present state")

1) Financial institutions shall determine their "current" cybersecurity position at regular intervals by evaluating all identifiable cybersecurity vulnerabilities; threats and the likelihood of successful exploit; potential impact (reputational, financial, regulatory etc.); and the associated risks to estimate the number of assets and efforts required to recover from losses/damage attributed to possible cyber incidents.
2) The assessment should include but not limited to the adequacy of cybersecurity governance; policies, procedures, and standards; inherent risks in business operations; visibility to emerging threats to information assets; capability to swiftly respond and recover from cyber-incidents; and efficacy of existing controls to mitigate the identified risks.
3) Each financial institution shall conduct regular cyber drill exercise. A review of the outcome of the exercise will highlight the needed skills to improve as well as policy adjustment and system hardening.

4.3 Regular Independent Assessment and Testing

To ensure readiness to mitigating cybersecurity risk, each Financial Institution shall carry out regular independent assessment and testing of the following functions by Internal Audit, Risk Management and External Audit.

4.3.1 Role of Risk Management Function

This comprises risk, control, compliance, and oversight functions which ultimately ensure that the FI’s management of data, processes, risks, and controls are effectively operating. It is the responsibility of risk management to ensure that cybersecurity risks are managed within the enterprise risk management framework. Each FIs risk management function shall include:

1) Ensure the development and implementation of cyber and information risk management strategy.
2) Consider and incorporate as appropriate relevant best practices and internationally adopted standards in the development of cyber and information risk strategy.
3) Assessing the risks and exposures related to cybersecurity and determining whether they are aligned to the FI’s risk appetite.
4) Monitoring current and emerging risks and changes to laws and regulations.
5) Conducting regular IT risk assessments.
6) Collaborating with system administrators and others charged with safeguarding the information assets of the FIs to ensure appropriate control design.
7) Maintain comprehensive cyber risk registers: Key cybersecurity risks should be regularly identified and assessed. Risk identification should be forward-looking and include security incident handling.
8) Safeguarding the confidentiality, integrity, and availability of information.
9) Ensure that a comprehensive inventory of IT assets, classified by business criticality, is establish and maintained and a Business Impact Analysis process is in place to regularly assess the business criticality of IT assets.
10) Quantify the potential impact by assessing the residual cyber risk and considering risks that need to be addressed through insurance as a way of transferring cyber risk.
11) Reporting all enterprise risks consistently and comprehensively to the Board to enable the comparison of all risks equally in ensuring that they are prioritised correctly.

4.3.2 Role of Internal Audit function

Each FI shall appoint a Certified Information System Auditor (CISA) within their Internal Audit team. IT audit functions can be outsourced or through internal placement. The internal IT auditors shall ensure that the audit scope includes:

1) Continuous review and report on cyber risks and controls of the IT systems within the FIs and other related third-party connections.
2) Conduct up-front due diligence to mitigate risks associated with third parties.
3) Assess both the design and effectiveness of the cybersecurity guideline implemented.
4) Conduct regular independent threat and vulnerability assessment tests.
5) Conduct comprehensive penetration tests.
6) Report to the Board the findings of the assessments.

4.3.3 Role of External Auditors

External auditors should ensure that the IT audit scope includes the following:

1) Obtaining an understanding of the institution's IT infrastructure, use of IT, operations, and the impact of IT on financial reporting statements.
2) Understanding the extent of the FI's automated controls as they relate to business reporting. This should include an understanding of:
    a) IT general controls that affect the automated controls.
    b) Reliability of data and reports used in the audit that are produced by the FI.
3) Conduct independent threat and vulnerability assessment.
4) A comprehensive review of the approved cybersecurity strategy and policy.
5) Report annually to the institution's Board on the findings of the assessments.

4.4 Outsourcing

For outsourcing of IT systems and services, all FIs are expected to meet the following criteria:

1) Shall develop a guideline with clear lines of responsibility for ongoing management, operational oversight, risk management and regular review of the firm's outsourcing service providers (OSPs).
2) Conduct a thorough due diligence on prospective OSPs. Due diligence shall include:
    a) Consideration of, inter-alia, the OSP's technical capabilities, performance track record and financial strength and viability.
    b) The due diligence also considers whether the OSP can meet its requirements related to service quality and reliability, security, and business continuity in both normal and stressed circumstances.
    c) Firms satisfy themselves that the selected OSP has sufficient and robust controls in place related to its cybersecurity.
    d) These controls should be at least as strong as the controls utilised by the firm itself.
3) Execute a contract between the firm and its selected OSP. The contract shall include a documented SLA or equivalent consisting of the following:
    a) Clearly sets out the nature, quality, and scope of the service to be delivered as well as the roles and responsibilities of the contracting parties.
    b) Includes requirements for service levels, availability, and reliability, including measurable performance metrics and remedies for performance shortfalls.

c) Using the key provisions of the SLA, institutions regularly monitor the service delivery performance to determine if the OSP is delivering to the required standards.

d) Where performance shortfalls are identified, these are addressed with the OSP in a timely manner; and

e) Includes provisions relating to system and information/data security, business continuity and disaster recovery, service scalability, assurance and service termination, where appropriate. In particular, where new storage services are utilised, such as cloud, contracts with cloud providers specify the location(s) where the institution's data is stored, processed and managed, and the security measures required when transmitting and storing data.

