UC Inclusive Credit Private Limited (UCIC)

INFORMATION TECHNOLOGY POLICY

Current Version No: 6.0
Current Version Approval Date: 8th September 2024
Current Version Effective Date: 1st October 2024

Table of Contents

CHAPTER 1: IT Governance Framework

Introduction

The Reserve Bank of India (RBI) issued circulars RBI/DNBS/2016-17/53 (Master Direction DNBS.PPD.No.04/66.15.001/2016-17) on June 8, 2017, and RBI/2023-24/107 (Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices) on November 7, 2023. These Directions provide a framework for IT governance, IT Policy, Information & Cyber Security, IT Operations, IS Audit, Business Continuity Planning and IT Services Outsourcing for entities regulated by RBI.

1. Purpose

The purpose of this Policy is to establish a structure for managing information and IT resources in line with industry best practices, legal regulations, and the specific requirements set forth by the Reserve Bank of India (RBI), in a time bound manner

2. Scope

This framework and policy apply to all IT and Information Security operations, activities, personnel (including employees, interns, and trainees), and third-party service providers, clients or customers, potential clients or customers and other parties associated with UC Inclusive Credit Pvt Ltd (UCIC/ the Company).

3. Objectives

The objectives of this policy are to ensure:

- Alignment of IT strategy with the accomplishment of UCIC's business objectives.
- Integration of Information Security and Privacy Risk management into business processes.
- Effective and efficient use of IT resources.
- Robust Business Continuity and Disaster Recovery Management.
- Compliance with applicable laws, standards, and regulatory requirements.

4. IT Governance Framework

The key focus areas of IT Governance at UCIC include strategic alignment, risk management, resource management, performance management, and Business Continuity/Disaster Recovery Management. UCIC shall implement a robust IT Governance Framework based on these focus areas, which:

- Specifies the governance structure and processes necessary to meet UCIC's business/strategic objectives.
- Outlines the roles and responsibilities, including authority, of the Board of Directors (Board)/Board level Committee and Senior Management.
- Incorporates adequate oversight mechanisms in a time bound manner to ensure accountability and the mitigation of IT and cyber/information security risks.

5. Role of the Board of Directors

The Board of Directors shall approve strategies and policies related to IT, Information Assets, Business Continuity, Information Security, and Cyber Security (including Incident Response and Recovery Management/Cyber Crisis Management). These strategies and policies shall be reviewed at least annually by the Board.

6. IT Strategy Committee of the Board

The IT Strategy Committee (ITSC) shall be constituted by the Board. The Committee shall be responsible for guiding the preparation of UCIC's IT strategy and ensuring that the IT Strategy aligns with the overall strategy of UCIC towards the accomplishment of its business objectives. The committee members shall meet quarterly to make strategic IT decisions.

6.1. ITSC Members Constitution

6.1.1. A minimum of three directors as members;
6.1.2. The Chairperson of the ITSC must be an independent director possessing significant expertise in overseeing and guiding information technology initiatives;
6.1.3. All members must demonstrate technical competence.

6.2. ITSC Terms of Reference:

6.2.1. Will Ensure that UCIC has an effective IT strategic planning process in place.
6.2.2. Guide in the preparation of IT Strategy and ensure alignment with UCIC's overall strategy towards achieving business objectives.
6.2.3. Verify that the IT Governance and Information Security Governance structure fosters accountability, is effective and efficient, has adequate skilled resources, well-defined objectives, and clear responsibilities.
6.2.4. Ensure that UCIC has processes for assessing and managing IT and cybersecurity risks.
6.2.5. Confirm that budgetary allocations for IT, including IT security and cyber security, are appropriate for UCIC's IT maturity, digital depth, threat environment, and industry standards, and are used effectively.
6.2.6. Review, at least annually, the adequacy and effectiveness of UCIC's Business Continuity Planning and Disaster Recovery Management.

7. IT Steering & Information Security Committee (ITSIC)

7.1. ITSIC Members Constitution:

7.1.1. UCIC shall establish an IT Steering Committee with representation at the Executive level from IT and business functions.

7.2. ITSIC Terms of Reference:

7.2.1. Execution of the IT Strategy approved by the Board.
7.2.2. Effective and efficient functioning of IT/IS and their support infrastructure.
7.2.3. Implementation of necessary IT risk management processes, fostering a culture of IT risk awareness and cyber hygiene practices.
7.2.4. Robust cyber security process for UCIC.
7.2.5. Contribution of IT to productivity, effectiveness, and efficiency in business operations.
7.2.6. Assisting the ITSC in strategic IT planning, oversight of IT performance, and aligning IT activities with business needs.
7.2.7. Overseeing processes for business continuity and disaster recovery.
7.2.8. Ensuring the implementation of a robust IT architecture meeting statutory and regulatory compliance.
7.2.9. Periodically updating the ITSC and Management on the activities of the IT Steering Committee.

