IT POLICY

Doc No: ISLL/IT/P/01

INFORMATION SECURITY MANAGEMENT SYSTEM

Ind-Swift Laboratories Limited

(Global Business Unit)

NH-21, Village Jawaharpur, Derabassi, District Mohali, Punjab,

India – 140507

Issue No.	Issue Date	Document No.	Prepared By	Reviewed by	Approved by
01	20-08-2025	ISLL/IT/P/01	ISO coordinator	CISO	CSM
			Sanyam Digitally signed by Sanyam Date: 2025.12.02 16:27:03 +05'30'	Sumeet Singh Digitally signed by Sumeet Singh Date: 2025.12.02 16:48:22 +05'30'	Ashok Kothari Digitally signed by Ashok Kothari Date: 2025.12.02 17:01:43 +05'30'

Revision History

Revision No.	Date of Release	Section/Page # Changed	Details of Changes	Reviewer	Approver
001	20-08-2025	Complete Document	First Issue of IT policy	CISO	CSM

Contents:

IT POLICY

Introduction:

At Ind-swift", information is important and protecting this information is critical for our business's survival. In order to safeguard this intellectual asset, an Information Security Policy is an absolute must. We are publishing this Information Security Policy Manual, which covers key areas of concern related to information security. This policy is for the awareness of all employees that Information Security is everyone's responsibility and that everyone is required to learn about Information Security and to attend events concerning the same.

This Information Security Policy is divided into different areas: Data Ownership, Antivirus and Malicious Programs, Internet-related Policies, Access Control, Network Policies, Physical Security, Operations Management, Business Continuity Policy and Personnel & Third-Party policies.

A System Administrator will co-ordinate and supervise the implementation of all security policies.

1. Ind-Swift Security Policy

A. Purpose

The purpose of the Ind-Swift Security Policy is to specify requirements and set direction for the organization's security from the high-level perspective of senior management.

B. Scope

The prime audience of this policy is department managers, while the secondary audience is all other employees of the organization.

C. Policy

1.1 Information security is everyone's responsibility.

1.2 All access to corporate resources and information should be on a 'Need to Know' basis.

1.3 A System Administrator will coordinate the implementation of all security policies. At a later stage an "Information Security Forum" may be formed, if required.

1.4 Information should be protected in terms of Confidentiality, Integrity, and Availability (CIA) when it is stored, processed, or transmitted, regardless of the storage medium and mode of transmission.

1.5 All of the organization's critical assets (e.g. hardware, software, equipment, and data) should be identified and appropriately protected.

1.6 A formal Inventory of all assets should be compiled. All Assets and Information should be appropriately classified and labeled as per the business's requirements.

1.7 Resource rights which are not explicitly assigned should be assumed to be denied.

1.8 When information is transmitted outside the organization, special measures should be taken to secure it.

1.9 The organization reserves the right to monitor information traffic and all Communications regardless of the medium being used.

1.10 The perimeter network should be appropriately protected with proper hardware and software.

1.11 Proper monitoring of the perimeter network and internal network should be done on a regular basis.

1.12 To provide protection against common threats to the organization, appropriate safeguards should be in place, including anti-virus programs and firewalls.

1.13 Regular checks on network, servers and other equipment should be conducted in order to make sure that the network is properly secure.

