SUPRIYA LIFESCIENCE LTD.

Information Security Policy

SLL/INFOSEC/POLICY001

Classification: Internal Document

Information Security Policy

Document Control

Document ID	SLL/Infosec/Policy001
Document Owner	CFO
Effective Date	01/04/2023

Document Workflow

Version	Prepared By	Reviewed By	Approved By	Approved Date
1.0	CISO	CFO	Director	01.05.2023

Revision History

Version	Release Date	Details of changes	Reviewed By	Approved By
1.0	01.05.2023	NEW	CFO	Director

Document Control Statement

- This is an Internal document and property of SLL
- This document may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced in any form or manner including by any electronic, digital, or mechanical means to any medium, electronic or otherwise, or machine-readable form including any information storage, scanning or retrieval system without the prior express, written consent from SLL,
- If this copy is found other than the intended location(s) please inform to cfo@supriyalifescience.com / cs@supriyalifescience.com
- The User is advised to ensure that the appropriate version of the document is obtained for the intended use.

Table of Contents

Information Security Policy

1. Purpose

The purpose of Information Security Management is to protect information assets from all threats, vulnerabilities, whether internal or external, deliberate or accidental thereby ensuring incessant services to customers and other interested parties. The implementation of this policy is important to maintain our integrity as a supplier of product / service to both internal and external customers.

2. Definition & Information Security Management System (ISMS)

Information can exist in any forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security aims at protecting information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investment and business opportunities. The 3 basic components in Information Security Management are:

1. **Confidentiality** - Ensuring that information is accessible on to those authorized to have access.
2. **Integrity** - Safeguarding the accuracy and completeness of information and processing methods.
3. **Availability** - Ensuring that authorized users have access to information and associated assets when required.

A system designed to meet the three basic components of Information Security and to provide protection to assets from vulnerabilities and threats is Information Security Management System.

This information security policy forms a part of the ISMS implemented in SLL in conjunction with ISO 27001:2022 implementation.

3. Management Intent

The management of SLL endeavors to support the establishment of security systems, set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of a Security Policy across the organization.

4. Objectives

- Protection of customer property and proprietary information
- Protection of company's information & information processing assets from Malicious Actors, Cyber Threats & System Failures
- Adoption of a systematic approach to risk assessment and risk treatment.
- Provide a comprehensive Business Continuity Plan encompassing the respective unit/ location
- Identify the value of information assets and to understand their threats & vulnerabilities through appropriate risk assessment.
- Manage the risks to an acceptable level through design, implementation and maintenance of a formal Information Security Management System (ISO 27001:2022).

5. Scope of Information Security Management System (ISMS)

The scope of this policy includes to all SLL units.

6. Applicability

This policy is applicable to users of all information, explicit as well as implied, including all contractual partners of the organization.

7. Delegation and Responsibility Allocation

The top management shall form an Information Security Management System core team to guide the entire organization in implementing the policy. All Unit Heads/HODs will check for compliance with the policy within their area of responsibility and within their skill sets. They will guide/participate in carrying out risk assessment and risk treatment plans. All users will abide by this policy and all related policies and procedures. They shall also report security incidents and weaknesses to designated personnel.

8. Regulatory

- Information Technology Act
- Indian Contracts Act
- Indian Copyright Act
- Indian Patent Act

9. Disciplinary Actions

Compliance with the policy and procedural requirements shall be effectively monitored by the Infosec team to ensure proper reporting mechanisms in case of lapses and penal provisions for nonconformance.

10. Review

This policy shall be reviewed periodically once a year by the Infosec team and where cases of influencing changes occur; it shall be appropriately modified & documented to meet our business requirements and our ability to serve our customers.

THIS SPACE IS INTENTIONALLY LEFT BLANK

APPENDIX - A

Topic Specific Policies

Sr No	Particulars	Policy No SLL/Infosec/Policy001/	Page No
01	Acceptable Use Policy	0001	7-12
02	Access Control Policy	0002	13-14
03	Antivirus Policy	0003	15-16
04	Password Protection Policy	0004	17-19
05	Email Policy	0005	20-21
06	Wireless Communication Policy	0006	22-24
07	Internet Usage Policy	0007	25-33
08	Remote Access Policy	0008	34-36
09	Disaster Recovery Policy	0009	37-38
10	Software Installation Policy	0010	39-40
11	Server Security Policy	0011	41-43
12	Data Classification Policy	0012	44-52
13	Lab Security Policy	0013	53-55
14	Supplier Relationship Policy	0014	56-57
15	VPN Policy	0015	58-59
16	Data Backup Policy	0016	60-63

Acceptable Use Policy

1. Overview

Information security Team’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to SLL’s established culture of openness, trust and integrity. SLL is committed to protecting SLL's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, mobile devices, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of SLL. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every SLL employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and other electronic devices at SLL. These rules are in place to protect the employee and SLL. Inappropriate use exposes SLL to cyber risks including virus attacks including ransomware, compromise of network systems and services, data breach, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct SLL business or interact with internal networks and business systems, whether owned or leased by SLL, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at SLL and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with SLL policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at SLL, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by SLL.

4. Policy

4.1 General Use and Ownership

4.1.1 SLL proprietary information stored on electronic and computing devices whether owned or leased by SLL, the employee or a third party, remains the sole property of SLL. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of SLL proprietary information.

4.1.3 You may access, use or share SLL proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within SLL may monitor equipment, systems, and network traffic at any time, per Infosec's Audit Policy.

4.1.6 SLL reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

4.2.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended

4.2.4 Postings by employees from a SLL email address to newsgroups or other online platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of SLL, unless posting is during business duties.

4.2.5 Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of SLL authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing SLL-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SLL.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which SLL or the end user does not have an active license is strictly prohibited.
- Accessing data, a server, or an account for any purpose other than conducting SLL business, even if you have authorized access, is prohibited.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).
- Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a SLL computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any SLL account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to the Infosec Team is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, or similar technology on the SLL network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, SLL employees to parties outside SLL.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within SLL's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SLL or connected via SLL's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

- Blogging or posting to social media platforms by employees, whether using SLL's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of SLL's systems to engage in blogging or other online posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate SLL's policy, is not detrimental to SLL's best interests, and does not interfere with an employee's regular work duties. Blogging or other online posting from SLL's systems is also subject to monitoring.
- SLL's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any SLL confidential or proprietary information, trade secrets or any other material covered by SLL's Confidential Information policy when engaged in blogging.

- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of SLL and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.
- Employees may also not attribute personal statements, opinions or beliefs to SLL when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of SLL. Employees assume any and all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, SLL's trademarks, logos and any other SLL intellectual property may also not be used in connection with any blogging or social media activity

5. Policy Compliance

5.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Definitions and Terms

The following definition and terms can be found in glossary:

- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam
- Ransomware

Access Control Policy

1. Overview

SLL's intention for publishing an Access Control Policy are not to impose restrictions that are contrary to the established culture of openness, trust and integrity

2. Purpose

The purpose of this policy is:

1. To outline the proper access level for information and information processing assets
2. To protect the information and information processing assets of the Organization and its customers by having proper access control
3. To prevent exposure to risks including unauthorized access, loss of information and disruption in network services

3. Scope

This policy applies to all employees and external parties of the Organization. It also applies to all information and information processing assets that are owned or leased by the Organization or customer / contractual partner provided.

4. Policy

To ensure that the information and information processing assets of the organization are accessed only by the authorized personnel, the following shall be implemented:

- The login IDs for getting local access to the SLL's network resources shall be created for an employee / external party only based on approval from the concerned dept. heads / authorized person.
- Depending on the job responsibilities, the Dept. Head shall request the IT Team to allot rights, clearly identifying the resources and the type of rights. Based on the request received, IT Team shall provide the necessary access.
- As defined at individual unit level, the access rights shall be reviewed periodically by the IT / Infosec Team in coordination with the Dept. Head.
- On termination / separation of an employee, the ID shall be deleted / disabled with immediate effect by IT Team, on receipt of intimation from HR dept. / concerned dept. head.
- In case it is necessary to access the information using such ID, the same shall be kept enabled for specific number of days, upon request received from the Dept. Head, by changing the password. The change shall be intimated to the Dept. Head.

- Only IT administrator equivalent users shall have the access rights to system files. Users shall have no rights to system files.
- The configuration / modification of the network devices such as switches, routers, etc., shall be carried out by IT team / nominated personnel only. For such activity, the admin ID shall be used. For monitoring purpose, separate ID with limited access shall be created to prevent any unauthorized / unwanted change in the configuration.
- The allocation of privileged access rights should be controlled through a formal authorization process and proper records should be maintained.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment based on the severity of violation and impact on business operations. However management decision shall be considered as final.

6. Related Standards, Policies and Processes

None

7. Definitions and Terms

The following definition and terms can be found in glossary:

- Network devices

Antivirus Policy

1. Overview

SLL's intentions for publishing an Antivirus Policy are not to impose restrictions that are contrary to the established culture of openness, trust and integrity.

2. Purpose

The purpose of this policy is:

1. To prevent information and information processing assets of SLL from virus attacks
2. To minimize unavailability / performance degradation of information processing facilities
3. To ensure integrity of information

3. Scope

This policy is applicable for all computers (PCs, workstations, laptops, servers etc.), which are connected to SLL's network and susceptible to virus attacks. All users and external parties who use the above-mentioned equipment are bound by this policy, while working within SLL's network.

4. Policy

4.1 Preventive Measures

- All PCs, workstations, laptops and servers on SLL's network shall be configured with antivirus software. The same shall be centrally managed in each unit from the anti-virus server and the regular updates of the antivirus definition shall be enforced on all the client machines from this server.
- Users shall check the anti-virus definition on the PCs/laptops etc. and inform the IT Team for any discrepancies.
- Users shall never open any file or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately and then empty the Trash. Delete spam, chain, and other junk email without forwarding.
- Never download / execute files from unknown or suspicious sources.
- Avoid direct hard disk / file / folder sharing with read/write access unless there is an absolute business requirement to do so.
- CDs, DVDs, pen drives etc. shall not be used unless there is business need to do so. Users shall always scan a CD/ DVD / pen drive from an unknown source for viruses before using it.

4.2 Damage Control

- New viruses are discovered almost every day. The Anti-virus server administrator shall periodically visit the antivirus sites and check for the possible virus threats, their symptoms and the remedies.
- Using a Behavioral based antivirus detection tools is advised.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- If a PC/workstation/laptop/server is found infected by virus, the user shall inform the IT administrators immediately. The IT administrator shall isolate the infected system to prevent the virus from spreading on to the network.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment based on the severity of violation and impact on business operations. However management decision shall be considered as final.

6. Definitions and Terms

The following definition and terms can be found in glossary:

- Back-up
- Virus

Password Protection Policy

1. Overview

Passwords are a critical aspect of computer security. A weak or compromised password can result in unauthorized access to our most sensitive data and/or exploitation of our resources. All staff, including contractors and vendors with access to SLL systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for the secure use and protection of all work related passwords.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any SLL facility, has access to the SLL network, or stores any non-public SLL information.

4. Policy

4.1 Password Creation and Use

- All user-level and system-level passwords must confirm to the Password Construction Guidelines.
- Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts.
- Staff are allowed to use authorized, approved password managers to securely store and manage all their work-related passwords.
- User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

4.2 Password Change

Passwords should be changed only when there is reason to believe a password has been compromised or fails to meet password creation requirements.

4.3 Password Protection

- Passwords must not be shared with anyone, including supervisors and co-workers. All passwords are to be treated as sensitive, confidential SLL information.
- Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any individual suspecting that their password may have been compromised must report the incident and change all relevant passwords.

4.4 Multi-Factor Authentication

Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts.

4.5 Password Construction Guideline

- Strong passwords are long, the more characters a password has the stronger it is. We recommend a minimum of 08 and maximum of 16 characters in all work related passwords. The password should be a mix of alphabets, numbers and special characters.

- Avoid using passwords that has reference to your personal name or names that can be guessed. Avoid using generic passwords.

- Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change.

- If the Passwords are created by the administrator (for applications like ERP, AD/DC, etc..) then the process shall be followed by the administrator.

- In case the User wishes to change / reset the Passwords the same shall be intimated to the administrator.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Definitions and Terms

None

THIS SPACE IS INTENTIONALLY LEFT BLANK

Email Policy

1. Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

2. Purpose

The purpose of this email policy is to ensure the proper use of SLL email system and make users aware of what SLL deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within SLL Network.

3. Scope

This policy covers appropriate use of any email sent from a SLL email address and applies to all employees, vendors, and agents operating on behalf of SLL.

