CYBER SECURITY POLICY

OF

THE SUNDARGARH DISTRICT CENTRAL CO-OPERATIVE BANK LTD., SUNDARGARH

Regd. No. 90/SG Dt. 01.06.1955
Updated on 27/08/2024

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
Regd. No.
90/SG
01.06.1955

Resolution by Circulation of the Committee of Management of the Sundargarh District Central Co-operative Bank Ltd., Sundargarh held on 14.08.2024

Agenda-5	**Resolution**
To consider approving the policy of Bank on Cyber Security Policy in compliance with Reserve Bank of India, guidelines on Information Security, Electronic Banking, and Technology Risk Management & to implement the same in the Bank.	Chief Executive Officer of the Bank put a draft Cyber Security Policy before the Committee in compliance with Reserve Bank of India, guidelines on Information Security, Electronic Banking, and Technology Risk Management outline an organization's approach to maintaining data confidentiality, integrity, and availability. Discussed the relevant Circulars, extant guidelines as above & it is resolved to accept the draft as Cyber Security Policy of the Bank. Further, Sri Hemanta Kumar Mahapatra, Manager (FAD) is designated as Chief Information Security Officer (CISO). The approved Cyber Security Policy comes into force with immediate effect. The Chief Executive Officer is authorized to do the needful.

Copy communicated to all members of the Managing Committee of Sundargarh District Central Co-operative Bank Ltd, Sundargarh for confirmation.

Chief Executive Officer

PRESIDENT

THE SUNDARGARH DISTRICT CENTRAL COOPERATIVE BANK LTD.
Regd No.
90/56
1.6.1955

THE SUNDARGARH DIST. CENTRAL CO-OP BANK LTD.
Regd. No.
01.06.1955

Table of Contents

Document Control

Document History

Prepared By	Date	Approved By	Owner	Location	Version
Sri Hemanta Kumar Mahapatra, Manager (FAD)		Sri Rabindranath Kalundia, CEO	CEO	SDCCB	1.0

Revision History

Name	Date	Reason for Change	Version

Distribution History

Distributed to	Date	Purpose	Approver

Confidentiality

The information contained in this document is confidential, privileged and only for the information of the intended recipient and may not be used, published, or redistributed withoutthe prior written consent of Sundargarh District Central Co-operative Bank Ltd. The opinions expressed are in good faith and while every care has been taken in preparing these documents, Sundargarh District Central Co-operative Bank Ltd. makes no representations and gives no warranties of whatever nature in respect of these documents, including but not limited to the accuracy or completeness of any information, facts and/or opinions contained therein. Sundargarh District Central Co-operative Bank Ltd. its subsidiaries, the directors, employees, and agents cannot be held liable for the use of and reliance of the opinions, estimates, forecasts, and findings in these documents.

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
Regd. No.
90/SG
0[illegible]1955

1. Introduction

Digital Age Banking has become an integral part of The Sundargarh District Central Cooperative Bank Ltd., Sundargarh (SDCCB) Operational Strategy. Reserve Bank of India,guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds has indicated that the measures suggested for implementation cannot be static and banks need to pro-actively create/fine-tune/modify their policies, procedures and technologies based on new developments and emerging concerns.

Use of technology at SDCCB has gained momentum and Business requirements demands introduction of newer systems and technologies into the Digital Platform to keep abreast with the on-going competition and growth of the Bank. On the other hand, the number, frequency, and impact of cyber incidents / attacks have increased multi-fold in the financial sector including banks, underlining the need to put in place a robust Cyber Security/Resilience framework at SDCCB, to ensure adequate Cyber Security preparedness on a continuous basis.

In view of the evolving nature, growing scale/velocity, motivation, and resourcefulness of cyber-threats, it has become essential to enhance the resilience of SDCCB IT Systems by improving the current defence mechanisms to address cyber risks. These would include, but not limited to, putting in place an adaptive Incident Response, Management and Recovery framework to deal with adverse incidents/disruptions when they occur.

In view of the high dependency of our Bank on Information Technology, the SDCCB Board has approved to immediately put in place a Cyber Security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk.

2. Statement of Intent

SDCCB's endeavour has been making optimum use of Information Technology to carry out business, not relegating under any circumstances, the important and pivotal aspect of information and data security. DCCB is committed to ensuring that business conducts its activities in such a way that, it makes right use of IT and at the same time its information assets are optimally secured.

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
Regd. No. [illegible]
01.06.1955

Embracing new technology exposes the bank to the risk of possible unauthorized access to bank's data. There could also be over dependency on IT Systems leading to breakdowns in business due to unavailability of technology support.

SDCCB is bounded by various regulatory requirements requiring a Cyber Security Policy implementation on business channels in place over the internet such as Internet Banking, Mobile Banking etc.

By combining a myriad of hardware, software, policy, and assessment tools, SDCCB can significantly decrease its risk exposure with a Layered security, or 'Defense in Depth approach.

This Policy therefore addresses framework recommended by RBI in their Cyber Security Framework, Policy and Guidelines to enhance and combat cyber-attacks on IT Systems and Network of SDCCB.

3. Purpose

This Policy of SDCCB is being established with an objective to develop, implement, and maintain appropriate Cyber Security measures for the Bank. The main purpose of this policy is to:

- Inform SDCCBEmployees, Contractors, Vendors, Customers, and other authorized users of their obligatory requirements for protecting the Technology and Information assets of the company.

This Cyber Security policy describes the technology and information assets that must be protected and identifies threats to those assets, user responsibilities and their privileges as to:

- What is considered as acceptable use?
- What are the rules regarding Internet access?
- What are the User limitations?
- Penalties that may be levied for violation etc.

Thepolicy also contains procedures for responding to incidents that threaten the security of the SDCCB IT Systems and Networkand maintain an appropriate security program, including:

- Conducting regular assessments of the threats, vulnerabilities, and risks to the data, applications, networks, and operating platforms, including those associated with operational control systems; and

- Implementing appropriate security controls to address identified threats, vulnerabilities, and risks, consistent with the types of data and systems to be protected and the nature and scope of the organization.

4. Scope

This policy is applicable to all information assets of Sundargarh District Central Co-operative Bank Ltd., that are electronically stored, processed, documented, transmitted, printed and/ or faxed.The policy applies to all employees and external parties which term includes suppliers, vendors, third party users, contract staff, outsourced service providers and consultants of the bank's Primary Data Centre, Disaster Recovery Centre, CBS, Department of IT, Branches as well as all other locations of the bank.

