SBFC Finance Limited

SBFC_29_Information_Security_Policy_v1.3

(Internal)

Authorization

Document Title: Information Security Policy

Document Code: SBFC_29_Information_Security_Policy_v1.3

Document Classification: Internal

Item	Description	Signature
Author	Shivaji Manwadkar (Manager)	
Recommended by	Gunjan Dedhia (Head Applications & Support)	
Reviewed by	Jay Mistry (Chief Compliance Officer)	
	Ganesh Vaidya (Chief Technology Officer)	
	Pankaj Poddar (Chief Risk Officer)	
	Aseem Dhru (MD & CEO)	
Approved by	Board Of Directors	

Document Approval History

Version	Approved (by)	Date	Signature/ Email /Meeting	Remarks
1.0	Board	02-06-2023	Board Of Directors	--
1.1	CTO	09-12-2023	Ganesh Vaidya	We have refined the versioning control
1.2	CTO	09-12-2023	Ganesh Vaidya	We have refined the versioning control
1.3	Board	25-01-2024	Jay Mistry	

Index

1. Purpose

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement to ensure the integrity and availability of the data environment mechanism at SBFC Finance Limited. The IT managers get overview of the policies and guidelines concerning the acceptable use of technology equipment, e-mail, Internet connections, voicemail, future technology resources and information processing.
The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all employees or temporary workers at all locations and by contractors working with the SBFC as subcontractors.

2.Scope

This policy document defines common security requirements for all personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of the entities in the private sector, legal, contractual, or fiduciary duty to protect said resources while in SBFC Finance Limited. In the event of a conflict, the more restrictive measures apply. This policy covers the network system which is comprised of various hardware, software, communication equipment and other devices designed to assist in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by them at its office locations or at remote locales.

3.Employee Responsibility

3.1 Employee requirement

The first line of defense in data security is the individual user. Users are responsible for the security of all data which may come to them in whatever format. The is responsible for maintaining ongoing training programs to inform all users of these requirements.

a. **Wear an Identifying Badge so that it may be easily viewed by others** - To help maintain building security, all employees should prominently display their employee identification badge. Contractors who may be in facilities are provided with different colored

identification badges. Other people who may be within the facilities should wear visitor badges and should be chaperoned.

b. Challenge Unrecognized Personnel - It is the responsibility of all personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted office location, you should challenge them as to their right to be there. All visitors to offices must sign in at the front desk. In addition, all visitors, excluding must wear a visitor/contractor badge. All other personnel must be employees of SBFC Finance Limited. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

c. Unattended Computers - Unattended computers should be locked up by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Employees are not allowed to take any action which would override this setting.

d. Home Use of Corporate Assets - Only computer hardware and software owned by SBFC Finance Limited and installed by SBFC Finance Limited is permitted to be connected to or installed on equipment. Only software that has been approved for corporate use by SBFC Finance Limited may be installed on the equipment. Personal computers supplied by SBFC Finance Limited are to be used solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by the for-home use.

e. Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the SBFC are the property of SBFC Finance Limited unless covered by a contractual agreement. Nothing contained herein applies to software purchased by employees at their own expense.

3.2 Prohibited Activities

Employees are prohibited from performing the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

a. Crashing of an information system: Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred because of user action, a repetition of the action by that user may be viewed as a deliberate act.

b. Attempting to break into an information resource or to bypass a security feature: This includes running password-cracking programs or sniffer programs and attempting to circumvent file or other resource permissions. Introducing, or attempting to introduce,

computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.

c. Exception: Authorized information system support personnel, or others authorized by the Privacy Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.

d. Personal or Unauthorized Software: Use of personal software is prohibited. All software installed on computers must be approved by the IT Team.

e. Software Use: Violating or attempting to violate the terms of use or license agreement of any software product used by SBFC Finance Limited is strictly prohibited.

f. System Use: Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures, or business interests of them is strictly prohibited.