1.14 All information abuses and security breaches should be reported to the System Administrator.

1.15 Business Continuity of the organization should be ensured with proper measures.

1.16 Proper Security Awareness programs should be organized by the System Administrator.

1.17 The organization resources should be used for management-approved purposes only.

1.18 Prime importance should be given to physical security.
1.19 The Information Security document should be reviewed on a quarterly basis.
1.20 Disciplinary action, ranging from verbal reprimand to termination of employment, depending on the severity of the violation, may be taken.
1.21 Proper procedures for "Incident Handling" should be in place.
1.22 All security incidents, weaknesses, and malfunctions should be reported to the System Administrator. The System Administrator will ensure that the issue is addressed and will devise a mechanism to prevent recurrence in the future.
1.23 The proper skills should be developed to address any security-related incidents.
1.24 Proper checking for vulnerability with the help of a Penetration test should be carried out on a regular basis.
1.25 All systems, especially the operating systems, should be hardened to an acceptable level.
1.26 Physical security is of prime importance. All efforts should be made to secure the physical perimeter, physical entry points, office rooms, and delivery/loading areas.
1.27 Proper measures should be taken for securing all equipment, power supplies, and cables.
1.28 Security of equipment while being maintained off-premises should be assured.
1.29 All employees should wear their identity badges when on the company premises.
1.30 Discussion of company business information in public places such as elevators or cafés is strictly prohibited.
1.31 At the end of a meeting, all whiteboards should be cleaned, and flip-chart paper removed.
1.32 A 'Clean Desk' policy should be observed throughout the organization.
1.33 No games should be stored or played on company computers.
1.34 All advertisements for jobs and help should be reviewed thoroughly and should not disclose any sensitive information or future company plans.
1.35 If a company employee is presenting a paper, giving a presentation, or delivering a speech in a public forum or conference, all material must be reviewed by his/her immediate manager prior to presentation.
1.36 An annual Audit of the system should be performed to check the control of the systems.
1.37 All documentation in the company should have a version control page with the document's history. All pages should be numbered.
1.38 Disciplinary action will be taken for non-compliance with a security policy.
1.39 A proper Business Impact Analysis and Risk Assessment should be performed for all critical business systems, either by the Department Heads or by an outsourced resource.
1.40 In the case where 'Specialist Advice' is required, an outside consulting company may be approached for help.
1.41 The organization should comply with all the legal requirements as specified by the government of the country. Employees shall not indulge in an activity that is illegal under local or international law.

D. Enforcement

In the case of a policy violation, disciplinary action will be taken which may include the termination of employment.

E. Responsibility

All employees, Departmental Managers and the System Administrator.

2. Acceptable Use Policy

A. Purpose

The purpose of the Acceptable Use Policy of Ind-Swift Laboratories Ltd. is to communicate the acceptable behavior of the employee which is necessary to ensure the Confidentiality, Availability, and Integrity (CIA) of the systems, assets and information.

B. Scope

The scope of this policy covers all permanent/contract employees, consultants, and vendor/third parties' assigned persons working for the organization.

C. Policy

2.1 Security is everyone's responsibility. All employees of Ind-Swift Laboratories Ltd. shall comply with all applicable information security policies, procedures, and controls relevant to their roles.

2.2 Organizational resources—including systems, networks, internet access, email, and hardware—shall be used strictly for authorized business purposes.

2.3 All guidelines, circulars, or instructions issued by management regarding security or acceptable use must be adhered to as part of mandatory compliance.

2.4 Lack of awareness or unfamiliarity with information security policies will not be considered a valid justification for non-compliance.

2.5 All information processed, stored, transmitted, or accessed through the organization's resources is the property of the organization. The organization reserves the right to monitor, audit, and review all such information and activities as required.

2.6 All confidential and sensitive information must be handled with strict confidentiality. Copying, transmitting, or sharing such information is prohibited unless required for legitimate business needs and authorized through defined processes.

2.7 Employees are responsible for safeguarding their passwords, passphrases, and authentication credentials. Sharing, disclosing, or writing down passwords is strictly prohibited.

2.8 Passwords must be changed in accordance with the organization's Password Management Policy and follow the defined complexity, history, and expiration rules.

2.9 All sensitive data stored on laptops, desktops, and portable devices must be protected using password protection and any other required security controls (e.g., encryption), as per ISMS guidelines.

2.10 All computing devices must run the latest approved antivirus and endpoint protection solutions. Employees must not disable, bypass, or tamper with malware protection tools or security configurations.

2.11 Unauthorized copying, installation, or use of software—including freeware, shareware, and pirated software—is strictly prohibited.

2.12 Organizational devices and systems must not be used to install or test any unapproved, experimental, or potentially malicious software. Exceptions are allowed only for approved business-related software following the defined authorization procedure.

D. Enforcement

In the case of a policy violation, disciplinary action will be taken which may include the termination of employment.

E. Responsibility All employees.

3. Security Awareness Policy

A. Purpose

The purpose of this policy is to keep employees up to date with information security, which is changing at an astonishing pace.

B. Scope

The policy applies to all employees, no matter what position they hold.

C. Policy

3.1 The System Administrator will organize IT workshops on a half-yearly basis for employees and the attendance of every employee will be mandatory.

3.2 In the case where an employee has not attended the workshop, his/her respective manager will be informed.

3.3 If necessary, the System Administrator takes help of brochures, Posters and/or special Security Awareness Screen Saver to increase Information Security.