4.1. Applicability

This policy applies to:

- All department and functions of SDCCB
- All branches and geographical locations of SDCCB
- All information technology assets used; and
- Third parties with whom SDCCB has a long-term association for regular operations
- Independent service providers engaged in providing IT services to SDCCB.

5. Baseline Cyber Security and ResilienceRequirements

An indicative but not exhaustive list of controlsshall be put in place at SDCCB to achieve baseline Cyber Security/Resilience as given below. This may be evaluated periodically to integrate risks that arise due to newer threats, products, or processes.Important security controls for effective Cyber Security management as may be articulated by CERT-In also shall be referred.

Points of considerationsshall be:

a. Growing technology adoption and potential threats.
b. Review by the IT Steering Committee of SDCCB.
c. Set the right tone at the top for Board level involvement and guidance.
d. Endeavour to stay ahead of the adversary.
e. Capacity to monitor various logs / incidents in real time / near real time through a C-SOC.
f. Keep vigil and to constantly remain alert.
g. Appropriately configure and secure hardware devices and software applications.
h. Provide appropriate awareness trainings during Induction Process of new recruits to communicate Cyber Security Policies of SDCCB.

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
Regd. No. 90[illegible]
[illegible].1935

i. Periodically organise and extend awareness trainings to employees, customers, vendors and other third-party support personnel of SDCCB.

6. Baseline Controls

To avert, remediate and monitor Cyber Security threats and to comply with regulatory body framework, policies, and guidelines, SDCCBshall be put in place the following critical controls.

(i) Inventory Management of Business IT Assets

(ii) Prevent Execution of Unauthorized Software

(iii) Environmental Controls

(iv) Network Management & Security

(v) Secure Configuration

(vi) Application Security Life Cycle

(vii) Patch / Vulnerability and Change Management

(viii) User Access Control Management

(ix) Authentication Framework for Customers

(x) Secure Mail and Messaging Systems

(xi) Vendor Risk Management

(xii) Removable Media Management

(xiii) Advanced Real-time Threat Defence and Management

(xiv) Anti-Phishing

(xv) Data Leak prevention strategy

(xvi) Maintenance, Monitoring, and Analysis of Audit Logs

(xvii) Audit Log settings

(xviii) Vulnerability assessment and Penetration Test and Red Team Exercises

(xix) Incident Response & Management

(xx) Risk based transaction monitoring

(xxi) Metrics

(xxii) Forensics

(xxiii) User / Employee/ Management Awareness

(xxiv) Customer Education and Awareness

(xxv) C-SOC

6.1. Inventory Management of Business IT Assets

a. SDCCB shall maintain an up-to-date inventory of Assets, business data/information including customer data/information, business applications, supporting IT infrastructure and facilities – hardware/software/network devices, key personnel, services, etc. indicating their business criticality.

b. SDCCB shall classify data / information based on information classification / sensitivity criteria.

THE SUNDARGARH DIST. CENTRAL CO-OP BANK LTD.
Regd. No.
01.06.1955

c. SDCCB shall appropriately manage and provide protection within and outside organisation borders / network taking into consideration how the data / information is stored, transmitted, processed, accessed, and used within / outside the bank's network, and level of risk they are exposed to depending on the sensitivity of the data/information.

(Annexure – 9 - SDCCB IT Asset RegisterFormat)

6.2. Prevent execution of unauthorized Software

a. SDCCB shall maintain an up-to-date and a centralised inventory of authorised / unauthorised software(s) and implement whitelisting of authorised applications / software / libraries, etc.

b. SDCCB shall implement a mechanism to control installation of software/applications centrally / otherwise on end-user PCs, laptops, workstations, servers, mobile devices, etc. and mechanism to block / prevent and identify installation and running of unauthorised software / applications on such devices/systems.

c. SDCCB shall continuously monitor the release of patches by various vendors / OEMs, advisories issued by CERT-in and other similar agencies and expeditiously apply security patches as per the patch management policy of the bank. SDCCB shall have a mechanism to apply patch / series of patches as and when they are released by the OEM / manufacturer / vendor for protection against well-known / well publicised / reported attacks exploiting the vulnerability by expeditiously following an emergency patch management process.

d. SDCCB shall clearly a framework including requirements justifying the exception(s), duration of exception(s), process of granting exceptions, and authority or approving, authority for review of exceptions granted on a periodic basis by officer(s) preferably at senior levels who are well equipped to understand the business and technical context of the exception(s).

(Refer Patch Management Policy Section 12 of SDCCB IS Policy)

6.3. Environmental Controls

a. Appropriate environmental controls shall be put in place for securing location of critical assets providing protection from natural and / man-made threats.

b. SDCCB shall put in place mechanisms for monitoring of breaches / compromises of environmental controls relating to temperature, water, smoke, access alarms, and service availability alerts (power supply, telecommunication, and servers), access logs, etc.

c. Appropriate physical security measures shall also be taken to protect the critical assets.

(Refer Physical Security Policy Section 12.4 of IS Policy)

6.4. Network Management and Security

a. SDCCB shall Prepare and maintain an up-to-date network architecture diagram including wired/wireless networks as appropriate.

b. SDCCB shall maintain an up to date / centralised inventory of authorised devices connected to bank's network (within / outside bank's premises) and authorised devices enabling the bank's network. The bank shall implement an automated network discovery and management tool to monitor devices connected to Banks network including branches.

c. SDCCB shall ensure that all the network devices are configured appropriately.

d. SDCCB shall periodically assess whether the configurations are appropriate to the desired level of network security.

e. SDCCB shall put in appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems.

f. SDCCB shall put in place mechanisms to identify authorised hardware / mobile devices like Laptops, mobile phones, tablets, etc. and ensure that they are provided connectivity only when they meet the security requirements of the bank.

g. SDCCB shall put in place a mechanism to automatically identify unauthorised device connections to the bank's network and block such connections.

h. SDCCB shall put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.

i. SDCCB shall establish Standard Operating Procedures (SOP) for all major IT activities including for connecting devices to the network.

j. SDCCB Security Operation Centre shall monitor the logs of various network activities and escalate any abnormal / undesirable activities to the officer in charge of security operations.

k. SDCCB shall put in place boundary defence system which shall be multi-layered, such as properly configured firewalls, proxies, DMZ perimeter networks, and network---based IPS and IDS. A mechanism to filter both inbound and outbound traffic shall also be implemented.