8. Head of IT Function

UCIC shall appoint a sufficiently senior-level, technically competent, and experienced official in IT-related aspects as Head of IT Function. The Head of IT Function shall be responsible for:

8.1.1. Ensuring alignment of IT projects/initiatives with UCIC's IT Policy and IT Strategy.
8.1.2. Maintaining an effective organizational structure to support IT functions.
8.1.3. Implementing an effective disaster recovery setup and business continuity strategy/plan.

The Head of IT Function shall ensure effective assessment, evaluation, and management of IT controls and IT risk, including the implementation of robust internal controls to secure UCIC's information assets and comply with internal policies, regulatory, and legal requirements on IT-related aspects.

9. Risk Management

9.1. **Risk Assessment :** UCIC shall conduct regular risk assessments on each information asset, existing systems, third parties, and partners to identify and assess IT and data-related risks. These assessments will cover areas such as cybersecurity, data breaches, operational disruptions, and compliance risks and shall take steps to adequately tackle cyber-attacks including phishing, spoofing attacks and mitigate their adverse effects. UCIC shall ensure that all staff members and service providers comply with the extant information security and acceptable-use policies as applicable to them.

9.2. **Business Continuity and Disaster Recovery:** A robust Business Continuity and Disaster Recovery (BCDR) plan shall be in place to ensure the uninterrupted operation of critical IT systems in case of disasters or disruptions. Regular testing and updates of the BCDR plan shall be conducted to maintain its effectiveness. The detailed BCDR Section covers the details

10. Performance Management

Performance management shall be an integral part of the overall IT governance and management. All employees will undergo a performance evaluation as per the human resource performance management policy. A similar performance evaluation shall be conducted on critical IT systems with clearly defined Key Result Areas, outcomes, shortfalls if any in expected performance, and a plan of action to bridge the identified gap.

11. Vendor Management

11.1. **Vendor Selection:** Vendor selection criteria shall include security risk assessments, regulatory compliance, and service-level agreements. It shall strictly adhere to the organization-wide Vendor Management Policy. Department-wise SOPs shall be defined for vendor selection and due diligence.

11.2. **Vendor Non-Disclosure Agreement** (NDA) shall be entered into between the potential vendor and UCIC to safeguard mutual interests.

11.3. **Vendor Audits and Compliance:** Regular vendor audits shall be conducted to ensure compliance with contractual and security requirements. Vendors found non-compliant may face penalties or termination of contracts.

12. IT Project Management

UCIC shall follow standardized project management processes, including initiation, planning, execution, monitoring, and closure. All IT projects must align with the organization's strategic goals and objectives.

13. Change Management

A well-defined change management process shall be in place to assess and implement changes to IT systems. All changes shall be thoroughly tested and approved before deployment to minimize disruptions.

14. Compliance and Reporting

14.1. **Regulatory Reporting:** UCIC is committed to meeting all regulatory reporting requirements imposed by RBI and other relevant authorities. The Compliance Team shall ensure timely and accurate reporting.

14.2. **Internal Audits and Compliance Checks:** Internal audits shall be conducted regularly to assess compliance with IT policies and regulatory requirements. Audit findings that are outside of the acceptable risk shall be addressed promptly, and corrective actions shall be implemented.

15. Training and Awareness

15.1. **Training Curriculum:** A comprehensive training curriculum shall be developed to promote awareness amongst employees of the Company on its IT policies, security practices, and compliance requirements. All employees shall strive to attend such mandatory trainings.

15.2. **Employee Awareness:** Regular awareness programs shall be conducted to keep employees informed about the latest cybersecurity threats and best practices. Employees are encouraged to report any suspicious activity promptly.

16. Document Management

Documents related to IT policies, procedures, and project documentation shall be stored securely and easily retrievable. Version control will be maintained for all documents. Document shall be retained for such duration as specified by the concerned regulatory authority.

17. E-signatures

UCIC shall strive to use Digital signatures (through DSC tokens) or Aadhar based signatures or other e-signatures to protect the authenticity and integrity of important electronic documents and also for high value fund transfer.

18. Review and Revision

This IT Policy will undergo regular reviews to ensure its relevance and effectiveness. The review schedule shall be determined by the IT Steering Committee, which is no later than a year from the previous approval date. The IT Steering Committee and relevant department heads are responsible for initiating policy revisions, which shall be approved by the Board. Employees are encouraged to provide genuine feedback for continuous improvement.

CHAPTER 2: Information and Cyber Security Policy

1. Purpose

This Policy is framed in compliance to Master Direction DNBS.PPD.No.04/66.15.001/2016-17 of RBI dated June 08, 2017 on Information Technology Framework for the NBFC Sector, that are expected to enhance safety, security, efficiency in processes leading to benefits for NBFCs and their customers. The focus of this IT framework is on IT Governance, IT Policy, Information & Cyber Security.