4. Policy

- All use of email must be consistent with SLL policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- SLL email account should be used primarily for SLL business-related purposes; personal communication is permitted on a limited basis, but non-SLL related commercial uses are prohibited.
- All SLL data contained within an email message or an attachment must be secured according to the Data Protection Standard Guidelines (refer glossary).
- Email should be retained only if it qualifies as a SLL business record. Email is a SLL business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
- Email that is identified as a SLL business record shall be retained according to SLL Record Retention Schedule as per company's policy.
- SLL email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any SLL employee should report the matter to their HR department immediately.

- Users are prohibited from automatically forwarding SLL email to a third party email system. Individual messages which are forwarded by the user must not contain SLL confidential or above information.
- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct SLL business, to create or memorialize any binding transactions, or to store or retain email on behalf of SLL. Any information related to emails, their attachments and transactions / databases pertaining to SLL shall not be stored externally in any device or forwarded to any personal email of the User / employee.
- Using a reasonable amount of SLL resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a SLL email account is prohibited.
- SLL employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
- SLL may monitor messages without prior notice. SLL is not obliged to monitor email messages.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Definitions and Terms

None

Wireless Communication Policy

1. Overview

With the mass explosion of Laptops, Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

2. Purpose

The purpose of this policy is to secure and protect the information assets owned by SLL. SLL provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. SLL grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to SLL network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Infosec / IT Team are approved for connectivity to a SLL network.

3. Scope

All employees, contractors, consultants, temporary and other workers at SLL, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of SLL must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a SLL network or reside on a SLL site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

4. Policy

4.1 General Requirements

All wireless infrastructure devices that reside at a SLL site and connect to a SLL network, or provide access to information classified as SLL Confidential, or above must:

- Abide by the standards specified in the Wireless Communication Standard Guidelines, section 4.4
- Be installed, supported, and maintained by an IT team.
- Use SLL approved authentication protocols, infrastructure and approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

4.2 Lab, Guest and Isolated Wireless Device Requirements

All Lab, Guest and isolated wireless infrastructure devices that provide access to SLL Confidential or above, must adhere to section 4.1 above. Guest and isolated wireless devices that do not provide general network connectivity to the SLL network must:

- Be isolated from the corporate network (that is it must not provide any corporate connectivity).
- Not interfere with wireless access deployments maintained by other support organizations.

4.3 Home Wireless Device Requirements

- Wireless infrastructure devices that provide direct access to the SLL corporate network, must confirm to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard Guidelines.
- Wireless infrastructure devices that fail to confirm to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the SLL corporate network. Access to the SLL corporate network through this device must use standard remote access authentication and VPN.

4.4 Wireless Communication Standard Guidelines

4.4.1 Work Environment

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol. *(Refer Glossary for details)*
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
- All Bluetooth devices must use Secure Simple Pairing with encryption enabled.
- Lab device Service Set Identifier (SSID) must be different from SLL production device SSID.
- Broadcast of lab device SSID must be disabled.

4.4.2 Home Environment

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Definitions and Terms

None

Internet usage Policy

1. Overview

Internet connectivity presents the company with new risks that must be addressed to safeguard the facility's vital information assets.

These risks include access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet. Additionally, the company may face loss of reputation and possible legal action through other types of misuse.

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate. Access to the Internet will be provided to users to support business activities and only on an as needed basis to perform their jobs and professional roles.

2. Purpose

The purpose of this policy is to define the appropriate uses of the Internet by employees and affiliates.

3. Scope

The Internet usage Policy applies to all Internet users (individuals working for the company, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The company's Internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

3.1 Internet Services Allowed

Internet access is to be used for business purposes only. Capabilities for the following standard Internet services will be provided to users as needed:

- E-mail - Send/receive E-mail messages to/from the Internet (with or without document attachments).
- Navigation - WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTPs) browser tool. Full access to the Internet; limited access from the Internet to dedicated company public web servers only.

Management reserves the right to add or delete services as business needs change or conditions warrant.

All other services will be considered unauthorized access to/from the Internet and will not be allowed.

3.2 Request & Approval Procedures

Internet access will be provided to users to support business activities and only as needed to perform their jobs.

3.2.1 Request for Internet Access

As part of the Internet access request process, the employee is required to read both this Internet usage Policy and the associated Internet/Intranet Security Policy The user must then sign the statements (located on page 33 pf this document) that he/she understands and agrees to comply with the policies. Users not complying with these policies could be subject to disciplinary action up to and including termination.

Policy awareness and acknowledgment, by signing the acknowledgment form, is required before access will be granted.

3.2.2 Approval

Internet access is requested by the user or user's manager submitting an IT Access Request form to the IT department along with an attached copy of a signed Internet usage Coverage Acknowledgment Form.

3.2.3 Removal of privileges

Internet access will be discontinued upon termination of employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be reevaluated by management annually. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users

4. Policy

4.1 Resource Usage

Access to the Internet will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on an employee's current job responsibilities. If an employee moves to another business unit or changes job functions, a new Internet access request must be submitted within 5 days.
User Internet access requirements will be reviewed periodically by company departments to ensure that continuing needs exist.

4.2 Allowed Usage

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Department.
Acceptable use of the Internet for performing job functions might include:

- Communication between employees and non-employees for business purposes;
- IT technical support downloading software upgrades and patches;
- Review of possible vendor web sites for product information;
- Reference regulatory or technical information;
- Research

4.3 Personal Usage

Using company computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination, especially during office hours.
All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.
Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The company is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property

4.4 Prohibited Usage

Information stored in the wallet, or any consequential loss of personal property. Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited. The company also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.
Other activities that are strictly prohibited include, but are not limited to:

- Accessing company information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
- Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.
- Deliberate pointing or hyper-linking of company Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the company.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international laws and regulations.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Any form of gambling.

Unless specifically authorized under the provisions of section 4.3, the following activities are also strictly prohibited:

- Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user's manager.
- Any ordering (shopping) of items or services on the Internet.
- Playing of any games.
- Forwarding of chain letters.
- Participation in any on-line contest or promotion.
- Acceptance of promotional gifts.

Bandwidth both within the company and in connecting to the Internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees. Specific departments may set guidelines on bandwidth use and resource allocation, and may ban the downloading of particular file types.

4.5 Software License

- The company strongly supports strict adherence to software vendors' license agreements. When at work, or when company computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the IT Department for review or to request a ruling from the Legal Department before any copying is done.
- Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document.
- Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with national / international copyright laws.
- Using company computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.
- All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.
- Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk.