(Refer Network & Internet Security Policy Section 8 of IS Policy)

6.5. Secure Configuration

Secure controls that shall be implemented at a minimum are as below:

- SDCCB shall document and apply baseline security requirements / configurations to all categories of devices (endpoints / workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security systems, etc.), throughout the lifecycle (from conception to deployment) and carry out periodic reviews.

- SDCCB shall periodically evaluate critical devices (such as firewall, network switches, security devices, etc.) configurations and patch levels for all systems in the bank's network including systems in the Data Centres, in the third party hosted sites, and shared-infrastructure locations.

(Refer Information Security Review Policy Section 17 of IS Policy)

6.6. Application Security Life Cycle (ASLC)

a. SDCCB shall Incorporate/Ensure information security across all stages of application life cycle.

a. Source code audits by professionally competent personnel/service providers shall be conducted in respect of critical business applications. Assurance from application providers / OEM's that the application is free from embedded malicious / fraudulent code shall be obtained.

b. Secure coding practices shall be implemented for internally / collaboratively developed applications.

c. Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking and exception handling shall be clearly specified at the initial and ongoing stages of system development/acquisition/implementation and implementation performed accordingly.

d. The development/test and production environments shall be properly segregated. The data used for development and testing shall be appropriately masked.

e. Software / Application development approach shall incorporate secure coding principles, security testing (based on global standards) and secure rollouts procedures.

f. In-house Software / application development shall address vulnerabilities based on best practices baselines such as Open Web Application Security Project (OWASP) proactively and adopt principle of defence-in-depth to provide layered security mechanism.

g. When adopting new technologies, it shall be adequately evaluated for existing/evolving security threats and that the IT/security team of the SDCCB achieve reasonable level of comfort and maturity with such technologies before introducing them for critical systems of SDCCB.

(Refer Application Security Life Cycle Management Policy Section 10 of IS Policy)

THE SUNDARGARH DIST. CENTRAL CO-OP BANK LTD.
Regd. No. [illegible] SG
01.05.1955

6.7. Patch / Vulnerability and Change Management

a. SDCCB shall follow a documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches to minimize the number of vulnerable systems and the time window of vulnerability/exposure.

b. SDCCB shall put in place systems and processes to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of Server operating Systems/Databases/Applications/ Middleware, etc.

c. Changes to business applications, supporting technology, service components and facilities shall be managed using robust **Configuration Management Processes (CMP)** that shall ensure integrity of any changes made to the systems.

d. SDCCB shall conduct VA/PTof internet facing web/mobile applications, servers & network components throughout their lifecycle (pre-implementation, post implementation, after changes etc.)once in 6 months.

e. As a threat mitigation strategy, root cause of an incident shall be identified, and necessary patches shall be applied to plug the vulnerabilities.

f. SDCCB shall periodically evaluate the access device configurations and patch levels to ensure that all access points, nodes between different VLANs in the Data Centre, LAN/WAN interfaces, Bank's network to external network and interconnections with partner, vendor and service provider networks are securely configured. Such evaluation shall be conducted as and when a new device / software is being deployed into the Bank's network.

(Refer VA/PT Policy & Change Management Policy Section16.10 & 17 of IS Policy)

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
Regd. No [illegible]
01.[illegible].1955

6.8. User Access Control Management

a. SDCCB shall only provide secure access to the bank's assets / services from within / outside bank's network by protecting data / information at rest (e.g., using encryption, if supported by the device) and in-transit (e.g., using technologies such as VPN or other secure web protocols, etc.).

b. SDCCB shall ensure customer access credentials such as logon user id, authentication information and tokens, access profiles, etc. are protected against leakage / attacks.

c. SDCCB shall disallow administrative rights on end-user Workstations / PCs / Laptops and provide access rights on a need-to-know basis and for specific duration when it is required following an established process.

d. A centralised authentication and authorisation system through an Identity and Access Management solution shall be implemented for accessing and administering critical applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication, securing privileged accesses following the principle of least privileges and separation of duties.

e. SDCCB shall Implement appropriate (e.g., centralised) systems and controls to allow, manage, log and monitor privileged / superuser / administrative access to critical systems (Servers / OS / DB, applications, network devices etc.).

f. Controls shall be implemented to minimize invalid logon counts and / deactivate dormant accounts.

g. SDCCB shall monitor any abnormal change in pattern of logon regularly.

h. Unauthorized installation of software on PCs / laptops of the Bank shall not be allowed.

i. Remote management / wiping / locking of mobile devices including laptops shall be implemented.

j. Use of VBA / macros in office documents, control permissible attachment types in email systems shall be restricted.

k. Centralised policies through Active Directory or Endpoint management systems to whitelist/blacklist/restrict removable media use shall be implemented.

(Refer User Access Control Policy section 2.4 of IS Policy)

6.9. Authentication Framework for Customers

a. SDCCB shall have adequate checks and balance to ensure (including security of customer access credentials held with them) that transactions are put only through the genuine / authorised applications and that authentication methodology is robust, secure, and centralised.

b. SDCCB shall Implement appropriate authentication framework/mechanism to securely verify and identify the Bank provided applications of SDCCB to customers.

(Refer Authentication & Authorization Policy Section 9.4 of IS Policy)

6.10. Secure Mail and Messaging Systems

a. Secure mail and messaging systems shall be implemented to include those used by bank's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.
b. Email Server Specific configuration shall be documented, maintained, and updated regularly.

(Refer E-Mail &Security Policy Section 16 of IS Policy)

6.11. Vendor Risk Management

a. Bank shall ensure and be accountable for appropriate management and assurance of security risks in outsourced and partner arrangements.
b. Proper evaluation shall be carried out when a need arises for outsourcing critical processes like facility management services, desktop management, UPS management etc.
c. A comprehensive risk assessment shall be carried out for Selection of vendor/partner.
d. SDCCBshall regularly conduct effective due diligence, oversight and management of third-party vendors/service providers & partners providing services to the Bank.
e. SDCCB shall establishappropriate framework, policies and procedures supported by baseline system security configuration standards to evaluate, assess, approve, review, control and monitor risks and materiality of all vendor/outsourcing activities in the bank.
f. SDCCB shall ensure necessary vendor / outsourcing partners also follow regulatory and legal requirements of the Bank. Such regulation / legal requirements shall be incorporated in the vendor / outsourcing contracts.
g. Reserve Bank of India shall be provided access to all information resources (online/in person) of the banks when sought, even if the infrastructure/enabling resources may not physically be in the premises of banks.
h. SDCCB shall adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of defined borders.