2. Policy Statement

UC Inclusive Credit Private Limited ("UCIC/ the Company") shall take all necessary steps to protect information and information infrastructure in internet/cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation from relevant external bodies both Private, Public and the Government.

The objective of this Policy is to proactively identify the Cyber threats and the risks manifested in information infrastructure and manage, mitigate, avoid, divert, transfer or accept the risks as per the risk appetite of the organization.

3. Scope

This policy applies to all data collected, processed and stored by UCIC during its business operations, including co-lending activities, and extends to its all trainees, employees, employers, Board Members, Observers, Advisors, Consultants, Auditors, contractors, partners, customers and any other person who either inadvertently or in the course of its dealings with the Company, obtains or collect any restricted personal data from the database of the Company . They shall be collectively be termed as "Users" under this policy.

4. Information Security (IS)

Information is an asset to the Company and Information Security (IS) refers to the protection of these assets in order to achieve organizational goals. The purpose of IS is to control access to sensitive information, ensuring the access and use only by legitimate Users so that data cannot be used or compromised without proper authorization. The Company shall ensure confidentiality, integrity, availability and authenticity of data managed by it.

5. Key Components of IS Policy:

18.1. **Identification and Classification of Information Assets:** Maintain a detailed inventory of all information assets with clear identification.

18.2. **Segregation of Functions:** Separate the duties of the Security Officer/Group (responsible for information systems security) from the Information Technology division (responsible for implementing computer systems). The Company shall ensure adequate staffing, skills, and tools for the information security function and clearly segregate responsibilities for system administration, database administration, and transaction processing.

18.3. **Role-Based Access Control:** Access to information should be based on well-defined user roles (system administrator, user manager, application owner etc.), NBFCs shall avoid dependence on one or few persons for a particular job. There should be clear delegation of authority for right to upgrade/change user profiles and permissions and also key business parameters (eg. interest rates) which should be documented.

18.4. **Personnel Security :** UCIC shall implement checks and balances for authorized application owners/users who have extensive knowledge of financial institution processes and conduct rigorous background checks and screenings for personnel with privileged access (e.g., system administrators, cybersecurity personnel).

18.5. **Physical Security:** The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. The Company needs to create a secured environment for physical security of IS Assets such as secure location of critical data, restricted access to sensitive areas like data center etc.

18.6. **Maker-Checker Principle:** UCIC shall implement a system where at least two individuals are required to complete each transaction to reduce errors and ensure information reliability.

18.7. **Incident Management:** The IS Policy should define what constitutes an incident. The Company shall develop and implement processes for preventing, detecting, analysing and responding to information security incidents.

18.8. **Audit Trails:** The Company shall ensure that audit trails exist for IT assets satisfying its business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution. If an employee, for instance, attempts to access an unauthorized section, this improper activity should be recorded in the audit trail.

18.9. **Public Key Infrastructure (PKI):** UCIC may increase the usage of PKI to ensure data confidentiality, access control, data integrity, authentication, and non-repudiation.

18.10. **Cyber Security:** The cyber security policy outlines strategies to combat cyber threats based on the complexity of their business and acceptable risk levels. This policy should be reviewed regularly to ensure security concerns are addressed promptly and must be approved by the board and clearly define the approach to managing cyber threats.

6. Components of the Cyber Security Policy

18.11. **Vulnerability Management:** A vulnerability can be defined as an inherent configuration flaw in an organization's information technology base, whether hardware or software, which can be exploited by a third party to gather sensitive information regarding the organization. Vulnerability management is an ongoing process to determine the process of eliminating or mitigating vulnerabilities based upon the risk and cost associated with the vulnerabilities.

18.12. **Cyber Security Preparedness Indicators:** Company shall develop indicators to measure cyber resilience and conduct regular compliance checks and audits. It should be ensured that stakeholders, including employees, are aware of these indicators.

18.13. **Cyber Crisis Management Plan (CCMP):** CCMP should address four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment.

18.13.1. Company need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond / recover / contain the fall out and must be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks.

Among other things, UCIC shall take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

7. Sharing of information on cyber-security incidents with RBI

The Company is required to report all types of unusual security incidents as specified in Annex I of the Master Directions including both successful and attempted incidents. RBI's latest template for reporting will be used.

8. Cyber-security awareness among stakeholders / Top Management / Board

It should be realized that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require a high level of awareness among staff at all levels. Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarization may be organized. The Company should proactively promote, among their Clients, vendors, Lenders and other service providers and other relevant stakeholders an understanding of their cyber resilience objectives, and require and ensure appropriate action to support their synchronized implementation and testing.

9. Digital Signatures

UCIC has procured Digital Signature Certificates (DSC) for its Authorised persons/ and is intended to be used for Corporate Banking, and other governmental websites like MCA, Income Tax, DGFT Website authentication, PF, GST, NeSL and other regulatory websites.