3.3 Electronic Communication, E-mail, Internet Usage

As a productivity enhancement tool, that encourages the business use of electronic communications. All electronic communication systems and all messages generated on or handled by owned equipment are considered the property of SBFC Finance Limited not the property of individual users. Consequently, this policy applies to all employees and contractors, which covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

Provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible as long as:

- It does not consume more than a trivial amount of employee time or resources,
- It does not interfere with staff productivity,
- It does not preempt any business activity,
- It does not violate any of the following:

a. Copyright violations – This includes the act of pirating software, images, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.

b. Illegal activities – Use of information resources for or in support of illegal purposes as defined by federal, state, or local law is strictly prohibited.

c. Commercial use – Use of information resources for personal or commercial profit is strictly prohibited.

d. **Political Activities** – All political activities are strictly prohibited on premises. The encourages all its employees to vote and to participate in the election process, but these activities must not be performed using assets or resources.

e. **Harassment** – The strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, SBFC Finance Limited prohibits the use of computers, e-mail, voice mail, instant messaging, texting, and the Internet in ways that are disruptive, offensive to others, or harmful to morale.

For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse include, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.

Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several people with a request that each send copies of the letter to an equal number of people. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward an e-mail message to anyone.

The IT Team is responsible for servicing and protecting these equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems, and detecting patterns of abuse or illegal activity.

SBFC Finance Limited reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed, or stored by others.

3.4 Internet Access

Internet access is provided for users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by SBFC Finance Limited should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc. Do not use the Internet as a radio or to constantly monitor the weather or stock market results. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by the routers and firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic/tor browser or Deep web, Dark Web sites will be disciplined and may be terminated.

3.5 Reporting Software Malfunctions

Users should inform the appropriate personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, the computer virus policy should be followed, and these steps should be taken immediately:

1) Stop using the computer.

2) Do not carry out any commands, including commands to <Save> data.

3) Do not close any of the computer's windows or programs.

4) Do not turn off the computer or peripheral devices.

5) If possible, physically disconnect the computer from networks to which it is attached.

6) Inform the appropriate Information Security personnel as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.

7) Write down any changes in hardware, software, or software use that preceded the malfunction.

8) Do not attempt to remove a suspected virus!

3.6 Report Security Incidents

It is the responsibility of each employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents immediately to the Information Security Personnel/Officers. Employees should report any perceived security incident to either their immediate supervisor, or to their department head, or to any members of the IT team.

Reports of security incidents shall be escalated as quickly as possible. Each member of the CST must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged, and the remedial action indicated. It is the responsibility of the ICT Team to provide

training on any procedural changes that may be required because of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the Privacy Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police.

3.7 Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by them and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of policy and will result in personnel action and may result in legal action.

3.8 Installation of authentication & encryption certificates on e-mail system

Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user. Once verified, the certificate is installed on both recipients' workstations, and the two may safely exchange secure e-mail.

4 Identification and Authentication

4.1 User Logon IDs

Individual users shall have unique logon IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- **a.** Each user shall be assigned a unique identifier.
- **b.** Users shall be responsible for the use and misuse of their individual login ID.

All user login IDs are audited at least twice yearly, and all inactive login IDs are revoked. The Human Resources Department notifies the appropriate person upon the departure of all employees and contractors, at which time login IDs are revoked.

The login ID is locked or revoked after a maximum of three (3) or five (5) unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

4.2 Passwords

User Account Passwords

User IDs and passwords are required to gain access to all networks and workstations. All passwords are restricted by a corporate-wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

We follow the process as per mentioned in the password management policy.

4.3 Confidentiality Agreement

Users of information resources shall sign, as a condition for employment, an appropriate confidentiality agreement. The agreement shall include the following statement, or a paraphrase of it:

I understand that any unauthorized use or disclosure of information residing on the SBFC Finance Limited information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing information resources.

Confidential agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending, or employees are leaving an organization.

4.4 Access Control

Information resources are protected using access control systems. Access control systems include both internal (i.e., passwords, encryption, access control lists, constrained user interfaces, etc.) and external (i.e., port protection devices, firewalls, host-based authentication, etc.).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources. This form can only be initiated by the appropriate department head and must be signed by the department head and the Security Officer or appropriate personnel.

Since the supervisor or department head is the person who most recognizes an employee's need to access data. Users may be added to the information system, network, only upon the signature of the Security Officer or appropriate personnel who is responsible for adding the employee to the network in a manner and fashion that ensures the employee is granted access to data only as specifically requested.

Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited and that violators will be subject to criminal prosecution.