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD. 1955

i. SDCCB shall verify and thoroughly satisfy themselves about the credentials of vendor/third-party personnel accessing and managing the bank's critical assets.

j. Background checks, non-disclosure, and security policy compliance agreements wherever necessary shall be mandated for all third-party service providers

(Refer Outsourcing/Third Party Policy Section 19 of IS Policy)

6.12. Removable Media

a. Policy for restriction and secure use of removable media / (Build Your Own Device) BYOD on various types / categories of devices shall be documented including but not limited to workstations / PCs / Laptops / Mobile devices / servers, etc. and secure erasure of data on such media after use shall be implemented.

b. Media types and information that could be transferred/copied to/from such devices shall be limited.

c. Removable media shall be scanned for malware/anti-virus prior before providing read/write access.

d. Centralized policies through Active Directory and Endpoint management systems to white list/blacklist/restrict removable media use shall be implemented.

e. As default rule, use of removable devices and media shall not be permitted in the banking environment unless specifically authorized for defined use and duration of use.

(Refer Acceptable Usage Policy Section 3 of IS Policy)

6.13. Advanced Real-time Threat Defense and Management

a. A robust defence at perimeter level and other required levels against the installation, spread, and execution of malicious code at multiple points in the enterprise shall be put in place.

b. Whitelisting of internet websites/systems at firewall level and at end point security level shall be implemented.

c. Anti-malware, Antivirus protection including behavioural detection systems for all categories of devices – (Endpoints such as PCs/laptops/ mobile devices etc.), servers (operating systems, databases, applications, etc.), Web/Internet gateways, email-gateways, Wireless networks, SMS servers etc. including tools and processes for centralized management and monitoring shall be implemented.

d. Secure web gateways with capability to deep scan network packets including secure (HTTPS, etc.) traffic passing through the web/internet gateway shall be implemented.

(Refer Environmental & Physical Security Policy Section 2 of IS Policy)

(Refer Incident Management Policy Section 4 of IS Policy)

(Refer Network & Internet Security Policy Section 8 of IS Policy)

(Refer Monitoring Policy Section 18 of IS Policy)

6.14. Anti-Phishing

a. SDCCB shall subscribe to Anti-phishing / anti-rogue application services from authorised external service providers for identifying and taking down phishing websites / rogue applications.

(Refer Anti-Phishing Policy in Annexure – 8.1)

6.15. Data Leak / Data Loss Prevention Strategy

a. SDCCB shall develop and implement a comprehensive data loss / leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information. This shall include protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.
b. Such arrangement shall be extended to vendor managed facilities of SDCCB as well.

(Refer Data Leak Prevention Strategy Annexure –8.2)

6.16. Maintenance, Monitoring & Analysis of Audit Logs

a. Systems administration team shall capture all audit logs pertaining to user actions of a system to facilitate forensic auditing if a situation arises so.
b. An alert mechanism shall be put in place to monitor any change in the log settings.
c. Scope, frequency, and storage of log collection shall be defined.
d. Systematic management and analysis of audit logs so as to detect, respond, understand or recover from an attack shall be implemented.
e. Appropriate logs/audit trails of each device, system software and application software shall be configured / stored and periodically validated to ensure logs include minimum information as well as uniquely identify the log.

f. Log retention shall be implemented as per the recommendations and best practices by consulting all the stakeholders before finalizing the scope, frequency and storage of log collection.
g. Logs shall be managed and analysed in a systematic manner to detect, understand or recover from an attack.
h. A syslog server shall be implemented to store logs pertaining to user actions.

(Refer Monitoring Policy Section 18 of IS Policy)

6.17. Audit Log Settings

a. Appropriate logs/audit trails of each device shall be captured and periodically validated.
b. Configuration of system software and application software's shall be done to ensure that logs include minimum information to uniquely identify the log for example by including a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or event and/or transaction.

(Refer Monitoring Policy Section 18 of IS Policy)

6.18. Vulnerability assessment and Penetration Test and IS Team Exercises

a. SDCCB shall conduct vulnerability assessment and penetration testing once in 6 months for all the critical systems, particularly those facing the internet.
b. The vulnerabilities detected shall be remedied promptly in terms of the bank's risk management / treatment framework to avoid exploitation of such vulnerabilities.
c. Penetration testing of public facing systems as well as other critical applications shallbe carried out by professionally qualified team once in 6 months.
d. Findings of VA/PT and the follow up actions necessitated shallbe reviewed as well as monitored closely by the IS Audit team as well as top Management.
e. IS Team shall be used to identify the vulnerabilities and the business risk, assess the efficacy of the defences, and check the mitigating controls already in place by simulating the objectives and actions of an attacker.

(Refer Audit& Assessment Policy Section 12.9 of IS Policy)

6.19. Incident Response and Management

a. An effective Incident Response programme shall be put in place to ensure appropriate action in case of any cyber security incident.

b. All Incidents shall be written and recorded. They must have written incident response procedures including the roles of staff / outsourced staff handling such incidents.

c. BCP/DR capabilities shall be put in place to adequately and effectively support the SDCCB's cyber resilience objectives.

d. BCP/DR shall be so designed and implemented to enable the SDCCB to recover rapidly from cyber-attacks/other incidents and safely resume critical operations aligned with recovery time objectives while ensuring security of processes and data is protected.

e. SDCCB shall have necessary arrangements, including a documented procedure, with such third-party vendors/service providers for such purpose. This shall include, among other things, to get informed about any cyber security incident occurring in respect of the bank on timely basis to early mitigate the risk as well as to meet extant regulatory requirements.

f. SDCCB shall have a mechanism to dynamically incorporate lessons learnt to continually improve the response strategies. Response strategies shall consider readiness to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication, and co-ordination with stakeholders during response.

(Refer Incident Management Policy Section 4 of IS Policy)

6.20. Risk Based Transaction Management

a. Risk based transaction monitoring and surveillance process shall be implemented as part of fraud risk management system across all delivery channels.

b. SDCCB shall also notify its customers, through alternate communication channels, of all payment or fund transfer transactions above a specified value determined by the customer.

(Refer Risk Management Policy Annexure -8.3)

6.21. Metrics

a. SDCCB shall develop a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators. Such illustrative metrics shall include coverage of anti-

THE SUNDARGARH DIST. CENTRAL CO-OP BANK LTD.

malware software and their updating percentage, patch latency, extent of user awareness training, vulnerability related metrics, etc.

