SANKALP
Capital Private Limited

IT Policy

1. Introduction

Reserve Bank of India vide its circular RBI/DNBS/2016-17/53 (Master Direction DNBS. PPD. No.04/66.15.001 / 2016-17) of June 8, 2017 has given guidelines for Information Technology Framework for the NBFC sector ("Guidelines"). These Guidelines aim to enhance safety, security, efficiency in processes leading to benefits for NBFCs and their customers. NBFCs, pursuant to these Guidelines, are required to conduct a formal gap analysis between their present status and stipulations as set out in the Guidelines and put in place a time-bound action plan to address the gap.

This IT Framework falls within the scope of Section B of the Guidelines i.e. NBFCs with asset size of below INR 500 crores (Indian Rupees Five Hundred Crores only).

IT governance is an integral part of corporate governance of SANKALP CAPITAL PRIVATE LIMITED (Sankalp), and effective IT governance is the responsibility of the board of directors of Sankalp ("Board") and its executive management. Sankalp has designated a Head of Technology as the Chief Technology Officer ("CTO") of its IT operations and the Board exercises oversight on the CTO. The CTO ensures implementation of this IT Framework which, inter alia, includes (i) Security aspects; (ii) User Role; (iii) Information Security and Cyber Security; (iv) Business Continuity Planning Policy; (v) Back-up Data. For the purpose of effective implementation of this IT Framework, the CTO shall ensure technical competence at senior/middle level management of Sankalp. The CTO is also responsible for periodic assessment of the IT training requirements to ensure the availability of sufficient, competent and capable human resources in Sankalp.

A. Security Aspects

(i) Password Policy

All users are responsible for keeping their passwords secure and confidential. The password credentials of the users must comply with the password parameters ("Complexity Requirements") and standards laid down in this IT Framework. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this IT Framework.

The Complexity Requirements for setting passwords are as follows:

- A strong password must be at least 8 (Eight) characters long.
- It should not contain any of the user's personal information—specifically his/her real name, user name, or even company name.
- It must be very unique from the passwords used previously by the users.
- It should not contain any word spelled completely.
- It should contain characters from the four primary categories: uppercase letters, lowercase letters, numbers, and characters.
- Users are encouraged to change the password every 30 (Thirty) days to ensure that a compromised password is not misused on a long-term basis.
- Passwords must not be stored in readable form in computers without access control systems or in other locations where unauthorized persons might discover them.

- Immediately upon assignment of the initial password and in case of password "reset" situations, the password must be immediately changed by the user to ensure confidentiality of all information.
- Under no circumstances, the users shall use another user's account or password without proper authorization.
- Under no circumstances, should the user share his/her password(s) with other user(s), unless the said user has obtained from the concerned branch manager/IT head the necessary approval in this regard. In such cases, the user shall be responsible for changing the password(s) immediately upon the completion of the task for which the password was shared.

(ii) Access Controls

- Access to the Sankalp's electronic information and information systems, and the facilities where they are housed, is a privilege that may be monitored and revoked without notification. Additionally, all access is governed by law and Sankalp policies including but not limited to requirements laid down in this policy.
- Persons or entities with access to the Sankalp's electronic information and information systems are accountable for all activities associated with their user credentials. They are responsible to protect the confidentiality, integrity, and availability of information collected, processed, transmitted, stored, or transmitted by Sankalp, irrespective of the medium on which the information resides.
- Access must be granted on the basis of least privilege – only to resources required by the current role and responsibilities of the person.

Requirements:

- All users must use a unique ID to access Sankalp's systems and applications.
- Alternative authentication mechanisms that do not rely on a unique ID and password must be formally approved.
- Remote access to Sankalp systems and applications must use a two-factor authentication where possible.
- System and application sessions must automatically lock after 10 (Ten) minutes of inactivity.