Identification and Authentication Requirements

The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

4.5 User Login Entitlement Reviews

If an employee changes positions at the, employee's new supervisor or department head shall promptly notify the Information Technology ("IT") Department of the change of roles by indicating on the Service Request both the roles or access that need to be added and the roles or access that need to be removed so that employee has access to the minimum necessary data to effectively perform their new job functions.

The effective date of the position change should also be noted on the Form so that the IT Department can ensure that the employee will have appropriate roles, access, and applications for their new job responsibilities. For a limited training period, it may be necessary for the employee who is changing positions to maintain their previous access as well as adding the roles and access necessary for their new job responsibilities.

No less than annually, the IT Manager shall facilitate entitlement reviews with department heads to ensure that all employees have the appropriate roles, access, and software necessary to perform their job functions effectively.

4.6 Termination of User Login Account

Upon termination of an employee, whether voluntary or involuntary, employee's supervisor or department head shall promptly notify the IT Department. If an employee's termination is voluntary and the employee provides notice, the employee's supervisor or department head shall promptly notify the IT Department of employee's last scheduled workday so that their user account(s) can be configured to expire. The employee's department head shall be responsible for ensuring that all keys, ID badges, and other access devices as well as equipment and property are returned to the Company prior to the employee leaving the Company on their final day of employment.

No less than **quarterly**, the IT Manager or their designer shall provide a list of active user accounts for both network and application access, to department heads for review. Department heads shall review the employee access lists within **five (7) business** working days of receipt. If any of the employees on the list are no longer employed by them, the department head will immediately notify the IT Department of the employee's termination status and submit the updated Network Access Request Form.

5 Network Connectivity

5.1 Telecommunication Equipment

Certain direct link connections may require a dedicated or leased phone line. These facilities are authorized only by the IT Team or appropriate personnel and ordered by the appropriate personnel. Telecommunication equipment and services include but are not limited to the following:

1. phone lines
2. fax lines
3. calling cards
4. phone headsets
5. software type phones installed on workstations.
6. conference calling contracts
7. cell phones
8. call routing software.
9. call reporting software.
10. phone system administration equipment
11. T1/Network lines
12. long distance lines
13. local phone lines
14. PRI circuits
15. telephone equipment

5.2 Permanent Connections

The security of systems can be jeopardized from third party locations if security and resources are inadequate. When there is a need to connect to a third-party location, a risk analysis should be conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of systems. The Privacy Officer or appropriate personnel should be involved in the process, design, and approval.

5.3 Emphasis on Security in Third Party Contracts

Access to computer systems or corporate networks should not be granted until a review of the following concerns has been made, and appropriate restrictions or covenants included in a Statement of Work ("SOW") with the party requesting access.

1. Applicable sections of the Information Security Policy have been reviewed and considered.
2. Policies and standards established in the information security program have been enforced.
3. A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
4. The right to audit contractual responsibilities should be included in the agreement or SOW.
5. A description of each service to be made available.
6. Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
7. A detailed list of users that have access to computer systems must be maintained and auditable.
8. If required under the contract, permission should be sought to screen authorized users.
9. Dates and times when the service is to be available should be agreed upon in advance.
10. Procedures regarding protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
11. Language restrictions on copying and disclosing information should be included in all agreements.
12. Responsibilities regarding hardware and software installation and maintenance should be understood and agreed upon in advance.
13. Measures to ensure the return or destruction of programs and information at the end of the contract should be written in the agreement.
14. If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
15. A formal method to grant authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
16. Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
17. A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.

5.4 Firewalls

Authority from the Privacy Officer or appropriate personnel must be received before any employee or contractor is granted access to a router or firewall.

6 Malicious Code

6.1 Antivirus Software Installation

Antivirus software is installed on all personal computers and servers. Virus update patterns are updated daily on the servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff that are responsible for keeping all virus patterns up to date.

a. **Configuration** - The antivirus software currently implemented by SBFC is Sentinel One. Updates are received directly from Sentinel One which is scheduled daily at specific time.

b. **Remote Deployment Configuration** - Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.

c. **Monitoring/Reporting** – A record of virus patterns for all workstations and servers on the network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the Privacy Officer or appropriate personnel.

6.2 New Software Distribution

Only software created by application staff, if applicable, or software approved by the Privacy Officer or appropriate personnel will be used on internal computers and networks. All new software will be tested by appropriate personnel to ensure compatibility with the currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from electronic bulletin boards, the Internet, or on disks (magnetic or CD-ROM and custom-developed software).

