Policy				
Title: Cyber Security Policy				
Department: Information Technology		Policy No.: **ICL/IT/CS/2024-003**		
Revision No.	Supersedes	Effective Date	Review Date	Page No.
00	Nil	24-01-2024	24-01-2026	1 of 6

1. PURPOSE

To lay down a procedure for Cyber Security Policy.

2. SCOPE

This procedure is applicable for all computing devices connected to the Innova Captab Limited network.

3. RESPONSIBILITY

Head IT/His designee is responsible for security of network /application deployed in Innova Captab Limited.

4. ACCOUNATBILTY

Head – IT department

5. PROCEDURE

The Cyber Security Policy provides guidelines to safeguard the company's data and technology infrastructure. It addresses potential threats like human errors, hacker attacks, and system malfunctions, emphasizing proactive measures, employee responsibilities, and reporting mechanisms to maintain data integrity and security The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and company reputation. For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. The following security measures which are used in Innova Captab Network to protect digital data:

	Prepared By	Checked By	Approved By
Name	Mukesh Kumar	Satyvir Verma	Vinay Lohariwala
Signature			
Date	24-01-2024	24-01-2024	24-01-2024

Access Restrictions (Internal)	
a	Changing Passwords
b	System Lock Out
Viruses/Firewalls/Tampering Prevention (External)	
a	Maintaining System logs/Integrity
b	Educating Employees on cyber attacks
c	Wi-Fi Enabled device Endpoint Security
d	Virus Quarantine Software
e	Securing Remote Access
Policies/Procedures/Management Support/Training	
a	Comprehensive Approach to IT Security
Server & Workstation Security L3,	
a	Controlling Workstation
b	Securing Server

5.3.1. Access Restrictions (Internal)

a. Changing Passwords:

i. Each user password shall be at least 10 characters long with the combination of alpha numeric and one special character in order to avoid easy detection.

ii. Each user password shall have an expiry period of 90 days, after which the user shall have to change his password, either on being prompted by the system or otherwise.

iii. Each user shall be allowed a maximum of 3 attempts to login. After three unsuccessful attempts to log in, the user ID shall be locked by the system.

iv. If user id of desktop or application gets lock then he will communicate verbal/through email to the IT department to unlock the user ID.

v. IT department keep the administrator password of each laptop/desktop itself and user's desktop/laptop run on user privileges.

	Prepared By	Checked By	Approved By
Name	Mukesh Kumar	Satyvir Verma	Vinay Lohariwala
Signature			
Date	24-01-2024	24-01-2024	24-01.2024

b. System Lock Out:

i. Users are encouraged to explicitly lock their desktop computer prior to leaving the computer unattended.

ii. Computer idle for more than 10 minutes will be automatically lockout

5.3.2. Viruses/Firewalls/Tampering Prevention (External)

a. Maintaining System logs/Integrity:

Company's IT system contains multilevel safeguards (Firewall/EPS), allowing the system to collect log and detect viruses, security violations, and tampering. This system allows the IT department to identify weaknesses and initiate efforts to safeguard the Company's IT systems.

b. Educating Employees on System Vulnerabilities:

IT personnel maintain a constant awareness of cyber attacks and counterattacks that are occurring with automated systems throughout many industries to ensure the company's network is protected from a breach. Alerts are given to system users to prevent virus attacks and improper release of information. These information passed to employee through training or mail communication.

c. Wi-Fi Enabled device Endpoint Security:

Wireless communication enabled device (Mainly Laptops) having endpoint security to keep device secure. In house Access point having separate guest SSID for outsider's assets.

	Prepared By	Checked By	Approved By
Name	Mukesh Kumar	Satyvir Verma	Vinay Lohariwala
Signature			
Date	24-01-2024	24-01-2024	24.01.2024

d. Virus Quarantine Software:

The organization use anti-virus product. Seqrite EPS/Quick Heal server Edition with Anti Spyware / Anti Malware is deployed on our corporate network. The following minimum requirements always remain in force.

i. The anti-virus product operate in real time protection on all servers and client computers.
ii. The anti-virus on the clients is centrally controlled by anti-virus server or individually where this centralization not available and the updating to its library definitions shall be forcefully pushed by the server and direct from vendor portal in-case users are working on remote location.
iii. EPS Anti-virus scans shall be done a minimum of once per week on all user controlled workstations.
iv. No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

e. Email Server Policy:

The email server will have additional protection since email with malware and ransom virus must be prevented from entering the network. This is a principal condition regardless the server is hosted internally or externally. Currently we use a hosted service (Icewarp-Email) that comes with Cisco virus protection. The anti-spam is also built-in.

f. Email Malware Scanning:

In addition to the standard anti-virus program, the email clients downloading all the mails will include Seqrite plugin for Microsoft Outlook/ Fortinet Email filtration (where EPS is not deployed) which will be used to scan all email for viruses and/or malware. This scanner will scan all email. When a virus is found or malware is found, the policy shall be to delete the email and not to notify either the sender or recipient.

	Prepared By	Checked By	Approved By
Name	Mukesh Kumar	Satyvir Verma	Vinay Lohariwala
Signature			
Date	24-01-2024	24-01-2024	24.01.2024

g. Securing Remote Access:

When required, company would implement a Virtual Private Network (VPN) for remote users to communicate with the ICL corporate network. The VPN handshake should have a random sequence of numbers that changes frequently in order to protect the system from unauthorized access.

5.3.3. Policies/Procedures/Management Support/Training

a. Comprehensive Approach to IT Security:

ICL regularly holds meetings that are attended by In-House Auditors to report information technology issues, including system security. ICL IT team has conducted a thorough analysis of system vulnerabilities; developed a data recovery plan; routinely identifies and responds to virus threats with the most up-to-date anti-virus software; and trains employees in information system security principles and data integrity. The IT security policy is fully documented and addresses access controls and system protection. Updates are communicated to employees. Employees are required to take a basic security awareness of this policy. Company fully supports the continuing education of its IT team members and gives them the opportunity to attend specialized training and conferences to keep up-to-date on information technology security.

5.3.4. Hardware & Workstation Security 13

a. Controlling Workstation:

1. After procurement of desktop/laptop the IT personnel format the system if it is DOS based or with window home OS and install Window professional/required application.
2. The IT personnel set Administrator password of asset and deploy in domain network.
3. If it is laptop, then EPS with latest patch deploy in this. After this activity the IT personnel will take user access management format and create the user with initial password in server. Then user use the asset after resetting the initial password

b. Securing Server:

1. Single person must be responsible for Server's In-Built default Administrator Password.
2. Separate ID create for another IT personnel using access management format.
3. Real time Antivirus deploy in Server and it remain behind the Fortinet firewall.

	Prepared By	Checked By	Approved By
Name	Mukesh Kumar	Satyvir Verma	Vinay Lohariwala
Signature		Satyvir	
Date	24-01-2024	24-01-2024	24.01.2024

6. LIST OF CROSS REFERANCES

S.No	SOP No / Document No	Title
01	SOP/IT/005 & SOP/GIT/005	Server user management

7. REVISION OF THE POLICY

The company reserves the right to revise, modify any or all the clauses of this policy depending upon the demand of business.

Sr. No.	REASON FOR CHANGE	REVISION NUMBER	Reference No.	EFFECTIVE DATE
1.	New Policy	00	ICL/IT/CS/2024-003	24-01-2024

	Prepared By	Checked By	Approved By
Name	Mukesh Kumar	Satyvir Verma	Vinay Lohariwala
Signature		Satyvir	
Date	24-01-2024	24-01-2024	24.01.2024