10. IT Risk Assessment

Company must undertake a comprehensive risk assessment of their IT systems at least on a yearly basis. The assessment should make an analysis on the threats and vulnerabilities to the information technology assets of the NBFC and its existing security controls and processes. The outcome of the exercise should be to find out the risks present and to determine the appropriate level of controls necessary for appropriate mitigation of risks. The risk assessment should be brought to the notice of the Chief Risk Officer (CRO), and the Board and should serve as an input for Information Security auditors.

11. Requirements with regards to Mobile Computing Policy

The mobile computing policy applies to all employees and staff provided with a company laptop or portable electronic device. It is the employee's responsibility to take proper care of the laptop computer / PED (Portable Electronic Device), data and accompanying software while using the same.

12. Social Media Risks

12.1. Usage of Social Media and restricted sites within UCIC network is prohibited, unless approved specifically.

12.2. Employees are personally responsible for the content they publish on- line, whether in a blog, social computing site or any other form of user- generated media.

12.3. Employees are not authorised to publish or discuss the following on Social Media:

- **12.3.1.** UCIC's confidential or other proprietary information
- **12.3.2.** To cite or reference Customers, partners or suppliers without their approval
- **12.3.3.** Any Unpublished Confidential or Price Sensitive Information pertaining to Customers, Clients, partners or suppliers without their written approval
- **12.3.4.** To use UCIC's logos or trademarks unless approved to do so.
- **12.3.5.** Anything libelous and slanderous against any person/ entity, in official capacity
- **12.3.6.** Any hate speech/ statement against any entity, person, caste, creed, religion or belief and nationality

13. IT Enabled Management Information System

UCIC shall put in place MIS that assist the Top Management as well as the business heads in decision making and also to maintain an oversight over operations of various business verticals and Supervisory requirements. With robust IT systems in place, UCIC may have inter alia the following as part of an effective system generated MIS:

13.1. A dashboard for the Top Management summarising financial position vis-à-vis targets. It may include information on trend on returns on assets across categories, major growth business segments, movement of net-worth, regulatory and statutory compliances, various trackers and e-tools for generating various reports.

13.2. System enabled identification and classification of Special Mention Accounts and NPA as well as generation of MIS reports in this regard.

13.3. The MIS should facilitate pricing of products, especially large ticket loans.

13.4. The MIS should capture regulatory requirements and their compliance.

13.5. Financial Reports including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, etc. (also regulatory compliance at transaction level)

13.6. Reports relating to treasury operations.

13.7. Fraud analysis- Suspicious transaction analysis, embezzlement, theft or suspected money-laundering, misappropriation of assets, manipulation of financial records etc. The regulatory requirement of reporting fraud to RBI should be system driven.

13.8. Capacity and performance analysis of IT security systems

13.9. Incident reporting, their impact and steps taken for non -recurrence of such events in the future.

14. IS Audit

14.1. **Policy for Information System Audit (IS Audit)**: The objective of the IS Audit is to provide an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the organization's IT infrastructure. IS Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local and wide area networks, physical and information security, telecommunications etc.

14.2. **Coverage:** IS Audit should cover effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up. IS Audit

should also evaluate the effectiveness of business continuity planning, disaster recovery set up and ensure that BCP is effectively implemented in the organization. During the process of IS Audit, due importance shall be given to compliance of all the applicable legal and statutory requirements.

14.3. **Personnel:** UCIC can conduct IS Audits using internal teams or engage external agencies with IT/IS audit expertise when internal skills are insufficient. Auditors need a balanced mix of technical skills and understanding of legal and regulatory standards. Independence from NBFC management is crucial for both internal and external auditors to ensure impartial assessments.

14.4. **Periodicit**y: The frequency of IS audits should ideally align with the size and operations of the NBFC, typically conducted at least annually. Conducting the IS Audit before the statutory audit allows auditors to incorporate IS Audit findings into their reports promptly.

14.5. **Reporting:** The framework should clearly prescribe the reporting framework, whether to the Board or a Committee of the Board viz. Audit Committee of the Board (ACB)

15. Compliance

The management of the Company is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during the IS Audit. Responsibilities for compliance/sustenance of compliance, reporting lines, timelines for submission of compliance, and authority for accepting compliance should be delineated in the framework.

Computer-Assisted Audit Techniques (CAATs): UCIC shall adopt a proper mix of manual techniques and CAATs for conducting IS audits. CAATs may be used in critical areas (such as detection of revenue leakage, treasury functions, assessing the impact of control weaknesses, monitoring customer transactions under AML requirements and generally in areas where a large volume of transactions are reported), particularly for critical functions or processes having financial/regulatory/legal implications.

16. Grievance Redressal

UCIC is committed to addressing grievances in a timely and efficient manner. For queries or concerns, you can write to **grievanceredressal@ucinclusive.com** and the team will respond to the same. The responsibilities of DPO are carried out by the head of Information Security.

17. Amendments

UCIC reserves the right to amend this policy at any time. The revised policy will be made available on our official website and communicated to data subjects where applicable.