4.7 Expectation of Privacy

4.7.1 Monitoring

Users should consider their Internet activities as periodically monitored and limit their activities accordingly.

Management reserves the right to examine E-mail, personal file directories, web access, and other information stored on company computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.

4.7.2 E-mail Confidentiality

Users should be aware that clear text E-mail is not a confidential means of communication. The company cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others.

Users should also be aware that once an E-mail is transmitted it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

4.8 Maintaining Corporate Image

4.8.1 Representation

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company", if not expressed it will be deemed to be considered as personal expressions (for which the company is not responsible / accountable) without written consent from the management.

4.8.2 Company Materials

Users must not place company material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service. Any posting of materials must be approved by the employee’s manager and the public relations / compliance / HR department and will be placed by an authorized individual.

4.8.3 Company Web Sites

Business units wishing to establish a corporate public facing websites must first develop content related to business, implementation, and maintenance plans. Formal authorization must be obtained through the IT Department for domain and hosting related activity. This will maintain publishing and content standards needed to ensure consistency and appropriateness.

Contents of the material made available to the public through the Internet must be formally reviewed and approved before being published. All material should be submitted to the Directors / CEO for initial approval to continue.

All company web sites must be protected from unwanted intrusion through formal security measures and vulnerability assessment which can be obtained from the Infosec Team.

4.9 Periodic Reviews

4.9.1 Usage Compliance Reviews

To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with usage policies.

4.9.2 Policy Maintenance Reviews

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage policies. These reviews may result in the modification, addition, or deletion of usage policies to better suit company information needs.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Additionally, the company may at its discretion seek legal remedies for damages incurred as a result of any violation. The company may also be required by law to report certain illegal activities to the proper enforcement agencies.

Before access to the Internet via company network is approved, the potential Internet user is required to read this Internet usage Policy and sign an acknowledgment form (located on the last page of this policy document). The signed acknowledgment form should be turned in and will be kept on file at the facility granting the access. For questions on the Internet usage Policy, contact the Information Technology (IT) Department.

6. Definitions and Terms

None

THIS PAGE SECTION IS INTENTIONALLY LEFT BLANK

7. Related Standards, Policies and Processes

INTERNET USAGE COVERAGE ACKNOWLEDGMENT FORM

After reading this policy, please sign the coverage form and submit it to your facility's IT department or granting facility's IT department for filing. By signing below, the individual requesting Internet access through company computing resources hereby acknowledges receipt of and compliance with the Internet Usage Policy. Furthermore, the undersigned also acknowledges that he/she has read and understands this policy before signing this form. Internet access will not be granted until this acknowledgment form is signed by the individual's manager. After completion, the form is filed in the individual's human resources file (for permanent employees), or in a folder specifically dedicated to Internet access (for contract workers, etc.), and maintained by the IT department. These acknowledgment forms are subject to internal audit.

ACKNOWLEDGMENT

I have read the *Internet Usage Policy*. I understand the contents, and I agree to comply with the said *Policy*.

Location *(Location and address)*

Name: ______________________________ Dept: __________________

Signature: ______________________________ Date: __________________

Manager /
Supervisor
Signature: ______________________________ Date: __________________

Remote Access Policy

1. Overview

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of SLL policy, we must mitigate these external risks the best of our ability.

2. Purpose

The purpose of this policy is to define rules and requirements for connecting to SLL's network from any host. These rules and requirements are designed to minimize the potential exposure to SLL from damages which may result from unauthorized use of SLL resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical SLL internal systems, and fines or other financial liabilities incurred as a result of those losses.

3. Scope

This policy applies to all SLL employees, contractors, vendors and agents with a SLL-owned or personally-owned computer or workstation used to connect to the SLL network. This policy applies to remote access connections used to do work on behalf of SLL, including reading or sending email or accessing servers and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to SLL networks.

4. Policy

- It is the responsibility of SLL employees, contractors, vendors and agents with remote access privileges to SLL's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to SLL.
- General access to the Internet for recreational use through the SLL network is strictly limited to SLL employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the SLL network from a personal computer, Authorized Users are responsible for preventing access to any SLL computer resources or data by non-Authorized Users. Performance of illegal activities through the SLL network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access.
- For further information and definitions, see the Acceptable Use Policy.

- Authorized Users will not use SLL networks to access the Internet for outside business interests.
- For additional information regarding SLL's remote access connection options, including how to obtain a remote access login, troubleshooting communicate with the local administrator (IT Team).

4.1 Remote Access to Critical and Sensitive Servers and Applications

- Access to critical and sensitive information assets like servers and applications, accessed remotely, shall be accessed only through approved VPN within a secured environment.
- Applications having client-server relationship shall not be given remote access within the company network, if accessed in the office or factory premises.
- Remote access should be restricted to the respective application, files and folders associated with user and privileges shall be assigned as per the unit managers approval.
- Remote access privileges shall be reviewed with the unit manager in 90 days.
- IT team shall have record of all remote access privileges provided.
- Remote access provided to the external users shall be time bound and should be recorded, reviewed and revoked.

4.2 Requirements to have Access Controls

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong passphrases. For further information see the Password Protection Policy.
- Authorized Users shall protect their login and password, even from family members.
- While using a SLL-owned computer to remotely connect to SLL's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- Use of external resources to conduct SLL business must be approved in advance by InfoSec and the appropriate business unit manager.
- All hosts that are connected to SLL internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the Supplier Relationship Policy.
- Personal equipment used to connect to SLL's networks must meet the requirements of SLL-owned equipment for remote access as stated in the Remote Access Policy to SLL Networks.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of SLL's network:

- Acceptable Use Policy
- Password Policy
- Remote Access Policy
- VPN Policy

7. Definitions and Terms

None

THIS PAGE SECTION IS INTENTIONALLY LEFT BLANK

Disaster Recovery Policy

1. Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan

2. Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by SLL that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

3. Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or subplans.

4. Policy

4.1 Contingency Plans

The following contingency plans must be created:

- Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Criticality of Service List: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.

- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- Mass Media Management: Who is in charge of giving information to the mass media?
- Also provide some guidelines on what data is appropriate to be provided.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Business Continuity Plan of the Company

7. Definitions and Terms

- Disaster

Software Installation Policy

1. Overview

Allowing employees to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization’s network are examples of the problems that can be introduced when employees install software on company equipment.

2. Purpose

The purpose of this policy is to outline the requirements around installation software on SLL computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within SLL computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

3. Scope

This policy applies to all SLL employees, contractors, vendors and agents with a SLL owned mobile devices. This policy covers all computers, servers, smartphones, tablets and other computing devices operating within SLL.