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the Privacy Officer or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on computers and networks. These precautions include determining that the software does not, harm because of faulty design, “misbehave” and interfere with or damage hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate personnel for instructions for scanning files for viruses.

Every diskette, CD-ROM, DVD and USB device is a potential source for a computer virus. Therefore, every diskette, CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a computer or network.

6.3 Retention of Ownership

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of SBFC Finance Limited are the property of SBFC Finance Limited unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging ownership at the time of employment. Nothing contained herein applies to software purchased by employees at their own expense.

7 Encryption

7.1 Encryption Key

An encryption key specifies the transformation of plain text into cipher text, or vice versa during decryption.

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, they shall establish the criteria in conjunction with the Privacy Officer or appropriate personnel. They employ several methods of secure data transmission.

7.2 File Transfer Protocol (FTP)

Files may be transferred to secure FTP sites using appropriate security precautions. Requests for any FTP transfers should be directed to the Privacy Officer or appropriate personnel.

8. Telecommuting

With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. SBFC Finance Limited considers telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all employees and contractors who work either permanently or only occasionally outside of the office environment. It applies to users who work from their home full time to employees on temporary travel, to users who work from a remote office location, and to any user who connects to the network, from a remote location.

8.1 Required Equipment

Employees approved for telecommuting must understand that SBFC Finance Limited will not provide all equipment necessary to ensure proper protection of information to which the employee has access; however, the following lists define the equipment and environment required:

Provided:

- Supplied workstation.
- If using VPN, an issued hardware firewall is required.
- If printing, a supplied printer.
- If approved by your supervisor, a supplied phone.

Employee Provided:

- Broadband connection and fees
- Secure office environment isolated from visitors and family.

8.2 Hardware Security Protections

a. **Virus Protection:** Home users must never stop the update process for Virus Protection. Virus Protection software is installed on all personal computers and is set to update the virus pattern daily. This update is critical to the security of all data and must be allowed to be completed.

b. **VPN and Firewall Use:** Established procedures must be rigidly followed when accessing information of any type. The requires the use of VPN software and a firewall device. Disabling a virus scanner or firewall is reason for termination.

c. **Lock Screens:** No matter what location, always lock the screen before walking away from the workstation. The data on the screen should be protected which may contain confidential information. So be sure the automatic lock feature has been set to automatically turn on after 5 minutes of inactivity.

8.3 Data Security Protection

a. **Data Backup:** Backup procedures have been established that encrypt the data being moved to an external media. Use only that procedure – do not create one on your own. Protect external media by keeping it in your possession when traveling.

b. **Transferring Data to SBFC Finance Limited:** Transferring data to SBFC Finance Limited requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent

established procedures, nor create your own method, when transferring data to SBFC Finance Limited.

c. **External System Access**: If you require access to an external system, contact your supervisor or department head. Privacy Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

d. **E-mail:** Do not send any individual-identifiable information (PII) via e-mail unless it is encrypted/ essential for office purpose or password protected. If you need assistance with this, contact the appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

e. **Non- Networks**: Extreme care must be taken when connecting equipment to a home or hotel network. Although the actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, the has no ability to monitor or control the security procedures on non-networks.

f. **Protect Data in Your Possession:** View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of PII level data is kept at a minimum and that old data is eliminated as soon as possible. Store electronic data only in encrypted workspaces. If your laptop has not been set up with an encrypted workspace, contact the Privacy Officer or appropriate personnel for assistance.

g. **Hard Copy Reports or Work Papers:** Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

h. **Data Entry When in a Public Location:** Do not perform work tasks which require the use of sensitive corporate or PII level information when you are in a public area, i.e., airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

i. **Sending Data Outside SBFC Finance Limited:** All external transfer of data must be associated with an official contract, non-discloser agreement, or appropriate Business Associate Agreement. Do not give or transfer any Confidential information to anyone outside SBFC Finance Limited without the written approval of your supervisor.

8.4 Disposal of Paper and/or External Media

Shredding: All paper which contains sensitive information that is no longer needed must be shredded before being disposed of. Do not place in a trash container without first shredding. All employees working from home, or in other non- work environments, must have direct access to a shredder.

Disposal of Electronic Media: All external media must be sanitized or destroyed in the proper manner.