CHAPTER 3: Data Privacy and Protection Policy

1. Purpose and Scope

This Data Privacy and Protection Policy outlines our commitment to managing, protecting, and processing personal data in alignment with the Digital Personal Data Protection (DPDP) Act, 2023 and relevant guidelines issued by Reserve Bank of India. The company also takes guidelines from CERISE and Client Protection Pathways frameworks.

This policy applies to all personal data collected, processed, and stored by UC Inclusive Credit Private Limited (UCIC/ the Company) during the course of its business operations, and extends to its all trainees, employees, employers, Board Members, Observers, Advisors, Consultants, Auditors, contractors, partners, customers and any other person who either inadvertently or in the course of its dealings with the Company, obtains or collect any restricted personal data from the database of the Company.

2. Data Privacy and Protection Principles

UCIC shall strictly adhere to the data protection principles as below:

2.1. **Lawfulness, Fairness, and Transparency:** UCIC is committed to processing all personal data in a lawful, fair, and transparent manner. UCIC shall ensure that every data processing activity is backed on a legal basis, such as consent or a contractual obligation. Transparency shall be maintained by providing clear, accessible, and understandable information to data subjects about how their data would be used, and ensuring their rights are easily exercised.

2.2. **Purpose Limitation:** UCIC shall collect personal data strictly for identified, explicit, and legitimate purposes. Data shall not further processed in any manner that is incompatible with those purposes. UCIC shall clearly inform the data subjects about these purposes at the point of collection to ensure informed consent and understanding.

2.3. **Data Minimization:** UCIC shall adhere to the principle of data minimization, ensuring that only data that is necessary for the intended purposes is collected and processed. This minimizes privacy risks and ensures that no excessive data is retained.

2.4. **Accuracy & Authenticity:** Accuracy of personal data is paramount. UCIC shall have mechanisms in place to ensure that inaccurate, incomplete, obsolete or outdated data is amended or deleted promptly. Data subjects are encouraged and facilitated to update their data periodically to ensure that it remains accurate and current.

2.5. **Storage Limitation:** UCIC shall retain personal data for a limited period, only as long as necessary to fulfill the purposes for which the data was collected or to comply with legal, regulatory or policy requirements. A data retention procedure shall be followed to ensure that data is securely deleted, anonymized, or archived after the retention period.

2.6. **Integrity and Confidentiality:** Personal data shall be protected by suitable security measures designed to prevent unauthorized access, alteration, disclosure, or destruction. These include technological, organizational, and procedural measures such as encryption, access controls, using authentic anti malware/ virus software or programmes and staff training to ensure the confidentiality and integrity of data.

2.7. **Accountability:** UCIC are committed to being accountable for its data protection practices. UCIC shall have internal policies, procedures, and controls in place to ensure and demonstrate compliance with data protection principles. These include regular audits and training.

3. Data Collection and Processing

UCIC is committed to:

3.1. Informing individuals regarding their data's collection and processing.

3.2. collecting data only for specific and legitimate purposes.

3.3. Ensuring data accuracy and updating it as necessary.

3.4. Storing data securely to maintain its confidentiality.

4. Data Subject Rights

UCIC respect data subject rights including:

4.1. Access to personal data
4.2. Rectification of inaccurate data
4.3. Restricting data processing
4.4. Data portability
4.5. Objection to processing.
4.6. Not being subject to automated decision-making

5. Security

UCIC shall have security measures to protect personal data, including:

5.1. Assigning the appropriate classification for Personally Identifiable Information data
5.2. Implementing clearly defined role and function-based access controls
5.3. Encrypting data during transmission and at rest.
5.4. Masking and redacting PI as per requirements to ensure enough access control and protection.
5.5. Regularly monitoring and testing security protocols.
5.6. Establishing incident response and breach notification procedures.
5.7. Identification and Classification of Information Assets
5.8. For key personnel with intimate knowledge and access to systems a comprehensive background check and screening is to be initiated
5.9. The incident of Data breach or security breach if any needs to be defined and reported along with necessary steps to be taken to prevent such incidents in the future

6. Third-Party Processors

UCIC shall take steps to ensure that third-party processors adhere to the Company's data protection and privacy requisites.

7. Data Privacy Impact Assessments (DPIA)

DPIAs are conducted for processing operations that pose specific risks to data subjects' rights and freedoms and to assess the overall privacy impact that UCIC may have.

8. Training and Awareness

Employees shall receive periodic training as per the information security and privacy awareness policy.

9. Cookies

Third parties may place cookies on specific pages; UCIC shall not control their cookie usage. However, UCIC may use cookies at its website/ webpage to enhance user's/ visitor's experience. One may configure the browser to refuse or alert about cookies, but this may affect website functionality. The Website/ webpage of the Company shall exhibit following disclaimer before admitting any user/ visitor:

10. Website Disclaimer

UCIC use cookies to gives the users the best possible experience with ucinclusive.in. Some are essential for the site to function; others help the company understand how the users use the site, so the company can improve it. UCIC may also use cookies for targeting purposes. The website will provide option for the users to accept the cookie policy or exit the site.