4. Policy

- Employees shall not install software on SLL computing devices operated within the network.
- Software requests must first be approved by the requester’s manager and then be made to the Information Technology department in writing or via email.
- Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester’s need.
- The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.
- Software's on test or trial should be installed on the user system with the approval of the requester's manager and the same should be uninstalled if SLL decides not to procure the license.
- Web based application installed at SLL shall follow all security drill including the process of access management by the web application company and database management on cloud or on premises.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Approved Software list

7. Definitions and Terms

None

THIS PAGE SECTION IS INTENTIONALLY LEFT BLANK

Server Security Policy

1. Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well

2. Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by SLL. Effective implementation of this policy will minimize unauthorized access to SLL proprietary information and technology.

3. Scope

All employees, contractors, consultants, temporary and other workers at SLL and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by SLL or registered under a SLL owned internal network domain.
This policy specifies requirements for equipment on the internal network

4. Policy

4.1 General Requirements

- All internal servers deployed on-premise must be owned by IT Team and is responsible for system administration. Server configuration guides must be established and maintained by each IT Team, based on business needs, and approved by the InfoSec team. IT Team should monitor configuration compliance and implement an exception policy tailored to their environment.
- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

  o Server contact(s) and location, and a backup contact
  o Hardware and Operating System/Version
  o Main functions and applications, if applicable

- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures

4.2 Configuration Requirements

- Operating System configuration should be in accordance with approved InfoSec team guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access control methods such as a web application firewall, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
- Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled, secured environment.
- Servers are specifically prohibited from operating from uncontrolled or unsecured cubicle areas.

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - All security related logs will be kept online for a minimum of 1 week.
  - Daily incremental tape backups will be retained for at least 1 month.
  - Weekly full tape backups of logs will be retained for at least 1 month.
  - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

None

7. Definitions and Terms

None

THIS PAGE SECTION IS INTENTIONALLY LEFT BLANK

Data Classification Policy

1. Overview

See Purpose

2. Purpose

The purpose of this policy is to establish a framework for classifying and handling SLL data based on its level of sensitivity, value and criticality to SLL. Classification of data will aid in determining baseline security controls for the protection of data.

3. Scope

This policy can be used to classify and protect any data that are stored, processed, or transmitted by the organization. The standard applies to all types of data but not limited to following:

- Electronic Data;
- Data recorded on paper; and
- Information shared orally, visually or by other means

This Policy will be applicable to all the employees, contractors and vendors of SLL and would cover all the information processing systems, and related equipment's in use which are vulnerable from the viewpoint of SLL.

THIS PAGE SECTION IS INTENTIONALLY LEFT BLANK

4. Policy

4.1 Data Classification Scheme

Classification Category	Description & Examples
Public	- **Data can be disclosed without restriction.** - Examples: Company Broachers, Advertisements, Press Release, Information on company's website, etc..
Internal	- **Confidentiality of data is preferred, but information contained in data may be subject to open records disclosure.** - Examples: Internal Circulars, Telephone numbers, Email Address Directories, Manuals, Training Materials, Policies, SOPs, Intranet Website, etc.
Confidential	- **Data that needs to be restricted to a limited set of users – internal or external.** - **Unauthorized disclosure, modification, or destruction of such data may result in significant damage to the business.** - Examples: All Customer Details, Loan details, Audit Reports, etc.
Restricted	- **Restricted data requires privacy and security protections. Special authorization may be required for use and collection.** - Examples: Sensitive Financial Information, Business Information Reports, Business strategy and forecasts, Intellectual Property Rights, etc.

4.2 Data Protection Scheme

Asset Category	Classification Category	
Media/Paper Documents/ Physical Access	Public	• Should be stored out of sight when unattended.
	Internal	• Should be stored out of sight when unattended.
	Confidential	• Media must be stored in a secure environment when unattended. • Systems storing such information must be housed in a secure environment.
	Restricted	• Must not be left unattended. • Media must be stored in secure environment when not in use or being worked on. • Systems storing such information must be segregated from other systems and housed in an area with enhanced physical security controls.

Asset Category	Classification Category	
Copies and Distribution	Public	- No need for control of distribution.
	Internal	- Copies must contain the same classification mark as the original.
	Confidential	- Must only be available to named individuals or distribution lists. - Printing/Copying processes must be physically controlled by the user, to ensure that no information remains left in the printers or copying machines. - Copies must contain the same classification mark as the original.
	Restricted	- Must only be available to named individuals in agreement with the information owner. - Printing/Copying processes must be physically controlled by the user, to ensure that no information remains left in the printers or copying machines. - Copies must contain the same classification mark as the original

Asset Category	Classification Category	
Electronic Storage	Public	- No need for additional protection.
	Internal	- Must be stored on systems which are only accessible to employees or authorized support staff.
	Confidential	- Must be stored on systems which are in secure environment and accessible only to employees and authorized support staff.
	Restricted	- Must be stored on systems which are in secure environment and accessible only to employees and authorized support staff. - Encryption should be used to protect such information if stored on portable device or if there is requirement to store it in non-secure environment. - Operating system or database access controls must be correctly configured to ensure authorized access.

Asset Category	Classification Category	
Electronic Transfer	Public	• No need for additional protection.
	Internal	• Must be password protected if transferred via an external network.
	Confidential	• Information must be encrypted if transferred via an external network.
	Restricted	• Information must be encrypted if transferred via an external network.
Change Control & Audit		• Secure publishing / release of public information e.g. use of restricted PDF settings to ensure information released to the public cannot be modified and republished once in the public domain'.
		• Standard Version control should apply.
		• Standard Version control should apply.
		• Standard Version control should apply. Access to such information should always be recorded on a secure audit trail.

Asset Category	Classification Category	
Physical Transfer	Public	• No need for additional protection.
	Internal	• Paper documents must be transferred in a sealed container / envelope that prevent the information from being read.
	Confidential	• Paper documents must be transferred in a sealed container / envelope which contain a clear indication that the document must be delivered by hand to the named individual.
	Restricted	• Paper documents must be transferred in a security sealed tamper evident container / envelope with a clear indication that the document must be delivered by hand to the named individual. Such paper documents must be transferred by an employee or a trusted third party

Asset Category	Classification Category	
Destruction of physical media	Public	- No need for additional protection.
	Internal	- No need for additional protection.
	Confidential	- All printed material and media must be shredded prior to disposal.
	Restricted	- All printed material and media must be shredded prior to disposal. - In addition, the shredded documentation must be incinerated.
Destruction of electronic information	Public	- No need for additional protection.
	Internal	- No need for additional protection.
	Confidential	- All such information is subjected to degaussing or secure erase by using specialized tools.
	Restricted	- All such information is subjected to secure erase by using specialized tools.