(Refer Risk Management Policy Annexure –8.3)

6.22. Forensics

a. SDCCB shall have a support / arrangement for network DDOS mitigation services on stand-by.

b. SDCCB shall periodically and actively participate in cyber drills conducted under the aegis of Cert-IN, IDRBT etc as and when notified and included.

(Refer Incident Management Policy Section 4 of IS Policy)

(Refer Forensics & Incident Analysis Procedure Annexure –8.4)

6.23. User / Employee / Management Awareness

a. SDCCB shall Define and communicate to users/employees, vendors & partners security policies covering secure and acceptable use of bank's network/assets including customer information/data, educating them about cybersecurity risks and protection measures at their level.

b. Users / Employees / Management shall report any suspicious behaviour / incidents to the incident management team.

c. SDCCB shall conduct targeted awareness/training for key personnel (at executive, operations, security related administration / operation and management roles, etc.). Cyber Security awareness programs shall also be mandatory for new recruits / employees.

d. Web-based quiz and training as appropriate training programs shall be implemented for lower, middle and upper management and shall be conducted every year.

e. Board members shall be sensitised on various technological developments and cyber security related developments periodically through an internal procedure.

f. Board members shall also be provided with awareness programmes on IT Risk / Cyber Security Risk and evolving best practices in this regard to cover all the Board members at least once a year.

(Refer Training & Awareness Policy Section 14.5 of IS Policy)

6.24. Customer Education and Awareness

a. Customer awareness programs shall be implemented to Improve and maintain customer awareness and education regarding cyber security policy and risks.

b. Customers shall be encouraged to report phishing mails/ phishing sites and on such reporting take effective remedial action.
c. Customers shall also be educated on the downside risk of sharing their login credentials /passwords etc. to any third-party vendor and the consequences thereof.

(Refer Training & Awareness Policy Section 14.5 of IS Policy)

7. Cyber Security Operation Centre

a. SDCCB shall set up a C-SoC (Cyber Security Operations Centre) to ensure continuous surveillance and keep itself regularly updated on the latest nature of emerging cyber threats.
b. Critical business and customer data/information shall be protected with appropriate controls.
c. Compliance with relevant internal guidelines, country regulations and laws shall be adhered to.
d. Real-time/near-real time information on and insight into the security posture shall be implemented
e. C-SOC shall have the ability to manage security operations effectively and efficiently by preparing for and responding to cyber risks/threat as well as facilitate continuity and recovery
f. C-SOC shall have capabilities to integrate various log types and logging options into a Security Information and Event Management (SIEM) system, ticketing/workflow/case management, unstructured data/big data, reporting/dashboard, use cases/rule design (customised based on risk and compliance requirements/drivers), etc.
g. C-SOC shall monitor the logs of various network activities and shall escalate any abnormal / undesirable activities.
h. Key Responsibilities of SDCCBC-SOC shall include:
   (i) Monitor, analyse and escalate security incidents
   (ii) Develop Response - protect, detect, respond, recover
   (iii) Conduct Incident Management and Forensic Analysis
   (iv) Co-ordination with relevant stakeholders within the UCB/external agencies
i. C-SOC shall ensure incident response capabilities in all interconnected systems and networks including those of vendors and partners and readiness demonstrated through collaborative and co-ordinated resilience testing that meet the SDCCB's recovery time objectives.
j. SDCCB shall implement a policy & framework for aligning Security Operation Centre, Incident Response and Digital forensics to reduce the business downtime/ to bounce back to normalcy.

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
Regd. No.
01.06.1955

k. SDCCB shall develop a comprehensive set of metrics that provides for prospective and retrospective measures, like key performance indicators and key risk indicators. Some illustrative metrics may include coverage of anti-malware software and their updation percentage, patch latency, extent of user awareness training, vulnerability related metrics, number of open vulnerabilities, IS/security audit observations, etc.

l. C-SOC shall have support/ arrangement for network forensics/forensic investigation/distributed denial-of-service (DDOS) mitigation services on stand-by.

m. SDCCBshall have a Board approved IT-related strategy and policies covering areas such as:
   (i) Existing and proposed hardware and networking architecture
   (ii) Standards for hardware or software prescribed by the proposed architecture
   (iii) Strategy for outsourcing, in-sourcing, procuring off-the-shelf software, and in-house development
   (iv) IT Department's Organisational Structure
   (v) Desired number and level of IT expertise or competencies
   (vi) Human resources, plan to bridge the gap (if any) and requirements relating to training and development
   (vii) Strategy for keeping abreast with technology developments and to update systems as and when required
   (viii) Strategy for independent assessment, evaluation and monitoring of IT risks, findings of IT/IS/Cyber security related audits.

n. SDCCB shall form a separate cyber security function/group to focus exclusively on cyber security management. The organisation of the cyber security function should be commensurate with the nature and size of activities of SDCCB including factors such as technologies adopted, delivery channels, digital products being offered, internal and external threats, etc. The cyber security function shall be adequately resourced in terms of the number of staff, level of skills and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc.

o. SDCCB shall set up a Board level IT Strategy Committee with a minimum of two directors as members, one of whom should be a professional director. At least two members of the IT Strategy Committee shall be technically competent while at least one member shall have substantial expertise in managing/guiding technology initiatives.

p. Roles and responsibilities of IT Strategy Committee/Board shall be:
   (i) Approving IT strategy and policy documents
   (ii) Ensuring that the management has put an effective strategic planning process in place

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
Regd. No.
01.06.1955

(iii) Ensuring that the IT organizational structure complements the business model and its direction

(iv) Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable

(v) Reviewing IT performance measurement and contribution of IT to businesses

q. SDCCB shall also form an IT Steering Committee with representatives from the IT, HR, legal and business sectors of the Bank. Its role shall be to assist the Executive Management in implementing IT strategy that has been approved by the Board from time to time. It shall include prioritization of IT-enabled investment, reviewing the status of projects (including, resource conflict), monitoring service levels and improvements, IT service delivery and projects. The IT Steering committee/Board should appraise/report to the IT strategy Committee periodically. The IT Steering committee shallalso focus on implementations.

r. Core functions of the IT Steering Committee include:

(i) Defining project priorities and assessing strategic fit for IT proposals

(ii) Reviewing, approving, and funding initiatives, after assessing value-addition to business process

(iii) Ensuring that all critical projects have a component for "project risk management"

(iv) Sponsoring or assisting in governance, risk and control framework, and also directing and monitoring key IT Governance processes

(v) Defining project success measures and following up progress on IT projects

(vi) Provide direction relating to technology standards and practices

(vii) Ensure that vulnerability assessments of new technology are performed

(viii) Verify compliance with technology standards and guidelines

(ix) Ensure compliance to regulatory and statutory requirements

(x) Provide direction to IT architecture design and ensure that the IT architecture reflects the need for legal and regulatory compliance, the ethical use of information and business continuity

s. A Senior level official shall be designated as Chief Information Security Officer (CISO), who shall be responsible for articulating and enforcing the policies that SDCCB uses to protect its information assets apart from coordinating the cyber security related issues / implementation within the organisation as well as relevant external agencies. The CISO shall primarily be responsible for ensuring compliance to various instructions issued on information/cyber security by RBI.

t. The following expectation shall become part of CISO overall responsibilities with regards to Cyber Security and Information Security Management.

