SILVER FINANCE SOLUTIONS PVT. LTD.

196, VINDHYANCHAL NAGAR,
AIRPORT ROAD,INDORE (M.P.)
Silverfinancesolutions@gmail.com

NBFC IT AND CYBER SECURITY POLICY

CONTACT:

Mr. Nirmal Agrawal (Director) - +91 94254 36370

Mr. Kamal Agrawal (Director) - +91 900900 5400

Mr. Pawan Agrawal (Director) - +91 94251 02155

PREAMBLE

An IT Security Policy is the most critical element of an IT security program. A security policy identifies the rules and procedures that all persons accessing computer resources must adhere to in order to ensure the confidentiality, integrity, and availability of data and resources. Furthermore, it puts into writing an organization's security posture, describes and assigns functions and responsibilities, grants authority to security professionals, and identifies the incident response processes and procedures.

The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (eLearning, virtual classrooms, etc) and Financial services (mobile banking / payment gateways), etc. Such initiatives have enabled increased IT adoption in the country through sectoral reforms and National programmes which have led to creation of large scale IT infrastructure with corporate / private participation.

Due to the dynamic nature of Technology, there is now a need for these actions to be unified, with an integrated vision and a set of sustained & coordinated strategies for implementation.

This Policy serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. It also enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs

This policy, therefore, aims to create a IT security framework, which leads to specific actions and programmes to enhance the security posture of country's IT sector.

I. VISION

To build a secure and resilient workspace for citizens, businesses, employees and government.

II.MISSION

To protect information and information infrastructure in the workspace, build capabilities to prevent and respond to threats, reduce vulnerabilities and minimize damage from incidents through a combination of institutional structures, people, processes, technology and cooperation.

III. OBJECTIVE

1. To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).
2. To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of data and for reducing economic losses due to cyber crime or data theft.
3. To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.
4. To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.

IV. STRATEGIES/POLICIES:

- **Access Control (Physical & Logical access control):**

Access to a critical system from a workstation external to its designated operation area can threaten its integrity and safety.
Access control – both physical and logical should be measurably higher than for other systems.

(a) Access control applies to all company owned networks, servers, workstations, laptops, mobile devices and services run on behalf of the company.

(b) Access to operating system commands will be restricted to those persons who are authorized to perform systems administration / management functions. Even, then such access must be operated under dual control requiring the specific approval of senior management."

(c) Staff user accounts can only be requested in writing, and by using the appropriate forms, by senior management.

- **Physical Control of System:**

  i. Protect the system from unauthorized use, loss or damage, e.g. the door should be locked when not in the office.
  ii. Position monitor and printers so that others cannot see sensitive data.
  iii. System should be properly shut down before leaving the office.
  iv. Install UPS system with adequate battery backups to avoid any data loss or corruption due to power failure.
  v. Always use mouse on mouse pad.
  vi. Make sure that there is some slack in the cables attached to your system.
  vii. Seek advice on disposal of equipment.
  viii. Visitor's log to be maintained at the entry level.

- **Managing Passwords:**

The use of a User ID and password as the sole means of access control may provide inadequate security to enable access to the organizations system especially where telephone dial up access is permitted.

  i. Keep the system screen saver enabled with password protection.
  ii. Don't share or disclose your password.
  iii. User should not have easily detectable passwords for Network access, screen saver etc.
  iv. A strong password must be as long as possible, include mixed-case letters, include digits and punctuation marks, not be based on any personal information, not be based on any dictionary word, in any language.
  v. Change password at regular intervals.
  vi. Never use the same password twice.

Information Security issues considered, when implementing the policy include the following:

- Password allocation via the System Administrator or other technical staff can compromise access control during which time unauthorized access may take place. This will be an unacceptable risk for highly sensitive systems.
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged

to keep the paper or digital document confidential and destroy it when their work is done.

ix. Never remove the cables when your PC is powered ON since this can cause an electrical short circuit.

- **Role based access control:**
  i. Assign permissions to individuals and groups.
  ii. Safely delegate tasks to the right people in line with the company policies.
  iii. Set the guard rails so the teams can work together easily and safely.
  iv. Track who made changes and create audit logs of actions taken.

- **Maker and Checker Policy:**
  i. For each transaction, there must be at least two individuals necessary for its completion as this will reduce the risk of error and will ensure reliability of information.
  ii. The checker cannot make modifications to the transaction entry. Modifications can only be done by maker.
  iii. If the checker rejects the transaction entry, it should be returned back to maker (with possible comments or suggested changes). The maker can then resubmit changes later.

- **Information and Cyber Security policy**:
  i. Information should be classified according to an appropriate level of Confidentiality, Integrity & availability.
  ii. Staff with particular responsibilities for information must ensure the classification of that information; must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.
  iii. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.
  a. On this basis, access to information will be on the basis of least privilege and need to know.

iv. Antivirus software will be set to update automatically. Employees are not permitted to turn off antivirus. All USB drives must be scanned for viruses.

v. To proactively promote, among their customers, vendors, 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.

- **Arrangement of Back up of Data Policies:**

i. Backup should be maintained regularly on the space provided on central server of the company or on the storage media as per the company policy.

ii. Keep the DAT's or other removable media in a secure location away from the computer.

iii. Backup files should be sent off-site to a physically secure location.

iv. Company should maintain backup infrastructure, including upgrading the hardware and software as needed.

v. The ability to restore data from backups shall be tested at least once per month.

- **Reporting Policies:**

i. Filing of various returns required by RBI w.r.t their deposit, acceptance, prudential norms compliance, Asset liability management, position of capital funds, Risk assets, important financial parameters etc.

ii. NBFCs may acknowledge receipt and confirm compliance to these return policies to the Regional Office under the jurisdiction of which they are registered.

iii. A BCP policy duly approved by the Board ensuring regular oversight of the Board by way of periodic reports (at least once every year).

iv. Report stolen or damaged equipment as soon as possible to the senior management.

- **Key Financial reports for Top management:**

i. Ensure that it is receiving all the key information to enable it to probe and question; focus on critical success areas and key performance indicators; and identify appropriate management actions where there are positive or negative variances from projected performance.

ii. Ensure that the performance reporting process links objectives, principles and practices to its needs.

iii. Periodically review the information it receives to ensure that it is getting what it needs and that all board members fully understand it. The board should guard against being inundated with an unnecessary amount of data that provides little or no information and which may prevent it from taking action.