4.3 Reponsibilities

- It is the responsibility of the IT Department to ensure that owners are identified for each information asset.
- The asset owners are responsible for identifying, classifying, labeling and ensuring the protection of their respective information assets as per the guidelines set above.
- The asset owners are responsible for ensuring the implementation of the required controls for the protection of information assets.
- All employees and third-party staff are responsible for handling information assets as per the classification of the asset.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

None

7. Definitions and Terms

None

Lab Security Policy

1. Overview

See Purpose

2. Purpose

This policy establishes the information security requirements to help manage and safeguard lab resources and SLL networks by minimizing the exposure of critical infrastructure and information assets to threats that may result from unprotected hosts and unauthorized access.

3. Scope

This policy applies to all employees, contractors, consultants, temporary and other workers at SLL and its subsidiaries must adhere to this policy. This policy applies to SLL owned and managed labs, including labs outside the corporate firewall.

4. Policy

4.1 General Requirements

- Assign lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with InfoSec and the Corporate Enterprise Management Team. Lab managers or their backup must be available around-the-clock for emergencies.
- Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard SLL from security vulnerabilities.
- Lab managers are responsible for the lab's compliance with all SLL security policies.
- The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.
- All user passwords must comply with SLL's Password Protection Policy.

- Individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months).
- PC-based lab computers must have SLL's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Lab Admins/Lab Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free.
- Any activities with the intention to create and/or distribute malicious programs into SLL's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use Policy.
- No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a Sales & Marketing team of the organization.
- In accordance with the Data Classification Policy, information that is marked as SLL Highly Confidential or SLL Restricted is prohibited on lab equipment.
- Immediate access to equipment and system logs must be granted to members of InfoSec and the Network Support Organization upon request.
- InfoSec will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Acceptable Use Policy
- Data Classification Policy
- Password Protection Policy

7. Definitions and Terms

- DMZ
- Firewall

THIS PAGE SECTION IS INTENTIONALLY LEFT BLANK

Supplier Relationship Policy

1. Overview

SLL's intention for publishing Supplier Relationship Policy is to build up a standardized process and lifecycle for managing supplier relationships

2. Purpose

The purpose of this policy is to establish a standard for:

- Identifying and documenting the types of suppliers
- Defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access
- Minimum information security requirements for individual supplier agreements
- Accuracy and completeness of controls to ensure the integrity of the information or information processing assets
- Conditions under which information security requirements and controls will be documented
- Managing the necessary transitions of information and information processing facilities

3. Scope

The scope of this policy includes all the employees who are responsible for establishing supplier relationships on or behalf of organization

4. Policy

4.1 General Requirements

Type of suppliers which includes but not limited to the following:

a. IT services,
b. IT infrastructure components
c. Housekeeping
d. Facility Management
e. Security
f. Canteen
g. Background Verification
h. Engineering
i. Manpower
j. Courier
k. Financial services,
l. Logistics utilities

4.2 Guidelines

While establishing agreements with the supplier concerned functional heads shall consider the following to serve as the basis for individual supplier agreements:

- Minimum information security requirements for each type of information and type of access based on SLL's business needs and requirements.
- Screening and background verification requirements
- Processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation
- Accuracy and completeness of controls w.r.t integrity of the information or information processing assets provided by either party
- Types of obligations applicable to suppliers to protect the organization's information (Non-disclosure of information)
- Handling incidents and contingencies associated with supplier access including responsibilities of both SLL and suppliers
- Resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party;
- Conditions under which information security requirements and controls will be documented in an agreement signed by both parties;
- Managing the necessary transitions of information, information processing facilities anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

6. Related Standards, Policies and Processes

None

7. Definitions and Terms

None

Virtual Private Network (VPN) Policy

1. Overview

See Purpose

2. Purpose

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to SLL corporate network.

3. Scope

This policy applies to all SLL employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the SLL network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

4. Policy

Approved SLL employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the Remote Access Policy. *Additionally*,

- It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to SLL internal networks;
- VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase;
- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped;
- Dual (split) tunneling is NOT permitted; only one network connection is allowed;
- VPN gateways will be set up and managed by SLL IT Team through Firewall or VPN private service application;
- All computers connected to SLL internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (details available with IT Team); this includes personal computers.

- VPN users will be automatically disconnected from SLL's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open;
- Users of computers that are not SLL owned equipment must configure the equipment to comply with SLL's VPN and Network policies;
- Only Infosec-approved VPN clients may be used;
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of SLL's network, and as such are subject to the same rules and regulations that apply to SLL-owned equipment, i.e., their machines must be configured to comply with Information Security Policies.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee or contractors found to have violated this policy may be subject to disciplinary action.

6. Related Standards, Policies and Processes

- Remote Access Policy

7. Definitions and Terms

- IPSec Concentrator
- Dual Split Tunneling

Data Backup Policy

1. Overview

Systems and computers fail periodically. Vital records, systems and work products may be irretrievably lost if they have only been stored on the failed computer or computer system. The resulting frustrations, lack of productivity and cost are few of the consequences. This policy is designed to prevent such occurrences by having alternative locations for these systems and data, so they can be restored.

2. Purpose

The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed – whether to simply recover a specific file or when a larger-scale recovery effort is needed.

3. Scope

This policy applies to all data stored on SLL systems, on all computers, both laptops and desktops, and to all servers (on-premise / cloud) owned by SLL and any other electronic devices that may have storage capacity and consists of relevant data.

4. Policy

4.1 Identification of Critical Data

SLL must identify what data is most critical. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process.
Data Classification Policy should be considered to classify data to identify Confidentiality & Restricted data, which is critical and sensitive to SLL.

4.2 Data to be Backed Up

- All data determined to be critical and sensitive to SLL operation and/or employee job function.
- All information stored on the SLL's file server(s). It is the user’s responsibility to ensure any data of importance is moved to the central file server.
- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.