4) Develop and maintain an exit management strategy to reduce the risks of business disruption should key IT outsourced services be unexpectedly withdrawn by the OSP, or voluntarily terminated by the institution. Viable options for resuming the impacted service(s) should be identified which are proportionate to the nature, scale, and complexity of the institution.

5) Institutions shall apply the same level of controls and oversight to intra-group IT outsourcing arrangements as to arrangements with external OSPs.

6) Institutions shall monitor the development of potential concentration risks and take appropriate action if they are, or are likely to become, reliant on a small number of OSPs to provide critical IT services.

7) All outsourcing policy shall include a provision that any outsourcing arrangements entered into by the institution should not impede effective on-site or off-site supervision of the institution by the Bank.

4.5 Awareness Training

1) Employees of financial institutions shall receive cyber and information security awareness training at least on an annual basis. This training shall be adjusted to the needs of various positions and levels within the institutions.

2) Each financial institution shall conduct an annual review of both the training calendar and curriculum and update them as required.

3) Senior Management shall allocate adequate funds for all required training and exercises as part of its overall IT/MIS budget.

4) All employees under cyber and information security domain shall be required to undergo in-depth and dedicated cyber and information security education, and examination by internationally recognised certification authorities.

5) An employee moving to a new position within the institution shall receive training in privacy protection and cyber and information security in line with the new position. The training shall be provided during the first month of employment in the new position or during the on-the-job training period whichever occurs first.

6) To equip the Board with the requisite knowledge to completely exercise its oversight function, financial institutions should have in place regular comprehensive technology risk and cybersecurity training programs for the Board members and Senior Management.

5 PART V REPORTING AND MONITORING

5.1 Monitoring

1) Financial institutions shall put in place metrics and monitoring processes to ensure compliance, provide feedback on the effectiveness of control and provide the basis for appropriate management decisions.
2) Each metrics should be properly aligned with strategic objectives and provide the information needed for effective decisions at the strategic, management and operational levels.
3) Each metrics should assess the effectiveness of the financial institutions' overall cybersecurity programme and measure its performance and efficiency.

5.2 Reporting

1) The Board and Senior Management of financial institutions shall establish effective and reliable reporting and communication channels throughout the institution to ensure the effectiveness and efficiency of the cybersecurity programme.
2) A reporting process that defines reporting and communication channels shall be established for the dissemination of security-related material such as changes in policies, standards, procedures, new or emerging threats and vulnerabilities.
3) The Senior Management shall be provided with quarterly reports to keep them abreast of the state of the cyber/information security programme and governance issues in the financial institution.
4) Financial institutions are required to report all cyber-incidents whether successful or not, immediately after such incident was identified to the Central Bank of The Gambia using the provided reporting format in APPENDIX II. Where necessary and applicable, additional information should be provided afterwards.

6 PART VI SANCTIONS

6.1 Penalty Clause

Any financial institution who contravenes any of the provisions of this guideline, shall attract appropriate sanctions as may be determined by the Central Bank of the Gambia in accordance with the provisions of the CBG act.

7 PART VII EFFECTIVE DATE

This guideline shall take effect………………………………………………………….2022

APPENDIX I
CHANGE MANAGEMENT TEMPLATE

CHANGE MANAGEMENT REQUEST FORM	CHANGE REQUEST NUMBER

NOTE: The change request needs to be reviewed and approved by ***SPONSOR NAME*** and IT/MIS Department, before the change is made.

SPONSOR- This person leads the change process and is accountable for ensuring the change plan is implemented.

INITIATED BY:

TITLE:
PRIORITY:

DATE RAISED:

DATE RESOLUTION REQUIRED:

CHANGE REQUEST DETAILS

DESCRIPTION:

JUSTIFICATION:

IMPACT IF NOT IMPLEMENTED:

CHANGE REQUEST IMPACT ANALYSIS	
SCOPE & REQUIREMENTS	
SCHEDULE	
RISK	
BUDGET	
MANAGEMENT	

CHANGE REQUEST SIGN-OFF:

SPONSOR SIGNATURE OF APPROVAL

SPONSOR NAME,

____

DATE:

IT SIGNATURE OF APPROVAL

IT/MIS DIRECTOR'S NAME,

____

DATE:

APPENDIX II
CYBER INCIDENT REPORT TEMPLATE

Institution Name:

Reporting Period:

Date of incident detection	Type of incident	Summary of incident	Physical Location/branch (if applicable)	Estimated/actual impact of the incident (financial and operational)	Internal reporting authority	Law enforcement authorities involved (if applicable)

Notes:

1) **Type of incident:** Intrusion/hacking, malware, malicious code, virus, phishing, denial of service, social engineering, unauthorised system usage, other (specify)
2) Please provide the amount in case of financial impact and description in case of operational impact.
3) To whom the event has been internally escalated.