1. Do not throw any media containing sensitive, protected information in the trash.
2. Return all external media to your supervisor.
3. External media must be wiped clean of all data. The Privacy Officer or appropriate personnel have very definitive procedures for doing this – so all external media must be sent to them.
4. The final step in this process is to forward the media for disposal by a certified destruction agency.

9. Change Management

To ensure that tracking changes to networks, systems, and workstations including software releases and software vulnerability patching in information systems Change tracking allows the Information Technology ("IT") Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

Procedure

1. The IT staff or other designated employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system.
    a. When changes are tracked within a system, i.e., Windows updates in the Add or Remove Programs updates performed and logged by the vendor, they do not need to be logged on the change management tracking log; however, the employee implementing the change will ensure that the change tracking is available for review if necessary.
2. The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
3. The employee implementing the change shall also be familiar with the rollback process if the change causes an adverse effect within the system and needs to be removed.

10. Information System Activity Review

To establish the process for conducting, on a periodic basis, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and access reports. SBFC Finance Limited shall conduct a regular internal review of records of system activity to minimize security violations.

1. The Information Technology Services shall be responsible for conducting reviews of SBFC information systems' activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately.
2. The Security Officer shall develop a report format to capture the review findings. Such report shall include the reviewer's name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible, such a report shall be in a checklist format.
3. Such reviews shall be conducted annually. Audits also shall be conducted if SBFC Finance Limited has reason to suspect wrongdoing. In conducting these reviews, the Information Technology Services shall examine audit logs for security-significant events including, but not limited to, the following:

a. **Logins** – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.

b. **File accesses** – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.

c. **Security incidents** – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.

d. **User Accounts** – Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have such access to the information and/or system.

All significant findings shall be recorded using the report format.

The Information Technology Services shall forward all completed reports, as well as recommended actions to be taken in response to findings, to the Security Officer for review. The Security Officer shall be responsible for maintaining such reports. The Security Officer shall consider such reports and recommendations in determining whether to make changes to administrative, physical, and technical safeguards. In the event a security incident is detected through such auditing, such matters shall be addressed pursuant to the policy entitled Employee Responsibilities (Report Security Incidents).

11. Data Integrity

SBFC Finance Limited User Shall implement and maintain appropriate electronic mechanisms to corroborate that Data has not been altered or destroyed in an unauthorized manner.

To prevent transmission errors as data passes from one computer to another, will be used, as determined to be appropriate, to preserve the integrity of data.

To prevent programming or software bugs, will test its information systems for accuracy and functionality before it starts to use them. will update its systems when IT vendors release fixes to address known bugs or problems.

1. The IT team will install and regularly update antivirus software on all workstations to detect and prevent malicious code from altering or destroying data.
2. To prevent exposing magnetic media to a strong magnetic field, workforce members shall keep magnetic media away from strong magnetic fields and heat. For example, computers should not be left in automobiles during the summer months.

12 Contingency Plan

To establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain data.

SBFC Finance Limited is committed to maintaining formal's for responding to an emergency or other occurrence that damages systems containing Data. shall continually assess potential risks and vulnerabilities to protect information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the Security Rule.

Procedure

1. Data Backup Plan

The data backup is initiated in the form of instances of Database and Applications. The Production environment is hosted in Mumbai region on AWS. N2WS is creating snapshots of instances & copying same to DR Hyderabad region. The following is the list of the Servers which provide us the type of instances type and the corresponding platform.

Sr No	*Server Name*	*Private IP*	*Platform*	*Instance Type*	*VCPU*	*RAM(GiB)*
1	FLEXYDIAL	10.10.2.238	Linux	c5.xlarge	4	8
2	OMEGADELTA-PROD	10.10.1.38	Linux	c5a.xlarge	4	8
3	MIFIN APP PROD	10.10.1.118	Windows	m5.4xlarge	16	64
4	CRM-APP	10.10.1.165	Windows	m5.xlarge	4	16
5	CRM-DB	10.10.1.175	Windows with SQL Server Standard	m5.xlarge	4	16

6	MIFIN-DB-DR-PROD	10.10.2.126	Windows with SQL Server Standard	m5.xlarge	4	16
7	SBFC-Website	10.10.1.16	Linux	m5.xlarge	4	16
8	CUSTOMERAPPPROD	10.10.11.171	Linux	m5a.large	2	8
9	MIFIN DB PROD	10.10.1.221	Windows with SQL Server Standard	r5.4xlarge	16	128
10	FTP Server	10.10.1.65	Linux	t3a.small	2	2

The IT Team shall monitor storage and removal of backups and ensure all applicable access controls are enforced. The backup procedures on an annual basis are made to ensure that exact copies of Data can be retrieved and made available. Such testing shall be documented by the IT Team. To the extent such testing indicates the need for improvement in backup procedures, the IT Team shall identify and implement such improvements in a timely manner.