3.4 It is the responsibility of every individual to keep him/herself up to date through involvement in security program training as conducted by the organization.

3.5 Any security breach or query about security should be communicated to the System Administrator immediately.

3.6 Knowledge of security policies is one of the areas that will be assessed during appraisal of the employee.

D. Enforcement

In case of a policy violation, disciplinary action will be taken which may include the termination of employment.

E. Responsibility

All employees, especially the System Administrator and IT manager.

4. Data Protection Policy

A. Purpose

The purpose of the policy is to implement proper data ownership for Information Security. The owner of the data needs to be clearly specified with corresponding duties and responsibilities.

B. Scope

The policy applies to all employees who at any time are responsible for data handling, using and owning.

C. Policy

4.1 The Data Owner should be specified for each application. The Data Owner is the person who heads or leads the business unit. For example, the finance department manager owns finance data, not the IT Department. IT is merely the "Data Custodian" or the "Data Trustee".

4.2 The Data Owner will communicate the importance of the data, level of sensitivity, controls and monitoring requirements to the Data Custodian.

4.3 The Data Custodian may not take any action on the data without the permission of the Data Owner.

4.4 It is the responsibility of the Data Owner to ensure that data is backed up and stored on a shared drive with user access permission.

4.5 The Data Custodian will make sure that there are proper safeguards in place to recover from any Disaster.

4.6 Any data which is not on the server or is not backed up by the corporate backup facility, e.g. laptop or workstation data, will be the responsibility of the end-user to make sure that recovery is possible in the case of system failure or hard disk crash.

4.7 The Data Custodian will make sure that all adequate controls are in place, as specified by the Data Owner.

4.8 The Data Custodian should maintain proper documentation of all activities involving the Owner's data.

4.9 The Data Custodian will inform the Data Owner of any risk or shortcomings as soon as they are identified.

D. Enforcement

In the case of a policy violation, disciplinary action will be taken which may include the termination of employment.

E. Responsibility

Data Owner, Data Custodians, Department Heads and System Administrator.

5. Information Safeguarding Policy

A. Purpose

This policy specifies the control and proper safeguard of information generated, stored and transmitted in the organization.

B. Scope

The policy applies to all forms of information regardless of what medium is used for their storage and communication.

C. Policy

5.1 The Data owner will decide about the frequency of their data being backed up based on the project requirement, on the basis of importance and retention period of the information. The data lost should not be more than 24 hours.

5.2 Corporate Server backup frequency and retention should be defined and implemented by coordination of data owner and System Administrator.

5.3 All backups should be verified to ensure that it is re-storable.

5.4 On-site backup of data and applications on critical machines is highly recommended and should be carried out daily on Magnetic tapes & stored at security gate in fireproof media safe.

5.5 The Data Owner should specify the data retention period.

5.6 No pirated or other illegal software may be used in the organization.

5.7 Any software is to be bought only after proper permission from the department head and to be installed by the System Administrator.

5.8 Proper measures such as the installation of anti-virus software, firewalls, Penetration test (half yearly) should be taken to address external and internal threats.

D. Enforcement

In the case of a policy violation, disciplinary action will be taken which may include the termination of employment.

E. Responsibility

All employees, Department Heads and System Administrator.

6. Virus Control Policy

A. Purpose

This document specifies the organization's policy related to malicious programs i.e. Viruses, Worms, Trojans and others.

B. Scope

The scope of the policy includes all electronic communication mediums as well as all storage media which can be infected or can store or propagate malicious programs.

C. Policy

6.1 All machines should run the latest anti-virus software as approved by organization management.

6.2 E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail which a/he thinks may contain virus.

6.3 All removable media should be blocked for use or scanned for viruses before being used.

6.4 No pirated software should be used on the corporate network.

6.5 In the case of a virus being found, the System Administrator should be informed immediately. The System Administrator will investigate and take proper measures to avoid the event in future.

6.6 No user should clean a virus from a computer

6.7 All encrypted material should be decrypted and checked for viruses before being used.

6.8 The e-mail Server should have the antivirus program installed and must check all of the e-mail attachments before sending it to individual mailbox.