(i) The CISO shall report directly to the top executive overseeing the risk management function or in his absence to the CEO directly.

(ii) The CISO shall have the requisite technical background and expertise.

(iii) The CISO shall have a reasonable minimum term.

(iv) The CISO shall place a separate review of cyber security arrangements/ preparedness of SDCCB before the Board on a quarterly basis.

(v) SDCCB's Board should be able to objectively measure steps to assess the effectiveness of the CISO's office.

(vi) The CISO will be responsible for bringing to the notice of the Board about the vulnerabilities and cyber security risks that SDCCB is exposed to.

(vii) The CISO, by virtue of his role as member secretary of information security and/or related committees(s), if any, may ensure, inter alia, current/ emerging cyber threats to banking (including payment systems) sector and SDCCB's preparedness in these aspects are invariably discussed in such committee(s).

(viii) The CISO's office shall manage and monitor the C-SOC and drive cyber security related projects. It can have a dotted relation with Chief Information Officer (CIO)/Chief Technology Officer (CTO) for driving such projects.

(ix) The CISO shall be an invitee to the IT Strategy committee and IT Steering Committee.

(x) The CISO may also be a member of (or invited to) committees on operational risk where IT/ IS risk is also discussed.

(xi) The CISO's office shall be adequately staffed with technically competent people, if necessary, through recruitment of specialist officers, commensurate with the business volume, extent of technology adoption and complexity.

(xii) The CISO shall not have any direct reporting relationship with the CIO/CTO and shall not be given any business targets.

(xiii) The budget for IT security/ CISO's office may be determined keeping in view the current/ emerging cyber threat landscape.

u. Since IT/ cyber security affects all aspects of the bank, it is necessary to consider IT/ cyber security from an Organization wide perspective. A steering committee of executives shall be formed with formal terms of reference.

v. The CISO shall be the member secretary of the Committee.

w. The Information Security Committee may include, among others, the Chief Executive Officer (CEO) or designee and two senior management officials well versed in the subject.

x. The Committee shall meet at least on a quarterly basis.

y. Major responsibilities of the Information Security Committee, inter-alia, include:

(i) Developing / Updating and facilitating the implementation of information security policies, standards, and procedures to ensure that all identified risks are managed within a SDCCB's risk appetite.

(ii) Approving and monitoring major cyber security projects and the status of cyber security plans and budgets, establishing priorities, approving standards and procedures.

(iii) Supporting the development and implementation of an Organization wide information security management programme.

(iv) Reviewing the position of security incidents and various information security assessments and monitoring activities across SDCCB.

(v) Reviewing the status of security awareness programmes.

(vi) Assessing new developments or issues relating to information/ cyber security

(vii) Reporting to the Board of Directors on cyber security activities

(viii) Minutes of the Information Security Committee meetings shall be maintained to document the committee's activities and decisions and a review on information/cyber security needs to be escalated to the Board on a quarterly basis.

z. SDCCB shall set up an Internal Audit Committee at the Board level. In addition to its prescribed role as per extant instructions, the IACB shall also be responsible for the following:

(i) Performance of IS Audit and Evaluation of significant IS Audit issues – The IACB should devote appropriate and sufficient time to IS Audit findings identified and members of IACB shall review critical issues highlighted and provide appropriate guidance to SDCCB's management.

(ii) Monitor the compliance in respect of the information security reviews/VA-PT audits under various scope conducted by internal as well as external auditors/consultants to ensure that open issues are closed on a timely basis and sustenance of the compliance is adhered to.

7.1. C-SOC Governance Aspects:

- Top Management/Board Briefing on Threat Intelligence.
- Dashboards and oversight.
- Policy, measurement, and enforcement (key metrics, reporting structure, define what is to be reported).
- Informing stakeholders, stakeholder participation.

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
Regd. No.
01.06.1955

8. Annexures

8.1. Anti-Phishing Policy

Guide to Developing the Policy

This Anti-Phishing policy applies throughout SDCCB as part of the Cyber Security Governance framework. It applies regardless of whether staff use computer systems and networks, since all staff are expected to protect all forms of information assets including computer data, written materials/paperwork, and intangible forms of knowledge and experience. This policy also applies to third party employees working for SDCCB whether they are explicitly bound contractual terms and conditions or implicitly bound by generally held standards of ethics and acceptable behaviour, to comply with SDCCB IS Policies.

Phishing

Phishing is a type of attack carried out to steal usernames, passwords, credit card information, Social Security Numbers, and other sensitive data. Phishing is most often seen in the form of malicious emails pretending to be from credible sources.

Attackers can use this information to:

- Steal money from victims (modify direct deposit information, drain bank accounts).
- Perform identity theft (run up charges on credit cards, open new accounts).
- Send spam from compromised email accounts.
- Use your credentials to access other systems, attack other systems, steal data, and jeopardize the mission of the organization.

Phishing emails wants our Banks credentials. Some attackers will set up fake web sites and send emails with an immediate call-to-action that demands you to "update your account information" or "login to confirm ownership of your account". If you enter your credentials into these illegitimate web sites you are sending your username and password directly to the attackers.

Combatting Phishing

SDCCB shall stop phishing attempts, spam emails, and virus infected messages. However, the methods scammers use change from time to time. SDCCB shall implement Phishing filtering which may block otherwise legitimate email.

Following actions shall be adhered to at SDCCB.

- Never send passwords, bank account numbers, or other private information in an email.
- Avoid clicking links in emails especially any that are requesting private information.
- Be wary of any unexpected email attachments or links, even from people you know.
- Look for 'https://' and a lock icon in the address bar before entering any private information.
- Have an updated anti-virus program that can scan email.