Sr No	Schedule Name	Repeat Every	Enabled on	Description
1	Daily_app	1 Day	Sunday/Monday/Tuesday/Wednesday/Thursday/Friday/Saturday 07:00 AM	This is Daily backup policy schedule for everyday
2	MIFINDB_DB_12 hrs	12 hours	Sunday/Monday/Tuesday/Wednesday/Thursday/Friday/Saturday 01:00 AM & 01:00 PM	MIFINDB_DB_Daily runs every 12 hours
3	Weekly	1 Week	8PM - Every Monday	This is Weekly backup policy schedule for every week
4	Daily-cpmdata	1 Day	Sunday/Monday/Tuesday/Wednesday/Thursday/Friday/Saturday 12:00 AM	This is Daily backup policy schedule for every 12 hours
5	MIFINDB_DB_6hrs	6 hours	Sunday/Monday/Tuesday/Wednesday/Thursday/Friday/Saturday 01:00 AM, 07:00 AM, 01:00 PM & 07:00 PM	MIFINDB runs every 6 hours
6	Daily_app_6hours	6 hours	Sunday/Monday/Tuesday/Wednesday/Thursday/Friday/Saturday 05:00 AM, 11:00 AM, 05:00 PM & 11:00 PM	Daily_App runs every 6 hours

2. Disaster Recovery and Emergency Mode Operations Plan

A. The Security Officer shall be responsible for developing and regularly updating the written disaster recovery and emergency mode operations plan for the purpose of:

B. Restoring or recovering any data and/or systems necessary to make data available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency, and Continuing operations during such time information systems are unavailable.

i. Such a written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall be maintained on-site and at the off-site locations at which backups are stored or other secure off-site locations.

C. The disaster recovery and emergency mode operation plan shall include the following:

i. Current copies of the information systems inventory and network configuration developed and updated as part of risk analysis.

ii. Current copy of the written backup procedures developed and updated pursuant to this policy.

iii. Identification of an emergency response team. Members of such team shall be responsible for the following:

a. Determining the impact of a disaster and/or system unavailability on operations.

b. In the event of a disaster, securing the site and providing ongoing physical security.

c. Retrieving lost data.

d. Identifying and implementing appropriate "workarounds" during such time information systems are unavailable.

e. Taking such steps is necessary to restore operations.

iv. Procedures for responding to loss of electronic data including, but not limited to retrieval and loading of backup data or methods for recreating data should backup data be unavailable. The procedures should identify the order in which data is to be restored based on the criticality analysis performed as part of risk analysis.

v. Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following:

a. Members of the immediate response team,

b. Facilities at which backup data is stored,

c. Information systems vendors, and

d. All current workforce members.

D. The disaster recovery team shall meet on at least an annual basis to:

i. Review the effectiveness of the plan in responding to any disaster or emergency experienced.

ii. In the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and evaluate the results of such drills; and

iii. Review the written disaster recovery and emergency mode operations plan and make appropriate changes to the plan. The Security Officer shall be responsible for convening and maintaining minutes of such meetings. The Security Officer also shall be responsible for revising the plan based on the recommendations of the disaster recovery team.

13 Security Awareness and Training

Statement of Policy

To establish a security awareness and training program for all members of ’s workforce, including management.

All workforce members shall receive appropriate training concerning ’s security policies and procedures. Such training shall be repeated annually for all employees.

A. Security Training Program

a) The Security Officer shall have responsibility for the development and delivery of initial security training. All workforce members shall receive such initial training addressing the requirements of Security. Security training shall be provided to all new workforce members as part of the orientation process. Attendance and/or participation in such training shall be mandatory for all workforce members. The Security Officer shall be responsible for maintaining appropriate documentation for all training activities. (Need to implement)

b) The Security Officer shall have responsibility for the development and delivery of ongoing security training provided to workforce members in response to environmental and operational changes impacting the security of data e.g., addition of new hardware or software, and increased threats.