6.9 All of the updates to the antivirus program should be automatic from the web or from the central server

6.10 Antivirus Program should be supplemented by following components:

- Personal Firewall
- Network Attack Blocking
- Capacity Management

D. Enforcement

In the case of a violation of the security policy, disciplinary action will be taken, up to and including employment termination.

E. Responsibility

All employees and System Administrator.

7. Internet Usage Policy

A. Purpose

This document specifies the organization policy related to cyber-surfing and Internet Usage.

B. Scope

The scope of the policy includes all employees, irrespective of their position.

C. Policy

7.1 Only official Internet connections should be used.

7.2 Internet facilities will be provided to employees for business use only. No Internet usage for personal purposes is allowed.

7.3 While using the Internet, no person is allowed to abuse, defame, stalk, harass or threaten any other person, or violate local or international legal rights.

7.4 No person is allowed to upload, post, publish or distribute any inappropriate, indecent, obscene, profane, infringing, defamatory or unlawful information or material on the Internet while using the corporate resources.

7.5 No person is allowed to post personal advertisements or offer any goods or services using the organization's resources.

7.6 In case of access of websites, there are predefined categories with specific permissions and assign user to specific access category with manager's approval

Category	Access Type
Full Access	All Websites Access
YouTube Access	YouTube + Restricted Access
Social Sites Access	All Social Sites + Restricted Access
Restricted Access	Search only websites with minimal permissions

7.7 A visit to any obscene sites or sites which are non-business related will be considered a serious offence.

D. Enforcement

In the case of a violation of the security policy disciplinary action will be taken, up to and including employment termination.

E. Responsibility

All employees, System Administrator.

8. E-mail Usage Policy

A. Purpose

This document specifies the organization policy related to e-mail usage, including the receiving, replying, forwarding and auto reply functions.

B. Scope

The scope of the policy includes all permanent and contract employees irrespective of their position in the organization.

C. Policy

8.1 The e-mail facility is for business use only. The e-mail address allocated to an employee should not be used for personal purposes.

8.2 No free e-mail facility should be used to receive or send business-related information.

8.3 No non-business-related newsgroup may be added to your organization's e-mail address book.

8.4 The e-mail facility of the organization should not be used to spam other users, whether they are inside or outside the organization.

8.5 No harassing or insulting messages should be sent inside or outside of the organization.

8.6 No person is allowed to forward chain letters or pyramid schemes using corporate e-mail.

8.7 No confidential document belonging to the organization may be sent to anyone, including to your own personal freemail account.

8.8 If sensitive information needs to be sent to someone outside the organization, proper measures should be taken as specified by the System Administrator.

a. Encryption of file/data, this helps in limiting the shared data access to those who have the encryption key.
b. Use of Secure Cloud Services for File-Sharing (Microsoft OneDrive) It ensures the data is shared safely and securely to intended recipient by entering the email address of that user & prevents sending files to unauthorized users.
c. Use of End-to-End Encryption secure tunnel: sharing the data to client/outsiders through secure VPN tunnels.

8.9 The organization's e-mail address can be used when posting to business-related newsgroups provided permission is obtained from the respective manager.

8.10 An e-mail program such as Outlook should not be running when employees leave at the end of the workday, as hackers may misuse it.

D. Enforcement

In the case of a violation of the security policy, disciplinary action will be taken, up to and including employment termination.

E. Responsibility

All employees, Departmental Managers and System Administrator.

9. Login Policy

A. Purpose

This document specifies the organization policy relating to login to critical machines and it discusses in detail the related standards.

B. Scope

The scope of the policy includes all logins to critical applications and servers, irrespective of their operating platforms.

C. Policy

9.1 Every user should have a uniquely assigned login name and password to access corporate computer systems.

9.2 Each person is responsible for the login name assigned to him/her

9.3 A password should not be displayed on the screen.

9.4 In the case where an incorrect login name or password is entered, no response which reveals any information should be given. For example, systems should not respond with "Incorrect Password for xxx login name". This message will reveal that such a valid username exists leaving the attacker having only to crack the password.

9.5 The system should log-off (lock) automatically after inactivity of 10 minutes or a period specified by the System Administrator.

9.6 In the case where a job function is based on a general USER ID, the USER ID should be changed to a unique one.

9.7 Time-based access should be implemented for the user login, where possible.

9.8 All login names and privileges should be reviewed at regular intervals in close co-operation with the Human Resources functions.