11. Review and Revision

UCIC may, at its discretion, may make changes to this Privacy Policy to reflect updates in its business processes, upgrades in privacy standards and procedures, or to implement applicable legislative or regulatory changes.

Any such policy changes shall be effective from the date of posting the same on the Company's website, and notification of these changes shall be published on the website. This policy is subject to annual review or updates upon significant changes in data processing activities.

12. Contact Information

For queries or concerns, one can write to **grievanceredressal@ucinclusive.com** and the team should respond to the same within 7 working days.

CHAPTER 4: Outsourcing of Information Technology Services

1. Introduction

To ensure that our outsourcing arrangements are in line with regulatory requirements and do not compromise our ability to meet customer obligations or impede effective supervision, UCIC has adopted this Outsourcing Policy. This policy aligns with the Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023, and aims to provide clear guidelines for managing outsourcing risks effectively.

2. Scope

This Outsourcing Policy applies to all IT and ITeS outsourcing arrangements undertaken by UCIC. It encompasses existing contracts, as well as new outsourcing agreements, to ensure that all such activities comply with the relevant regulatory guidelines and internal risk management frameworks.

Specifically, this policy covers:

- IT infrastructure management, maintenance, and support (hardware, software, or firmware).
- Network and security solutions and maintenance (hardware, software, or firmware).
- Application development, maintenance, and testing.
- Services and operations related to data centers.
- Cloud computing services.
- Managed security services.
- Management of IT infrastructure and technology services associated with the payment system ecosystem.

3. Objectives

The primary objectives of this Outsourcing Policy are to:

3.1. Ensure compliance with the Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023.

3.2. Mitigate risks associated with the outsourcing of IT and ITeS activities.

3.3. Safeguard the interests of our customers by ensuring the integrity, security, and confidentiality of their information.

3.4. Ensure that outsourcing arrangements do not impede our ability to meet regulatory and supervisory requirements.

3.5. Provide a structured framework for the evaluation, selection, and management of third-party service providers.

4. Due Diligence on Service Providers

When evaluating or renewing an outsourcing arrangement for IT services, UCIC will perform thorough due diligence to ensure the service provider meets its obligations under the outsourcing agreement consistently.

Risk-Based Approach: UCIC will adopt a risk-based approach in conducting due diligence, considering various factors to assess the provider's capability.

Due Diligence Factors:

4.1. Qualitative Factors:

4.1.1. Experience and Competence: Past performance and ability to implement and support the IT activity throughout the contract period.

4.1.2. Reputation and Culture: Business reputation, compliance history, complaints, and any outstanding or potential litigations.

4.1.3. Conflict of Interest: Any potential conflicts of interest.

4.2. Quantitative Factors:

4.2.1. Financial stability and ability to meet commitments under adverse conditions.

4.2.2. Stability, security, internal controls, audit coverage, reporting procedures, data backup, business continuity, and disaster recovery plans.

4.3. Operational Factors:

4.3.1. Data Management: Capability to identify and segregate UCIC's data.

4.3.2. Employee and Sub-Contractor Due Diligence: Quality of due diligence performed on employees and subcontractors.

4.4. **Service Capacity:**

4.4.1. Ability to effectively service all customers while maintaining confidentiality.

4.5. Legal and Compliance Factors

4.5.1. Regulatory Compliance: Capability to adhere to regulatory and legal requirements related to IT outsourcing.

4.5.2. Information/Cyber Security: Risk assessment and data protection measures.

4.5.3. External Factors: Jurisdictional Environment: Political, economic, social, and legal factors in the service provider's operating jurisdiction.

4.5.4. Controls and Assurance:

4.5.5. Contractual Arrangements: Ensuring controls, assurance requirements, and contractual arrangements are in place to protect UCIC's data and access rights.

4.5.6. Enforcement Capability:

4.5.7. Agreement Enforcement: Ability to enforce agreements and protect rights related to data storage, protection, and confidentiality.

5. Independent Reviews and Market Feedback

Where possible, UCIC will seek independent reviews and market feedback to supplement its own assessments.

6. Legally Binding Agreement

For UCIC's outsourcing of IT services, it is essential to establish a legally binding written agreement that clearly defines the rights and obligations of both UCIC and the service provider. The agreement should address the critical nature of the outsourced task, associated risks, and strategies for managing those risks. It must be reviewed and vetted by UCIC's legal counsel to ensure enforceability and flexibility, allowing UCIC to retain adequate control and meet legal and regulatory obligations.

7. Risk Management Framework

UCIC shall set up a comprehensive Risk Management Framework for IT outsourcing, covering risk identification, measurement, mitigation, management, and reporting.