Actions for Suspected or Confirmed Phishing Attempts

SDCCB DIT requires that each, in the event of suspected or confirmed phishing targeting conduct the following actions.

- Change your User login credentials
- Change your Username and other related passwords
- Set mobile devices to delete all data via Exchange and/or FindMyiPad.
- Change login and password for any personal accounts that share the same password such as:
    - Online banking
    - Personal email
    - Online purchasing (PayPal, Amazon, eBay, etc.)
    - iTunes account
    - Social media (Facebook, Twitter, blogs, etc.)
    - Online backup service or file sharing (Dropbox, Mozy, Carbonite, etc.)
- Contact the abuse or fraud department of the service being impersonated (eBay, PayPal, etc.)
- Call the Technology Service Centre
- If you suspect a bank or credit card account may have been compromised, contact that institution to check your account immediately and request a credit report.

Phishing Awareness Training

SDCCB requires that all employees who are authorised to use Computer Systems to undergo Internal Trainings from time to time as announced by the DIT/HRD.

Compliance & Non-Compliance with Policy

Compliance with this policy is mandatory for all employees of SDCCB, including contractors and executives.SDCCB DIT will monitor compliance and non-compliance with this policy and report to the Executive team as appropriate.

Non-compliance includes but is not limited to:

- Failure to adhere to the Policy

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
01.06.1955

- Failure to attend training sessions including a social engineering exercise
  - Social engineering exercise includes but is not limited to:
    - Clicking on a URL within a phishing test
    - Replying with any information to a phishing test
    - Opening an attachment that is part of a phishing test
    - Enabling macros that are within an attachment as part of a phishing test
    - Allowing exploit code to run as part of a phishing test
    - Entering any data within a landing page as part of a phishing test
    - Transmitting any information as part of a vishing test
    - Replying with any information to a smishing test
    - Plugging in a USB stick or removable drive as part of a social engineering exercise
    - Failing to follow company policies during a physical social engineering exercise.

8.2. Data Leak Prevention Policy

Data Leak Prevention

Data leakage prevention (DLP) can be defined as the practice of detecting and preventing the unauthorised disclosure of data. Also referred to as data loss prevention and data loss protection, the main purpose of DLP is to ensure that specified sensitive data is not leaked. It can also be used to help prevent data being mishandled or improperly accessed.

This Policy establishes the principles by which SDCCB will identify, protect and respond to the unauthorized disclosure of Protected Information by electronic means. The specific purposes of this Policy are to:

a. Protect Data-in-Motion (Data that is traversing the College Network or otherwise being transferred electronically and includes, but is not limited to, email, instant messages, ftp, and web traffic utilizing Information Technology Resources), Data-in-Use (Data that is being manipulated by a user, and includes, but is not limited to, transferring Data to a USB drive or copying, altering and/or pasting Data) and Data-at-Rest (stored or archived Data and includes, but is not limited to, Data stored on Information Technology Resources).
b. Authorize Security Administrators to take reasonable measures to secure Protected Information by using, among other techniques and methods, Data Loss Prevention (DLP) software and equipment to monitor, identify and block the unauthorized disclosure of Protected Information.

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
Regd. No. 90/SG
01.05.1955

c. Prescribe mechanisms that help to identify and address areas of high risk for the unauthorized release of Protected Information and the misuse of Data, applications, the Network and Computers.

d. Reduce the risk of exposure and identity theft or other personal identifying information is used as a primary identifier and to provide for the consistent, secure and proper management of such information.

Acceptable Use

Please refer Part II section 3 of the IS Policy.

Content Protection

SDCCB shall protect the following contents from Data Leakage / Loss.

- Bank's Confidential Intellectual Property
- Customer Credit / Debit Card Information
- Financial Data
- Personally, Identifiable Information (PII)

The Policy includes the following enforcement:

- **Alert & Log** – DLP responses may not always require actions to data found in violation of policy. Notification may be sufficient to report to a user, the data owner, or an administrative/supervisory resource that a file or other data was detected through a policy detection action. This action will not disrupt workflows.
- **Reroute and Pass, or Block/Quarantine** – Policy may require that data shall not be allowed to move to an intended destination, triggering an enforcement action that blocks transit by either stopping, or quarantining a file. This type of action may disrupt legitimate workflows and is highly dependent upon the detection engine; therefore, testing of the provider's DLP detection capabilities is essential.
- **Delete** – Policy may require that a file be deleted. Legalities must be considered prior to any data/file deletion.
- **Encrypt** – Unprotected information may trigger an enforcement action to encrypt the data. Encryption may occur in several ways, and DLP system should be capable of integrating with a suitable range of encryption methods. Encryption can avoid disruption of workflows for information by providing recipients with encrypted copies of a file. However, encryption must align with encryption policy. Once information is encrypted, it may not appear again in violation of policy, but users of that now-encrypted data must be able to access it and use it according to the defined policy. Below guidelines shall be considered for enforcement through encryption:

THE SUNDARGARH DIST. CENTRAL CO.OP. BANK LTD.
Regd. No.
01.06.1955

- Interoperable encryption should be used to ensure that encrypted data could be decrypted across different platforms and applications through standard APIs and interfaces.
- Encryption keys should be held by the data owners or possibly delegated to trusted third parties (preferably not the cloud provider who stores the data).
- Data should be encrypted before it moves to the Internet / cloud and attached with appropriate usage permissions. However, prior to encryption, the DLP system may inspect the databased on policy, and then allow the data to pass to the cloud.
- The data owner should be able to specify the policy governing access and use of the data (e.g., which identities/roles can use which data objects for which purposes).

Compliance & Non-Compliance with Policy

Compliance with this policy is mandatory for all employees of SDCCB, including contractors and executives. SDCCB DIT will monitor compliance and non-compliance with this policy and report to the Executive team as appropriate.

Non-compliance includes but is not limited to:

- Failure to adhere to the Policy
- Failure to attend training sessions regarding acceptable and sensitive data usage.

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
Regd. No.
01.06.1955

8.3. Risk Management Policy

In line with the Company's objective towards increasing stakeholder value, a risk management policy has been framed, which attempts to identify the key events / risks impacting the business objectives of the Company and attempts to develop risk policies and strategies to ensure timely evaluation, reporting and monitoring of key business risks.