B. Security Reminders

a) The IT Team shall generate and distribute to all workforce members routine security reminders on a regular basis. Periodic reminders shall address password security, malicious software, incident identification and response, and access control. The Security Officer may provide such reminders through formal training, e-mail messages, discussions during staff meetings, screen savers, log-in banners, newsletter/intranet articles, posters, promotional items such as coffee mugs,

mouse pads, sticky notes, etc. The Security Officer shall be responsible for maintaining appropriate documentation of all periodic security reminders.

b) The Security Officer shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

C. Protection from Malicious Software

As part of the Security Training Program and Security Reminders, the Security Officer shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:

- Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail.
- The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current.
- Instructions to never download files from unknown or suspicious sources,
- Recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software.
- The importance of backing up critical data on a regular basis and storing the data in a safe place.
- Damage caused by viruses and worms, and
- What to do if a virus or worm is detected.

D. Password Management

As part of the Security Training Program and Security Reminders, the Security Officer shall provide training concerning password management. Such training shall address the importance of confidential passwords in maintaining computer security. We follow the process as per mentioned in the password management policy.

14 Security Management Process

SBFC Finance Limited shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to confidentiality, integrity, and availability. shall conduct an accurate and thorough risk analysis to serve as the basis for Security Rule compliance efforts. shall reassess the security risks to its most effectiveness of its security measures and safeguards as necessary considering changes to business and technological advancements.

Procedure

The Security Officer shall be responsible for coordinating risk analysis. The Security Officer shall identify appropriate persons within the organization to assist with the risk analysis.

The risk analysis shall proceed in the following manner:

- Update/develop information systems inventory. List the following information for all hardware (i.e., network devices, workstations, printers, scanners, mobile devices) and software (i.e., operating system, various applications, interfaces): date acquired, location, vendor, licenses, maintenance schedule, and function. Update/develop network diagram illustrating how organization's information system network is configured.
- Update/develop facility layout showing location of all information systems equipment, power sources, telephone jacks, and other telecommunications equipment, network access points, fire and burglary alarm equipment, and storage for hazardous materials.
- For each application identified, identify each licensee (*i.e.,* authorized user) by job title and describe the way authorization is granted.

For each application identified:

- Describe the data associated with that application.
- Determine whether the data is created by the organization or received from a third party. If data is received from a third party, identify that party and the purpose and manner of receipt.
- Determine whether the data is maintained within the organization only or transmitted to third parties. If data is transmitted to a third party, identify that party and the purpose and manner of transmission.
- Define the criticality of the application and related data as high, medium, or low. Criticality is the degree of impact on the organization if the application and/or related data were unavailable for a period.
- Define the sensitivity of the data as high, medium, or low. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident.

i) For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls.

a. Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") of data created, received, maintained, or transmitted by. Consider the following:

i) Natural threats, e.g., earthquakes, storm damage.

ii) Environmental threats, e.g., fire and smoke damage, power outage, utility problems.

iii) Human threats

a) Accidental acts, e.g., input errors and missions, faulty application programming or processing procedures, failure to update/upgrade software/security devices, lack of adequate financial and human resources to support necessary security controls.

b) Inappropriate activities, e.g., inappropriate conduct, abuse of privileges or rights, workplace violence, waste of corporate assets, harassment

c) Illegal operations and intentional attacks, e.g., eavesdropping, snooping, fraud, theft, vandalism, sabotage, blackmail

d) External attacks, e.g., malicious cracking, scanning, demon dialing, virus introduction

iv) Identify and document vulnerabilities in information systems. A vulnerability is a flaw or weakness in security policies and procedures, design, implementation, or controls that could be accidentally triggered or intentionally exploited, resulting in unauthorized access to data, modification of data, denial of service, or repudiation (*i.e.,* the inability to

identify the source and hold some person accountable for an action). To accomplish this task, conduct a SBFC-analysis utilizing the standards and implementation specifications to identify vulnerabilities.

b. Determine and document probability and criticality of identified risks.

Assign probability level, i.e., likelihood of a security incident involving identified risk.

i) "Very Likely" (3) is defined as having a probable chance of occurrence.

ii) "Likely" (2) is defined as having a significant chance of occurrence.

iii) "Not Likely" (1) is defined as a modest or insignificant chance of occurrence.