9.9 A login which is not successful should be logged and the log reviewed at regular intervals.

9.10 A login ID not used for 90 days will be disabled and later disabled with the permission of the employee's Department Manager.

D. Enforcement

In the case of a violation of the security policy, disciplinary action would be taken, up to and including employment termination.

E. Responsibility

All employees, Departmental Managers and the System Administrator.

10. Password Protection Policy

A. Purpose

This document specifies the organization policy related to password protection, change and maintenance.

B. Scope

The scope of the policy includes all employees, irrespective of their position.

C. Policy

10.1 All default passwords should be changed by the user prior to use of the system.

10.2 Password strength should at least be 8 characters long, made up of a mixture of alphabetic (upper case and lowercase), numeric and alpha numeric characters/symbols.

10.3 A password should be changed every 45 days or whenever compromised.

10.4 No common name or personal information should be used as a password e.g. date of birth, spouse's name, pet name or phone number.

10.5 A password should be different from the last 3 passwords.

10.6 A password should always be kept secret and should never be disclosed to co- workers and colleagues.

10.7 All PCs should have the login password enabled.

10.8 No person should leave his/her PC or terminal without logging off or password protecting the screen.

10.9 The initial password is given by the System Administrator which is changed by the user to login to the system.

D. Enforcement

In the case of a policy violation, disciplinary action will be taken which may include the termination of employment.

E. Responsibility

All employees, Departmental Managers

11. Firewall Security Policy

A. Purpose

Network Routers and Firewalls are the most vulnerable components of network security. This document provides the minimum-security protection for the firewalls.

B. Scope

The scope covers the firewall and routers of the network.

C. Policy

11.1 Routers and firewalls should be placed in a physically secure area.

11.2 The firewall management terminal should be separate from the main box.
11.3 The password for firewalls should match the restrictions of Password Policy.
11.4 The Firewall should be a dedicated machine. It should not be used to run any services other than related to firewall and protection.
11.5 Routers and firewalls should disallow all invalid IP addresses coming from the Internet
11.6 Routers and firewalls should not allow IP broadcasts.
11.7 The firewall should be configured to stop SYN attack.
11.8 Firewall should stop IP spoofing, fragmented packets, and teardrop.
11.9 The relevant Department Manager should approve the list of Access rules prior to deployment of routers.
11.10 The backup of the configuration files of the firewall should be stored at a safe place.
11.11 The firewall must hide all internal network addresses from the outside world.

D. Enforcement

In the case of a policy violation, disciplinary action will be taken which may include the termination of employment.

E. Responsibility

Network administrator, Firewall administrator

12. Virtual Private Network (VPN) Policy

A. Purpose

The purpose of the VPN policy is to provide guidelines for secure remote access to the local networks.

B. Scope

The VPN policy applies to connections to the organization and to third parties including consultants, vendors and contractors.

C. Policy

12.1 As VPN is an extension of the corporate network, all of the security rules apply to the remote client as if they were within the organization.
12.2 All critical connections to the outside should use the safe channel. Corporate choice is to use SSL for VPN, where available.
12.3 It is highly recommended that a one-time password be used.
12.4 "Tunnel Mode" is preferred whenever the VPN is used. If performance is an issue, "Transport Mode" may be used.
with the permission of the System Administrator.
12.5 All files transferred through VPNs should be subject to antivirus scanning.
12.6 The VPN timeout period is 300 seconds of inactivity.

D. Enforcement

Any Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibility

Network administrator, VPN user and the System Administrator.

13. Wireless Communication Policy

A. Purpose

The Purpose of the policy is to provide guidelines for network connections via wireless communication.

B. Scope

The policy covers all wireless devices such as mobile phones, PDA and laptop computers and others, which are connected to the organization corporate network.

C. Policy

13.1 The System Administrator should approve all wireless devices connected to the corporate network.

13.2 A Wi-Fi Controller should be used to grant permission to the wireless devices.

13.3 Prior to the granting of a connection to the network devices, it would be preferable that the Wi-Fi controller verify the hardware level address check the MAC address.

D. Enforcement

Any Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

Equipment user and the System Administrator.

14. General Physical Security Policy

A. Purpose

This policy specifies the requirements for physical security. No matter how good the security solutions and products are, if physical security is weak, everything can be compromised.

B. Scope

This policy is applicable to all physical areas of the office/s of the organization, including those available now and those which may be added in the future.