7.1. Documenting Risk Assessments:

7.1.1. All risk assessments will be documented with necessary approvals, aligning with the roles and responsibilities of the Board of Directors, Senior Management, and IT Function.

7.1.2. Periodic internal and external quality assurance reviews will be conducted as per Board-approved policy.

7.2. Confidentiality and Data Integrity

7.2.1. UCIC will ensure the confidentiality and integrity of customer data handled by service providers.

7.2.2. Access to data at UCIC's locations or data centers by service providers will be restricted to a need-to-know basis, with controls to prevent security breaches and data misuse.

7.3. Customer Trust and Data Security

7.3.1. To maintain public confidence and customer trust, UCIC will ensure the protection of customer information held by service providers.

7.3.2. Access to customer information by service provider staff will be limited to a need-to-know basis.

7.4. Cyber Incident Reporting

7.4.1. Service providers must report cyber incidents to UCIC without undue delay.

7.4.2. UCIC will report these incidents to the RBI within 6 hours of detection by the service provider.

7.5. Monitoring Control Processes

7.5.1. UCIC will review and monitor service providers' control processes and security practices to identify security breaches.

7.5.2. UCIC shall notify the RBI immediately in the event of a security breach or leakage of confidential customer information, adhering to RBI's instructions on Incident Response and Recovery Management.

8. Business Continuity and Disaster Recovery

The Company shall:

8.1. Ensure that the service providers to develop and establish a robust framework for documenting, maintaining and testing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) commensurate with the nature and scope of the outsourced activity as per extant instructions issued by RBI from time to time on BCP/ DR requirements.

8.2. In establishing a viable contingency plan, shall consider the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house in an emergency, and the costs, time and resources that would be involved.

8.3. In order to mitigate the risk of unexpected termination of the outsourcing agreement or insolvency/ liquidation of the service provider, the Company shall retain an appropriate level of control over their IT-outsourcing arrangement along with right to intervene, with appropriate measures to continue its business operations.

8.4. ensure that service providers are able to isolate the information, documents and records and other assets. This is to ensure that, in adverse conditions or termination of the contract, all documents, record of transactions and information with the service provider and assets of the shall be removed from the possession of the service provider, or deleted, destroyed or rendered unusable.

9. Monitoring and Control of Outsourced Activities

9.1. The Company shall have in place a management structure to monitor and control Outsourced IT activities. This shall include monitoring the performance, uptime of the systems and resources, service availability, adherence to service level agreement requirements, incident response mechanism, etc.

9.2. UCIC shall conduct regular audits of service providers with regard to the activity outsourced by it. Such audits may be conducted either by internal auditors or external auditors appointed.

9.3. The audits shall assess the performance of the service provider, adequacy of the risk management practices adopted by the service provider, compliance with laws and regulations, etc. The frequency of the audit shall be determined based on the nature and extent of risk and impact from the outsourcing arrangements. Reports on the monitoring and control activities shall be reviewed periodically by the IT Steering Committee and in case of any adverse development, the same shall be put up to the Board for information.

9.4. The Company shall ensure assurance on the controls and procedures required to safeguard data security at the service provider's end.

9.5. Periodic review of the financial and operational condition of the service provider to assess its ability to continue to meet its Outsourcing of IT Services obligations. The Company shall adopt risk-based approach in defining the periodicity. Such due diligence reviews shall highlight any deterioration or breach in performance standards, confidentiality, and security, and in operational resilience preparedness.

9.6. The Company shall ensure that the service provider grants unrestricted and effective access to a) data related to the outsourced activities; b) the relevant business premises of the service provider; subject to appropriate security protocols, for the purpose of effective oversight use by UCIC, their auditors, regulators and other relevant Competent Authorities, as authorised under law.

CHAPTER 5: Business Continuity Planning and Disaster Recovery

1. Introduction

Business Continuity Planning in UC Inclusive Credit Private Limited ("UCIC/Company") forms a part of an organization's overall Business Continuity Management (BCM) plan, which is the "preparedness of an organization", which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes, at an agreed level and limit the impact of the disaster on people, processes and infrastructure (includes IT); or to minimize the operational, financial, legal, reputational and other material consequences arising from such a disaster. Effective business continuity management typically incorporates business impact analyses, recovery strategies and business continuity plans, as well as a governance programme covering a testing program, training and awareness program, communication and crisis management program.

2. Purpose

The purpose of Business Continuity policy is to minimize the operational, financial, legal, reputational and other material consequences arising from a disaster

BCP forms a significant part of an organisation's overall Business Continuity Management plan, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. BCP shall be designed to minimise the operational, financial, legal, reputational and other material consequences arising from a disaster.

3. Scope

This policy manual applies to

3.1. All staff members working for UCIC who have access to the organization's and/or client's information.

3.2. All staff members, vendors and third-party employees who have access to UCIC's information processing systems and the data contained in them including PII (Personally Identifiable Information). This includes the data accessed by licensed third parties, which is in turn deployed to and used by their clients.

