SRF Limited

Cyber Security Policy

Document Control

S. No.	Type of Information	Document Data
1.	Document Title	Cyber Security Policy
2.	Document Code	IS-ISP-CS-01
3.	Date of Release	JULY 2022
4.	Version No	1
5.	Document Owner	Rajeev Verma

S. No.	Author	Designation	Date	Signature
1.	Rajeev Verma	AVP – Information Security	1/7/2022	

S. No.	Approver	Designation	Date	Signature
2.	Sanjay Rao	Chief Information Officer (CIO)	25/7/2022	

Version	Revision Date	Nature of Change	Changes Done by	Next Review Date
0.1	01/07/2022	Initial Draft	Rajeev Verma	NA

Contents

Introduction

The risk of data theft, scams, and security breaches from the cyber space can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, SRF has created this policy to help outline and complement the security measures and practices put in place to ensure IT infrastructure and information remains secure and protected from cyber threats.

Purpose

The purpose of this policy is to

- protect SRF data and infrastructure from cyber threats,
- outline the protocols and guidelines that govern cyber security measures,
- define the rules for company and personal use, and
- list the company's disciplinary process for policy violations.

Scope.

This policy applies to all SRF's permanent and part-time employees, remote workers, contractors, volunteers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

Confidential Data.

SRF defines "confidential data" as:

- Unreleased and classified financial information.
- Customer, supplier, and shareholder information.
- Customer leads and sales-related data.
- Patents, business processes, and/or new technologies.
- Plant designs, product formulations and recipes
- Employees' passwords, assignments, and personal information.
- Company contracts and legal records.

Device Security.

Company Device.

To ensure the security of all company-issued devices and information, SRF employees are required to:

- Keep all company-issued devices, including tablets, computers, and mobile devices, password-protected. Do not share company issued devices.
- Secure all relevant devices before leaving your desk.

- Refrain from sharing private passwords with coworkers, personal acquaintances, senior personnel, and/or shareholders.
- Regularly update devices with the latest security software.
- Dual factor authentication is enabled to reduce credentials compromise risks.

Personal Device.

SRF recognizes that employees may be required to use personal devices to access company systems. SRF selectively offer two ways to access corporate systems and the controls we expect employees to follow are different in both scenarios. SRF reserves the right to provide and limit access to its network and infrastructure on personal devices. SRF reserves the right to protect SRF data on personal devices through MAM solutions to avoid unauthorized data transfers.

1. When you are accessing the companies' systems and data directly over VPN or over HTTPS, please ensure the following:
    - Ensure all personal devices used to access company-related systems are password/pin protected.
    - Install full-featured antivirus software where applicable.
    - Regularly upgrade antivirus software where applicable.
    - Lock all devices when left unattended.
    - Ensure all devices are physically protected at all times.
    - Always use secure and private networks.

2. When you are using a VDI (Virtual Desktop Infrastructure) machine.
    - Do not leave the machine connected and unattended
    - By default, we do not allow any data transfer from VDI to Local client.
    - Do not share your Active Directory credentials with anyone.
    - Do not connect to VDI from unknown PCs.

Password Security.

Password leaks are dangerous since they can compromise our entire infrastructure. Passwords for corporate and personal systems should be kept a secret and should be secure enough to avoid being easily hacked. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- 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.
- Change their passwords frequently or when prompted by the system.
- Avoid using the same passwords in corporate systems and in your personal/social applications.

Email Security.

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, SRF requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact the IT department regarding any suspicious emails.

Transferring Data.

SRF recognizes the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to unauthorized employees and outside parties.
- Transfer confidential data to authorized employees only over SRF networks.
- Obtain the necessary authorization from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Adhere to SRF's data protection law (Applicable to data related to data subjects from EU) and confidentiality agreement.
- Immediately alert the IT department of any breaches, malicious software, and/or scams.

Additional measures.

To reduce the likelihood of security breaches, we also instruct our employees to:

- Report stolen or damaged equipment as soon as possible to [HR/ IT Department]
- Change all account passwords at once when a device is lost or stolen.
- Refrain from downloading suspicious, unauthorized, or illegal software on their company or personal equipment.
- Avoid accessing suspicious websites.

Disciplinary Action.

Violation of this policy can lead to disciplinary action, up to and including termination. SRF's disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, frequent violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on the case circumstances.

We also expect our employees to comply with our Information Security Policy and acceptable usage policy.