C. Policy

14.1 The Operations Manager should define security zones within the organization as per industry requirement.

14.2 The Operations Manager should apply appropriate measures for each of the zones.

14.3 Office floor plans and diagrams of telephone, electrical, water and network cabling lines, as well as extinguisher locations should be documented and maintained.

14.4 A proper Access Control List with corresponding work times should be maintained.

14.5 The entrance of the organization should be properly guarded.

14.6 Proper fire prevention and detection mechanisms should be in place.

14.7 A Telephone Directory for emergency phone numbers should be maintained and must be easily accessible.

14.8 A First Aid Box should be provided and must be easily accessible and regularly checked and replenished.

14.9 All areas of the office should be properly lighted

D. Enforcement

A Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

Operations & HR Department/representative.

15. Computer Room/Data Center Security Policy

A. Purpose

This policy discusses the requirements for safeguarding the computer systems and personnel operating in the computer room/data center.

B. Scope

This policy is applicable to all physical areas of the office/s of the organization, including those which are available now and those which may be added in the future.

C. Policy

15.1 Access to the computer room will be restricted to organization authorized persons only.

15.2 No public visits or tours of the computer room are allowed.

15.3 Vendor and third-party representatives, if they visit the room, should be escorted.

15.4 A proper fire alarm and fire extinguisher system should be in place.

15.5 A proper temperature should be maintained and monitored.

15.6 A proper Emergency procedure for the computer room should be developed and be easily accessible. Personnel should be trained so that the procedure is executed efficiently, when required. All procedures should be audited at regular intervals. (To make Emergency Procedure document)

15.7 The System Administrator will co-ordinate the development of computer room standards.

15.8 The System Administrator will co-ordinate measures to ensure that a reliable power supply to the computer room is in place and that adequate safeguards are there to protect the equipment.

15.9 No drinking, eating or smoking is allowed in the computer room.

15.10 Use of a cellular phone is prohibited in the data center.

D. Enforcement

A Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities System Administrator.

16. Magnetic Media Policy

A. Purpose

This policy discusses the requirements for the handling of Magnetic media.

B. Scope

This policy is applicable to all portable media

C. Policy

16.1 An inventory of all critical magnetic media should be maintained and kept in the secure magnetic media library.

16.2 All magnetic media should be properly labeled.

16.3 All magnetic media should be physically destroyed prior to discarding.

16.4 All media should be scanned for viruses prior to use.

D. Enforcement

A Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities System Administrator.

17. Server Security Policy

A. Purpose

This security policy discusses the issue of securing the internal servers of the organization. This is to make sure that there is no unauthorized access to corporate information.

B. Scope

This policy applies to all servers either owned or operated by the organization.

C. Policy

17.1 The Server should be in a physically secure place.

17.2 All configuration of the servers should be documented and approved by the IT Manager and System Administrator.

17.3 All Change Management Policies should be strictly implemented on the servers.

17.4 The System Administrator should approve all configuration of servers.

17.5 Services not required, such as the web server and others, should be disabled.

17.6 The Log of the server should be monitored on a regular basis, as specified by the System Administrator.

17.7 All security patches should be installed on the server after confirmation that they will not have any adverse effect on the running applications.

17.8 All guests and default accounts will be either disabled or their password changed.

17.9 If remote management of the server is required, a secure channel should be used for this purpose.

17.10 The privileged account like super user and root should only be used when required.

17.11 A regular Audit would be performed by the System Administrator

D. Enforcement

A Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

System Administrators, System Administrator and IT Manager.

18. Configuration Management Policy

A. Purpose

This security policy deals with proper documentation for the configuration of critical systems.

B. Scope

This policy applies to all servers, network equipment and others, either owned or operated by the organization.

C. Policy

18.1 All system configurations, including hardware, software and core business software should be documented.

18.2 There should be a hard copy and a soft copy of the documentation.

18.3 Configuration Management should be considered as the documentation baseline. All change from this baseline should be documented as per the Change Management Policy.

18.4 Prior to roll out, any modification made to the default configuration should be documented in the configuration management documentation.

18.5 The System Administrator should approve all configuration documentation.

18.6 Configuration management and change management documentation should be used together, in case of recovery.

D. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

System Administrators, System Administrator and IT Manager.

19. Change Management Policy

A. Purpose

This security policy sets out the proper change management documentation for all critical systems.

