CYBER SECURITY POLICY

❖ Purpose & Background:

Under Master Direction DNBS.PPD.No.04/66.15.001/2016-17 of RBI dated June 08, 2017 on Information Technology Framework for the NBFC Sector, directions on IT Framework for the NBFC sector that are expected to enhance safety, security, efficiency in processes leading to benefits for NBFCs and their customers are provided. The focus of the proposed IT framework is on IT Governance, IT Policy, Information & Cyber Security. The policy is created to comply with the said Master Direction of RBI.

❖ Applicability

The Cyber Security Policy is applicable to all the employees of Sustainable Agro-commercial Finance Limited (SAFL). All the employees of the Company will be termed as "Users" under this policy.

❖ Information security and cyber security

1. Users are restricted to carry personal data card to offices nor to copy any data into external pen drive.

2. SAFL IT Team regularly educates employees about phishing sites and unwanted mails access.

3. SAFL IT Team has conveyed to employees not to disclose their passwords, whenever the users are not on their seat and to lock their computer screen, during their absence on their seat.

4. Internet access to the employees is given as per each department's requirement. Other unwanted websites are blocked as per IT policy of the Company.

5. Firewall is deployed at the gateway level of the internet. Firewall is configured with gateway level with Threat Protection and Capture ATP software.

6. DMZ is configured and installed on the firewall to protect outside threats to the internal servers and computer systems.

***Policy approved by the Board of Directors at the meeting held on 09th February, 2023.**

7. Email security Anti-Spam Server is configured on Microsoft O365 Email Exchange Server. Hence, all emails received by users are majorly protected on Microsoft cloud gateway level for the organisation.

8. Once an employee is relieved from services of SAFL, his/her emails are forwarded to the successor or his supervisor, as per the HR directions.

❖ **Requirements with regards to Digital Signature Certificates**

1. SAFL has purchased Digital Signature Certificates for the Authorised persons/members to be used for Corporate Banking, and other governmental websites like MCA, DGFT Website authentication, PF, GST, and other Taxation websites, etc.

2. Digital signature is password protected and are maintained by each individual to whom the signature pertains.

❖ **Requirements with regards to Mobile Computing Policy**

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

❖ **Requirements with regards to Social Media**

1. Usage of Social Media within SAFL's network is restricted, unless approved specifically.
2. Employees are personally responsible for the content they publish on- line, whether in a blog, social computing site or any other form of user- generated media.
3. Employees are not authorised to publish or discuss the following on Social Media:

- SAFL's confidential or other proprietary information
- To cite or reference Customers, partners or suppliers without their approval
- To use SAFL's logos or trademarks unless approved to do so.

❖ **Requirements with regards to Compliance with Information Security policy and procedures**

- Information processing facilities shall be used as per information security policy and acceptable usage policy.
- Exception to security policy and procedure shall be approved through the exception management process.
- Policy exceptions shall be reviewed at least annually and as deemed necessary based on security risks envisaged, emerging threats etc.
- Violations or any attempted violations of security policies and procedures shall result in disciplinary actions.

❖ **Requirements with regards to Network Level Security**

- SAFL network at all levels (LAN, WAN) shall be designed in such a way that no foreign computing resources shall be automatically connected.
- All temporary connections to external agencies within SAFL or from outside using VPN shall be through prior approval of Management.

****