B. Information Security and Cyber Security

(i) Information Security

- **Identification and classification of information assets:** Sankalp maintains a detailed inventory of information assets with distinct and clear identification of the asset.
- **Functions:** The information security function is adequately resourced in terms of the number of staff, level of skill, and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. Further, there is a clear segregation of responsibilities relating to system administration, database administration, and transaction processing.
- **Role-based access control:** Access to information is based on well-defined user roles (system administrator, user manager, application owner). Sankalp has a clear delegation of authority to upgrade/change user profiles and permissions and also key business parameters.
- **Personnel Security:** A few authorized application owners/users may have intimate knowledge of financial institution processes and they pose potential threats to systems and data. Sankalp has a process of appropriate checks and balances to avoid any such threat to its systems and data.

Personnel with privileged access like system administrators, cybersecurity personnel, etc., are subject to rigorous background checks and screening.

- **Physical Security:** The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. Sankalp has created a secured environment for physical security of information assets such as secure location of critical data, restricted access to sensitive areas like data centers, etc., and has further obtained adequate insurance to safeguard such data.
- **Maker-checker:** Maker-checker is one of the important principles of authorization in the information systems of financial entities. It means that for each transaction, there are at least two individuals necessary for its completion as this will reduce the risk of error and will ensure reliability of information. Sankalp ensures that it complies with this requirement to carry out all its business operations.
- **Trails:** Sankalp ensures 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 is recorded in the audit trail.
- **Mobile Financial Services:** Sankalp has a mechanism for safeguarding information assets that are used by mobile applications to provide services to customers. The technology used by Sankalp for mobile services ensures confidentiality, integrity, and authenticity and provides for end-to-end encryption.
- **Social Media Risks:** Sankalp uses social media to market their products and is well equipped in handling social media risks and threats in order to avoid any account takeover or malware distribution. Sankalp further ensures proper controls such as encryption and secure connections to mitigate such risks.
- **Digital Signatures:** A Digital signature certificate authenticates an entity's identity electronically. Sankalp protects the authenticity and integrity of important electronic documents and also for high-value fund transfers.
- **Regulatory Returns:** Sankalp has adequate systems and formats to file regulatory returns to the RBI on a periodic basis. Filing of regulatory returns is managed and verified by the authorized representatives of Sankalp.

(ii) Cyber Security

- Sankalp takes effective measures to prevent cyber-attacks and to promptly detect any cyber intrusions to respond/recover/contain the fallout. Among other things, Sankalp takes necessary preventive and corrective measures in addressing various types of cyber threats which include denial of service, distributed denial of services (DDoS), ransomware/cryptoware, 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, and password-related frauds.
- Sankalp realizes that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This requires a high level of awareness among staff at all levels. Sankalp ensures that the top management and the Board have a fair degree of awareness of the fine nuances of the threats. Further, it also proactively promotes, among their customers, vendors, service providers, and other relevant stakeholders, an understanding of their cyber resilience objectives, and ensures appropriate action to support their synchronized implementation and testing.

(iii) Confidentiality

- Sankalp, 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.
- Access to customer information by employees of the service provider to Sankalp is on a 'need to know' basis, i.e., limited to those areas where the information is required in order to perform the outsourced function.
- Sankalp further ensures that the service provider isolates and clearly identifies Sankalp's customer information, documents, records, and assets to protect the confidentiality of the information. Sankalp has strong safeguards in place so that there is no comingling of information/documents, records, and assets.
- Sankalp ensures that it immediately notifies RBI in the event of any breach of security and leakage of confidential customer-related information.
- In furtherance to this Policy, Sankalp has implemented various internal IT policies in the Company as below:
    1. Acceptable Usage Policy
    2. Antivirus Policy
    3. Application Security Policy
    4. Asset Management Policy
    5. Backup and Restoration Policy
    6. Card Data Management and Retention Policy
    7. Change Management Policy & Procedure
    8. Clear Desk and Clear Screen Policy
    9. Control Effectiveness Measurement
    10. Corrective Action Procedure
    11. Cryptographic Policy
    12. Data Classification, Retention, and Disposal Policy
    13. Data Physical Access Control Policy
    14. Data Protection Policy
    15. Desktop Hardening Policy
    16. Disaster Recovery Planning Policy
    17. Email Policy
    18. Endpoint Security Policy
    19. Exit Procedure
    20. Firewall Security Policy
    21. Human Resource Policy
    22. Incident Management Procedure
    23. Information Classification, Labelling, and Handling Policy
    24. Information Security Incident Management Policy
    25. Information Security Policy
    26. Internal Audit Procedure
    27. Internal Policy
    28. Internet Policy
    29. IP and Copyrights Policy
    30. ISMS Scope and Objectives
    31. Log Retention Policy
    32. Logging and Monitoring Policy
    33. Logical Access Control Policy
    34. Mail Size Restriction Policy
    35. Management Review Procedure