4.3 Backup Storage

- When stored onsite (Using External Hard Drive or Tapes), backup media must be stored in a fireproof container in an access-controlled area.
- Geographic separation from the backups (sufficient distance) must be maintained, to some degree, in order to protect from fire, flood, or other regional or large-scale catastrophes, to escape any damage from a disaster at the main site.
- When moved offsite, backup media should be reasonably secured from theft or fire and should be stored in a hardened facility that uses accepted methods of environmental controls, and access controlled secure, to ensure the integrity of the backup media.
- Online / Cloud should be used more effectively for backups.

4.4 Backup Procedure / Schedule

- Backups shall be carried out at regular intervals.
- Backup frequency is critical to successful data recovery. SLL has to determine a backup schedule (for all applications, database, servers, devices etc…) for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.
- All staff are reminded that they are individually responsible for data held locally on their desktop or laptop computer and all critical data shall be stored on central file server at SLL.
- The necessary level of backup should be defined.

4.5 Restoration

The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not misinterpreted by readers other than the backup administrator, and confusing during a time of crisis.

4.6 Backup Retention

SLL should determine the time required for backup retention, and what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data.

Backup copies must be maintained in accordance with the Retention and Disposal Schedule for backup copies. The schedule will determine the status of the information, as to whether it can be disposed of, cycled back into production or remain in archive storage.

4.7 Backup Stored Copies

- Stored copies must be stored with a short description like Backup date / Resource name / type of backup method (Full/Incremental), Department / Owner.
- A record of the physical and logical movements of all backup copies shall be maintained.
- Physical and logical movement of backup copies
  - The initial backup copy and its transit to storage.
  - Any movement of backup copies from their storage location to another location.

4.8 Handling Backup copies

The request for stored data must be approved by an authorized person nominated by a Director/Manager in the appropriate department. Requests for stored data must include:

- Completion of a form that outlines the specifics of the request, including what copy is being requested, where and when the requester would like it delivered and why they are requesting the copy.
- Acknowledgment that the backup copy will be returned or destroyed promptly upon completion of its use.
- Submission of a return receipt as evidence that the backup copy has been returned.
- Backup information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site; the controls applied to media at the main site should be extended to cover the backup site.
- Access to backup on cloud should be avoided to any user other than the IT team.

4.9 Restoration Testing

Restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery, and report on its ability to recover data.

- Backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary.
- Backup restores must be tested when any change is made that may affect the backup system.

On a daily basis, log information generated from each backup job will be reviewed for the following purposes:

- To check for and correct errors.
- To monitor the duration of the backup job.
- To optimize backup performance where possible.

4.10 Backup Media

Backup media in transit and store shall be protected from unauthorized access, misuse or corruption, including sufficient protection to avoid any physical damage arising during transit and store. Backups in transit shall be encrypted with an approved encryption technology.

All backup media shall be appropriately disposed of. Media will be retired and disposed of as described below:

- Prior to retirement and disposal, the media must be prepared.
- The media should no longer contains active backup images.
- The media's current or former contents shouldn't be read or recovered by an unauthorized party.
- Physical destruction of all backup media should be prior to disposal.

Certain types of backup media have a limited functional lifespan. After a certain time in service the media can no longer be considered dependable. When backup media is put into service the date must be recorded on the media. The media must then be retired from service after its time in use exceeds manufacturer specifications.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

6. Related Standards, Policies and Processes

None

7. Definitions and Terms

None

Reference

- Information Technology Act

  The Information Technology Act, 2000 is a legislation in India that provides legal recognition to electronic transactions, digital signatures, and electronic records. It aims to facilitate e-commerce, govern cybercrime, and promote secure electronic communication. The act establishes provisions for data protection, privacy, and cybersecurity, and it outlines penalties for offenses such as unauthorized access, hacking, and identity theft.

- Indian Contracts Act

  The Indian Contracts Act, 1872 is a law that governs the formation and enforcement of contracts in India. It defines the rights, duties, and obligations of parties involved in contractual agreements. The act specifies essential elements for a valid contract, rules for offer and acceptance, conditions for contract performance, and remedies for breach of contract. It ensures fairness, legality, and enforceability of contracts across various sectors and transactions.

- Indian Copyright Act

  The Indian Copyright Act, 1957 protects original literary, artistic, musical, and dramatic works, as well as cinematographic films and sound recordings, from unauthorized reproduction, distribution, public performance, and adaptation. It grants exclusive rights to creators or copyright owners and establishes provisions for licensing, infringement, and remedies for copyright violations. The act promotes creativity, encourages the growth of the arts, and safeguards the rights of authors, artists, and other copyright holders.

- Indian Patent Act

  The Indian Patent Act, 1970 governs the granting and protection of patents in India. It establishes the criteria for patentability, the process of patent application, and the rights conferred to patent holders. The act promotes innovation and technological advancement by granting exclusive rights to inventors over their inventions for a limited period. It also outlines provisions for compulsory licensing, revocation of patents, and patent infringement disputes.

Data Protection Standard Guidelines

1. Purpose

   A framework and guidelines for the protection of sensitive and confidential data within our company.

2. Scope

   These guidelines apply to all employees, contractors, and third parties who handle or have access to company data, regardless of the format or location of the data.

3. Data Classification

   Refer the Data Classification Policy

   - Data should be classified based on its sensitivity and criticality. Common classifications may include public, internal, confidential, and restricted.
   - Each classification level should have associated access controls, storage and transmission requirements, and guidelines for data handling.

4. Data Handling

   - Data should be handled in a manner that ensures confidentiality, integrity, and availability.
   - Only authorized personnel with a legitimate business need should have access to sensitive data.
   - Data should be encrypted when stored or transmitted, especially if it contains personally identifiable information (PII) or other sensitive data.
   - Data should be disposed of securely when no longer needed, following approved data retention and destruction policies.

5. Data Privacy

   - Privacy principles, such as data minimization and consent, should be followed when collecting, processing, or sharing personal data.
   - Data subjects should be informed about their rights regarding their personal data and how it will be used.
   - Privacy policies should be clearly communicated to employees and stakeholders, and compliance with privacy laws should be ensured.

6. Monitoring and Compliance

   - Regular monitoring and auditing should be conducted to ensure compliance with these guidelines and applicable data protection laws.
   - Non-compliance should be addressed promptly, and appropriate disciplinary actions should be taken as necessary.