SDCCB risk management approach shall comprise primarily of three components:

- Risk Governance
- Risk Identification
- Risk Assessment and Control

Risk Governance:

- The functional heads of SDCCB shall be responsible for managing risk on various parameters and ensure implementation of appropriate risk mitigation measures.
- The Risk Management Committee shall provide oversight and reviews the risk management policy from time to time.

Risk Identification:

External and internal risk factors shall be managed as identified in the context of business objectives.

Risk Assessment and Control:

Risk Assessment and Monitoring shall comprise the following:

- Risk assessment and reporting
- Risk control
- Capability development

SDCCB risk management shall Include but not limited to:

- **Asset and Risk Identification** - Identifying critical information assets and subjecting them to IT specific risk assessments.
- **Identifying the threats and vulnerabilities** - Assessing exposure to a list of common threats and vulnerabilities.
- **Business Impact Assessment & Risk Assessment** - Maintaining risk registers, which include information security and operational risks. Implementing technical, policy, Business Continuity and Management initiatives to reduce or eliminate identified risks.

- Calculating the resulting risk exposure and impact.
- Agreeing controls, activities and processes to treat risks
- Implementing risk treatment initiatives and controls

Compliance & Non-Compliance with Policy

Compliance with this policy is mandatory for all employees of SDCCB, including contractors and executives. SDCCB DIT will monitor compliance and non-compliance with this policy and report to the Executive team as appropriate.

Non-compliance includes but is not limited to:

- Failure to adhere to the Policy
- Failure to attend User Awareness Trainings.

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
Regd. No. 30/SG
01.06.1955

8.4. Forensics & Incident Analysis Policy

Digital forensics seeks to capture digital evidence such that the forensic integrity of the data is preserved for legal purposes. Forensic tools and techniques shall be used in incident handling and to respond to an event by investigating suspect systems, gathering and preserving evidence, reconstructing events, and assessing the current state of an event.

Forensics Process shall comprise of the following phases:

- **Collection** - The first phase in the process is to identify, label, record, and acquire data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data. Collection is typically performed in a timely manner because of the likelihood of losing dynamic data such as current network connections, as well as losing data from battery-powered devices (e.g., cell phones, PDAs).
- **Examination** - Examinations involve forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data.
- **Analysis** - The next phase of the process is to analyse the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.
- **Reporting** - The final phase is reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process. The formality of the reporting step varies greatly depending on the situation.

SDCCB Forensics and Incident Handling team shall comprise of designated members from the IS Organization, Network and Security Administration Staff. If any forensics activity is required to be carried out upon reporting of an incident, a proper investigation procedure shall be followed to carry out the forensics.

Compliance & Non-Compliance with Policy

Compliance with this policy is mandatory for Information Security Organization, Network and Security Administrators, including contractors and executives, who will be involved in the Incident Management. SDCCB DIT will monitor compliance and non-compliance with this policy and report to the Executive team as appropriate.

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
Regd. No.
[illegible]
[illegible]1953

9. Formats

9.1. IT Asset Register

ASSET REGISTIER

Asset ID	Asset Name	Asset Type	Asset Classification	Location	Asset Owner	Assigned to	Confidentiality	Integrity	Availability	Remarks

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD.
Regd. No.
01.06.1955

9.2. Risk Assessment Template

RISK ASSESSMENT MATRIX – THE SUNDARGARH DISTRICT CENTRAL CO-OPERATIVE BANK LTD. (Hybrid Approach)

Item No	Asset	Threat	Vulnerability	Vulnerability Rating	Likelihood	Impact	Risk Value	Existing Control	Financial Loss	Treatment	Revised Risk Value		
											Likelihood	Impact	Risk Value
									*				
									*				
									*				
									*				
									*				
									*				
									*				
									*				
									*				
									*				
									*				
									*				
									*				
									*				
									*				
									*				

*Financial Loss Column may be used as appropriate.

THE SUNDARGARH DIST. CENTRAL CO. BANK LTD.
Regd. No.
90/SG
01.06.1955

9.3. Incident Report Format

(This form can be filled up on hardcopy, online or sent by email to Service Desk)

For User Reporting Incident:

Username & Employee Name	
Location i.e., Dept or Place of Incidence	
Incident Date & Time	
Reporting Date	
Equipment or Service Details	
Contact Number of User who reported	
Incidence Domain (Operating System, Database, Application, Network etc.)	

Incident Description by User (Give details of activity that triggered the incident, error messages etc and expected result)

For use of DIT / Service Desk:

Incident Number and Severity	
Date and Time of Receipt of Incident	
Incident Date & Time	
Check Incident Known Errors	Yes / No
First Level of Action Possible	Yes / NO
Temporary Solution/ Resolving Action	
Referred to Technical Support Team	Name & Contact Number
Date and Time of Response from TS Group	
Date and Time of Responding to User	
Escalation to Second Level – Date & Time	
Date and Time of Final Resolution	
Details of Solutions and Action Suggested	
Date of Updation to Known Error Database	
RFC to Change Management Team	
Updation to Configuration Management	

THE SUNDARGARH DIST. CENTRAL CO-OP. BANK LTD. 1955

Escalation to Problem Management	
Closure of Incident – Date and Time	

Prepared By		Reviewed By	
Signature		Signature	

9.4. Change Request Format

CHANGE REQUEST FORMAT

PROJECT NAME		CHANGE REQUEST NUMBER
PROJECT MGR.		

CHANGE REQUEST			
REQUESTER NAME		DATE OF REQUEST	
REQUESTER CONTACT		PRIORITY	
ITEM TO BE CHANGED			
CHANGE DESCRIPTION			

PREDICTED TIMELINE	ESTIMATED COSTS

CHANGE EVALUATION			
EVALUATOR NAME		DATE OF EVAL	
EXPECTED OUTCOME			
WORK REQUIRED			

AREA OF IMPACT	IMPACT DESCRIPTION	IMPACT LEVEL
SCOPE		
SCHEDULE		
COST		
QUALITY		

THE SUNDARGARH DISTRICT CENTRAL COOPERATIVE BANK LTD. ★ Regd. No. 90/55 1.6.1955

CHANGE REVIEW / APPROVAL			
REVIEWER NAME		STATUS	ACCEPTED / REJECTED
REVIEWER SIGNATURE		DATE OF REVIEW	
ADDITIONAL COMMENTS			

CHANGE TRACKING			
TRACKING AGENT		LAST UPDATED	
TRACKING AGENT SIGNATURE		VERSION NUMBER	
ADDITIONAL COMMENTS			

File original Change Request Form in the Project File and update the Change Register. Pass copy to Sponsor (if required)