3.3. All stakeholders and interested parties who are relevant to the operations of UCIC.

4. Objectives

The policy has been developed with an objective:

4.1. To determine as how the institution will manage and control identified risks

4.2. To Allocate knowledgeable personnel and sufficient financial resources to implement the BCP

4.3. For the top management to annually review the adequacy of the institution's business recovery, contingency plans and the test results and put up the same to the Board.

4.4. For the top management to evaluate the adequacy of contingency planning and their periodic testing by service providers whenever critical operations are outsourced.

5. Components of a Business Continuity Plan

5.1. The Company shall further develop its IT Infrastructure, including a wide array of Backups and recovery mechanism to protect Company's and its clients' data from system crash, natural or man-made disasters, erroneous or accidental deletions or any other event that could damage data infrastructure or cripple critical business operations.

5.2. The Company shall also keep in place a system to prevent occurrence of man-made disasters to the best extent possible

5.3. The Company shall also have in place necessary backup sites for its critical business systems and arrangements for storage of data and important documents.

5.4. The Company shall ensure that all its critical assets are insured adequately.

5.5. The Committee shall also identify key individuals who will manage the process of recovery and restoration

5.6. The Company shall require its service providers to develop and establish a robust framework for documenting, maintaining, and testing business continuity and recovery procedures. The service provider shall periodically test the Business Continuity and Recovery Plan and occasionally conducts joint testing and recovery exercises. The IT Steering Committee shall evaluate the outcome of such tests and act accordingly.

5.7. In order to mitigate the risk of unexpected termination of the key outsourcing agreements or liquidation of any key service provider, the Company shall retain an appropriate level of control over their outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in its operations and services to its clients.

5.8. The Company shall implement a system that to retrieve all its assets, documents, records of transactions and other information given to the service provider, from their possession once the services are terminated due to any reason so that continuity of Company's business operations is not affected.

5.9. Also, the Company shall find means to delete, destroy or render the assets unusable, in relation to the assets which are of no or little use to the Company. Before deletion/ destruction of any assets, the Company shall ensure back up of relevant information, if so required.

5.10. The Company shall have the option of alternate service providers and would be able to bring the outsourced activity back in-house in case of an emergency.

5.11. The aforesaid action plans should also be tested by the Company on an occasional basis. The results of the same along with the gap analysis should be placed by the IT Steering Committee annually before the Board for their direction.

5.12. The Company, along with preservation and protection of the security (as set out in detail above), also ensures confidentiality of customer information in the custody or possession of the service provider.

6. Testing of a Business Continuity Plan

Business Continuity plans shall be tested on an annual basis to determine the effectiveness of the plan and UCIC's readiness to execute the plan

6.1. Classroom exercises shall be conducted where a walkthrough of crisis scenarios and corresponding response plan is discussed with each member of the crisis management team.

6.2. The plan can also be tested by simulating a disruption and ensuring that the controls work as expected.

7. Disaster Recovery Management

7.1. Periodicity of DR drills for critical systems shall be at least on a half-yearly basis and for all other systems at least on a yearly basis. Any major issues observed during the drill shall be resolved and tested again, to ensure successful conduct of drill before the next cycle. The DR testing shall involve switching over to the DR/ alternate site and thus using it as the primary site for sufficiently longer period where usual business operations of at least a full working day (including Beginning of Day to End of Day operations) are covered.

7.2. UCIC shall document recovery strategies / details of the actions that the teams will take in order to continue or recover prioritized activities within predetermined timeframes and to monitor the effects of the disruption and the organization's response to it.

7.3. The company shall document on communicating internally and externally to relevant interested parties, including what, when, with whom and how to communicate.

7.4. Shall Backup data and periodically restore such backed-up data to check its usability. The integrity of such backup data shall be preserved along with securing it from unauthorised access.

7.5. In a scenario of non-zero RPO, shall have a documented methodology for reconciliation of data, while resuming operations from the alternate location.

7.6. The Company shall ensure that the configurations of servers, network devices, other products and deployed security patches at the DC and DR (DC refers to primary data centre for a given application/ system and DR its Disaster Recovery site/ alternate site) are identical.

7.7. Relevant personnel shall be trained on business continuity and disaster recovery plans and informed about their roles and responsibilities.

7.8. Documentation of the BCP/DR plans shall be maintained (including off site as necessary) to ensure it is accessible when the business continuity plan or the disaster recovery plan has to be invoked.

7.9. BCP/DR plans shall also consider vendors/suppliers/third parties as part of establishing, documenting, evaluation/testing and maintaining the BCP/DR plans

8. Updates and Review

UCIC shall update its BCM Policy whenever there is a material change to its operations, structure, business or location. In addition, the BCP of various functions shall be reviewed annually or as and when required to incorporate changes in its operations, structure, business, or locations.