Definitions & Terms

- Blogging: Blogging refers to the practice of creating and maintaining an online platform where individuals or organizations can share their thoughts, opinions, experiences, or information on various topics. It involves writing and publishing blog posts on a website or a blogging platform. From an information security perspective, bloggers need to be mindful of protecting their website from potential cyber threats such as hacking attempts or malware injections.
  - Example: A person starts a personal blog where they share travel stories, provide tips and recommendations for destinations, and share photographs from their journeys. They regularly update their blog with new posts, engage with readers through comments, and promote their content through social media platforms.

- Honeypot: A honeypot is a decoy system or network designed to attract and detect unauthorized access attempts or malicious activities. It mimics a vulnerable or valuable target to lure attackers, allowing security professionals to monitor their techniques, gather information about their methods, and develop countermeasures to protect real systems or networks.
  - Example: A company sets up a honeypot server that appears to contain sensitive customer data. It intentionally leaves security vulnerabilities to entice potential hackers. When an attacker tries to exploit the vulnerabilities, the honeypot captures their actions, logs their activities, and provides valuable insights into their tactics.

- Honeynet: A honeynet is a network of interconnected honeypots deployed to simulate a larger network environment. It allows organizations to observe and analyze the behavior of attackers across multiple systems, identify trends, and gather intelligence about emerging threats.
  - Example: A cybersecurity firm sets up a honeynet consisting of multiple virtual machines connected to a simulated corporate network. The honeynet is designed to mimic various network services and contains attractive targets for attackers. By monitoring the traffic and activities within the honeynet, the firm gains valuable insights into new attack techniques and develops effective countermeasures.

Definitions & Terms

- Proprietary Information: Proprietary information refers to confidential, sensitive, or valuable data that is owned or controlled by a person, organization, or entity. It typically includes trade secrets, intellectual property, customer lists, financial data, or any information that gives a competitive advantage to its owner.
    - Example: A software company has proprietary information in the form of its source code, algorithms, and product development plans. This information is critical to maintaining the company's competitive edge in the market. To protect this proprietary information, the company implements strict access controls, encrypts sensitive data, and establishes confidentiality agreements with employees and partners.

- Spam: Spam refers to unsolicited and unwanted bulk electronic messages, typically sent via email. It often includes advertisements, promotional offers, or malicious content. Spam messages are sent indiscriminately to a large number of recipients, with the intention of reaching potential victims or promoting fraudulent activities.
    - Example: A user's email inbox receives numerous unsolicited emails advertising fake products, phishing attempts, or fraudulent investment schemes. These spam messages are sent by unknown individuals or organizations trying to trick recipients into disclosing personal information, purchasing counterfeit goods, or clicking on malicious links.

- Ransomware: Ransomware is a type of malicious software that encrypts files or locks access to a victim's computer system until a ransom is paid. It is typically distributed through phishing emails, malicious downloads, or exploit kits and can cause significant disruption and financial loss to individuals and organizations.
    - Example: A user unknowingly opens an email attachment infected with ransomware. The ransomware encrypts all the user's files, rendering them inaccessible. The attacker demands a ransom payment in cryptocurrency in exchange for the decryption key. If the ransom is not paid, the files remain locked or are permanently deleted.

Definitions & Terms

- Disaster: In the context of information technology, a disaster refers to an event or incident that causes significant disruption or damage to an organization's IT infrastructure, systems, or data. It can be natural disasters like floods or earthquakes or human-made incidents such as fires, power outages, or cyberattacks. Disasters can lead to data loss, system downtime, financial loss, and reputational damage if appropriate measures for disaster recovery and business continuity are not in place.
    - Example: A company's data center experiences a severe fire, resulting in the destruction of servers, networking equipment, and critical data stored on-site. The fire causes a complete outage of IT services, impacting the company's operations and customer services. The company had not implemented off-site data backups or a disaster recovery plan, leading to extended downtime and significant data loss.

- DMZ (Demilitarized Zone): In the context of network security, a DMZ is a separate network zone that acts as a buffer between an organization's internal network (intranet) and external networks (such as the internet). The DMZ is designed to host publicly accessible services while isolating them from the internal network to enhance security and protect sensitive information.
    - Example: A company sets up a DMZ to host its web servers, email servers, and other services that need to be accessible from the internet. By placing these servers in the DMZ, external users can access the company's public-facing services without directly connecting to the internal network, reducing the risk of unauthorized access to sensitive data or systems.

- Firewall: A firewall is a network security device that acts as a barrier between an internal network and external networks, controlling the incoming and outgoing network traffic based on predetermined security rules. It monitors and filters network packets to enforce security policies and protect against unauthorized access and malicious activities.
    - Example: An organization deploys a firewall at its network perimeter to regulate traffic flow between the internal network and the internet. The firewall inspects incoming and outgoing network packets, blocking suspicious or unauthorized connections, preventing unauthorized access attempts, and allowing only approved traffic to pass through according to the organization's security policies.

Definitions & Terms

- IPSec Concentrator: An IPSec (Internet Protocol Security) concentrator is a network device or software application that facilitates secure communication between multiple remote locations or networks over the internet using IPSec protocols. It provides encryption, authentication, and data integrity for VPN (Virtual Private Network) connections, ensuring secure transmission of sensitive information.
  - Example: A multinational corporation establishes an IPSec concentrator at its headquarters to connect and secure communication with its branch offices located in different countries. The IPSec concentrator establishes encrypted VPN tunnels between the headquarters and each branch office, allowing employees to securely access shared resources, exchange confidential data, and communicate confidentially over the internet.

- Dual Split Tunneling: Dual split tunneling is a VPN configuration method that allows the separation of network traffic from a VPN client into two separate tunnels. In this setup, only specific traffic, such as corporate resources or sensitive data, is routed through the VPN tunnel, while other traffic, such as internet browsing or non-sensitive applications, directly accesses the internet.
  - Example: An employee working remotely connects to their company's VPN using dual split tunneling. The VPN is configured to send all traffic related to accessing internal company resources, such as databases and file servers, through the VPN tunnel for enhanced security. However, the employee's non-work-related traffic, such as streaming services or social media browsing, directly accesses the internet without routing through the VPN tunnel.

Approvals

Published Date: ________________

	Prepared By	Reviewed By	Approved By
Signature:	Pravin Nair		
Name:	Pravin Nair	Krishna Raghunathan	Saloni Wagh
Designation:	CSO / CISO	CFO	Director

Published Media:

- Internal document - Controlled User Manual for reference only (upload / photocopies not allowed)
- External stakeholders or vendors - Controlled Manual for reference only (upload / photocopies not allowed)
- Copies for Statutory Submission (Upload allowed, if mandatory, only with approval)