36. Mobile Computing Device Handling Policy
37. Network Security Policy
38. Password Policy
39. Patch Management Policy
40. Physical Access Control Policy
41. Physical and Environmental Security Policy
42. Preventive Action Procedure
43. Procedure for Deleting Card Data
44. Remote Access Policy
45. Risk Assessment Methodology
46. Secure Data Transmission Policy
47. Secure Login Procedure
48. Security Monitoring Policy
49. Service Provider Management Policy
50. Software Acquisition Policy
51. Software Development Life Cycle
52. Software Installation Procedure
53. System Acquisition, Development & Maintenance
54. Third Party Network Access Procedure
55. Third Party Security Policy
56. Time Synchronization Policy
57. Vulnerability Management Policy
58. Wireless Security Policy
59. Business Continuity Management Policy
60. Communication and Operations Management Policy
61. Human Resource Security Policy
62. IT Security Compliance Policy
63. Mobile Device Policy
64. Supplier Relationship Policy
65. ISMS_APEX_01 Information Security Management Scope

C. Business Continuity Planning (BCP)

- BCP forms a significant part of any organization's overall Business Continuity Management plan, which includes policies, standards, and procedures to ensure continuity, resumption, and recovery of critical business processes. BCP at Sankalp is also designed to minimize the operational, financial, legal, reputational, and other material consequences arising from a disaster. Sankalp has a Board-approved BCP Policy. The functioning of BCP shall be monitored by the Board by way of periodic reports.
- Sankalp requires its service providers to develop and establish a robust framework for documenting, maintaining, and testing business continuity and recovery procedures. Sankalp ensures that the service provider periodically tests the Business Continuity and Recovery Plan and occasionally conducts joint testing and recovery exercises with its service provider.
- In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, Sankalp retains 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 the operations of Sankalp and its services to the customers.
- Sankalp ensures that service providers are able to isolate Sankalp's information, documents, records, and other assets. In appropriate situations, Sankalp can remove all its assets,

documents, records of transactions, and information given to the service provider, from the possession of the service provider in order to continue its business operations, or delete, destroy, or render the same unusable.

- The CTO is responsible for formulation, review, and monitoring of BCP to ensure continued effectiveness, including identifying critical business verticals, locations, and shared resources to prepare a detailed business impact analysis.
- After the vulnerabilities and interrelationships between various systems, departments, and business processes are identified, there should be a recovery strategy available with the CTO to minimize losses in case of a disaster. Sankalp also has the option of alternate service providers and would be able to bring the outsourced activity back in-house in case of an emergency.
- Sankalp also has in place necessary backup sites for their critical business systems and Data centers. These plans are also tested by Sankalp on a regular basis. The results along with the gap analysis are placed by the CTO before the Board.

D. Back-Up of Data with Periodic Testing

- In order to prevent loss of information by destruction of the magnetic means in which it is stored, a periodic backup procedure is carried out. The responsibility of backing up the information located in shared access servers is the network administrators.
- Restoration testing on a time-to-time basis is done as both hard disks and magnetic tapes are prone to errors. As a general rule, daily full backup happens for all critical business applications, and a complete weekly full backup is carried out, including file servers/old data kept on servers.The Board approves of this IT Framework and has overall charge of the operational functions of Sankalp. The Board is further responsible for timely amending this IT Framework pursuant to its operations and/or any change in the regulations or new regulations issued by the RBI in relation to this IT Framework.

E. System Generated Reports

Sankalp shall ensure that system-generated reports shall be generated for Top Management summarizing financial position, including operating and non-operating revenues and expenses, cost-benefit analysis of segments/verticals, cost of funds, etc.

F. Regulatory Returns to RBI (COSMOS Returns)

Sankalp shall ensure adequacy to file regulatory returns to RBI (COSMOS Returns).