Determine risk score for each identified risk. Multiply the probability score and criticality score. Those risks with a higher risk score require more immediate attention.

c. Identify and document appropriate security measures and safeguards to address key vulnerabilities. To accomplish this task, review the vulnerabilities you have identified in relation to the standards and implementation specifications. Focus on those vulnerabilities with high-risk scores, as well as specific security measures and safeguards required by the Security Rule.

d. Develop and document an implementation strategy for critical security measures and safeguards.

i) Determine timeline for implementation.

ii) Determine costs of such measures and safeguards and secure funding.

iii) Assign responsibility for implementing specific measures and safeguards to appropriate person(s).

iv) Make necessary adjustments based on implementation experiences.

v) Document actual completion dates.

14.1 Human Resource Security

The Human Resources Security Policy specifies the information security requirements that need to be integrated in the HR processes such as recruitment and employment life cycle or separation change of employment.

This policy covers controls that need to be implemented for all employees for adherence to information security and ensure that the Human Resources (HR) processes are aligned with Information Security Policies and Initiatives of the organization.

Failure to adhere to information security responsibilities may force us to take appropriate disciplinary actions.

14.2 Prior to Employment:

The security responsibilities of individuals must be addressed at the hiring stage, during orientation and monitored during the entire tenure of employment. Job definition should include general responsibility of implementing or maintaining security policy as well as specific responsibility of protection of critical assets and security processes or activities.

A. Screening

All employees shall be subjected to background verification screening to ascertain claimed identity, credentials, and references. The background verification checks should ensure that all personal information is kept confidential, and the privacy of the prospective employee's data is maintained.

B. Terms and Conditions of employment

All employees will have to sign a confidentiality agreement (or Non-Disclosure Agreement) as part of a formal process which will hold them liable for any unauthorized disclosure, modification and/ or destruction of information. (Need to implement)

Terms and Conditions of Employment reflect the information security requirements and include the following: -

a) The responsibility for maintaining the confidentiality and integrity of information.

b) The actions to be taken if an employee disregards the organization's security requirements.

c) The continuation of the employee's responsibilities for protecting the confidentiality of the information of SBFC Finance Limited even after termination of employment.

14.3 During Employment

Objective is to ensure that the Human Resources (HR) processes are aligned with Information Security Policies and Initiatives of the organization.

a. Ensure that the employees understand their roles and responsibilities regarding Information Security and Cyber Security.

b. Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

c. All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function on an annual basis.

d. There shall be a formal and communicated disciplinary process in place to act against employees who have committed an information security breach.

4.1 Termination or Change of Employment:

Objective is to protect the organization's interests as part of the process of changing or terminating.

employment.

A. Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor, and enforced.

B. All employees and external party users shall return all the organizational assets in their possession upon termination of their employment, contract, or agreement.

C. Process shall follow for the revocation of access rights of the resigned employee.

D. HR to intimate IT and other respective department once employee (on-role / off-role) is resigned.

E. When an employee is planning to resign/move to another project, respective Line Managers will approve the request with a generic concern of IT Team.

F. IT Team would reduce resigned/planning to resign employee's rights to the minimum level.

G. The IT Team shall restrict below access and update the CISO.

a. Email: The employee's email account should be disabled or deleted to prevent them from accessing SBFC emails and attachments.

b. **Computer & Network access:** The employee's login credentials should be disabled or revoked to prevent them from accessing SBFC computers and network systems.

c. **Cloud services:** If the employee had access to cloud-based services such as Dropbox, Google Drive, or Microsoft OneDrive, their account should be deactivated or their access to shared files should be removed.

d. **Application:** The employee's access to any company-specific applications or software should be revoked.

e. **Social media accounts:** if the Employee had access to the company's social media accounts, their credentials should be revoked, or their access should be removed.

f. **VPN access:** If the employee had access to SBFC VPN, their access should be revoked.

g. **Customer information:** If the employee had access to customer information, such as a customer relationship management (CRM) system, their access should be revoked.

15.Enforcements

1. All staff (Permanent, Temporary, Contractors and Third-Party staff) are required to comply with this policy and any personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.
2. Staff having knowledge of any misuse or malpractice of SBFC IT Systems and their associated information processing facilities must report to their respective managers immediately and subsequently report as an Information Security Incident for necessary action.