B. Scope

This policy applies to all critical servers, network equipment and business-critical software owned or operated by the organization in the Non-GxP Environment.

C. Policy

19.1 Standardized methods and procedures should be used for the efficient and prompt handling of the changes and revision control.

19.2 All changes should be documented, and prior approval must be obtained for all changes made to critical production systems.

19.3 A "Change Request" should be presented to the relevant manager for approval. The System Administrator will coordinate the workflow for change approval.

19.4 All requested changes should be evaluated and have their impact assessed before approval or disapproval.

19.5 All changes, once approved, should be scheduled in such a way as to ensure the availability of a time slot for a rollback, should something unexpected happen.

19.6 Documentation for a change request should be accompanied by detailed, step-by-step procedures to do the change. It should also include detailed rollback procedure, in case the change fails, and the desired result is not achieved.

19.7 Whenever there is a need to change the application software, system software, LAN or any hardware, the change should be appropriately authorized and approved.

19.8 Every change should be thoroughly tested and fully documented.

19.9 Changes should be made when there is minimum or no activity on the system. In cases where there is more than one change to be carried out at a given time, the changes should be queued on the basis of business and technical priority.

19.10 Changes should only be approved after adequate consideration of the associated impact and implications.

19.11 Changes, once accepted, should be entered into the Change Management log.

19.12 The Change should be fully tested, and the result presented to the respective manager.

19.13 A Change Management Summary report should be presented to higher management once the changes are implemented.

D. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities System Administrator.

20. Printed Output and Distribution Policy

A. Purpose

This security policy sets out the requirements for printed output and its distribution.

B. Scope

This policy applies to all critical servers, network equipment and business-critical software owned or operated by the organization.

C. Policy

20.1 The System Administrator will ensure that a procedure exists that ensures that the report goes only to the authorized individual.

20.2 The person who prints the report is responsible for ensuring the proper protection of the information it contains.

20.3 Should someone find a report that is classified and is not intended for him/her, s/he should inform the System Administrator.

D. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

Report Printing User, System Administrator

21. General Business Continuity Policy

A. Purpose

The purpose of this policy is to provide directions regarding business continuity.

B. Scope

This policy applies to all business-critical systems as referred to in the Business Impact Analysis and Risk Assessment in the Ind-Swift Security Policy.

C. Policy

21.1 The System Administrator will ensure that the availability of the business-critical system is ensured as per the Risk Assessment requirement of the Corporate Policy.

21.2 Depending on the Risk Assessment report (as per the Ind-Swift Security Policy), Senior Management will decide the scope of the recovery plan.

21.3 Crucial systems, as per the risk assessment, should have reliable recovery procedures in case of disaster.

21.4 The word “Disaster” needs to be defined, and the respective risk evaluated by senior management. The System Administrator should coordinate this task.

21.5 All documentation related to business continuity should be regularly updated.

21.6 The Information Security Manager will ensure that there is an appropriate Contingency plan, and "Emergency Response Plan” are in place.

D. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

Business Department Heads, System Administrator, and IT Manager.

22. Backup and Recovery Policy

A. Purpose

This security policy specifies the backup and recovery standards for the organization.

B. Scope

This policy applies to all critical servers such as database servers, application servers and network equipment such as firewall’s configuration owned or operated by the organization.

C. Policy

22.1 Backup of all critical devices including servers and network equipment should be undertaken.

22.2 Frequency of the backup will be decided according to the nature of the application being used.

22.3 The backup method to follow is "Full Backup".

22.4 The timing of "Distributed Backups" should be planned to have the minimum impact on the corporate network.

22.5 The backup process should not violate the confidentiality of the system.

22.6 No public computers should be used for backing up sensitive data.

22.7 All archive data must be tested on a regular basis.

22.8 All backups should be verified to check the validity of the media.

22.9 A copy of critical data should be stored in a remote location.

22.10 A remote location can be a branch office of the organization located in a different city /country.

22.11 The data stored in a different location should be used in case of disaster occurring at the site level.

22.12 Once the backup media is no longer usable, it should be physically destroyed or preferably burnt.

D. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

All employees, System Administrator and IT Manager.

23. Personnel Policy

A. Purpose

This security policy specifies guidelines and standards related to Human Resource (HR) with special reference to Information Security.

B. Scope

This policy applies to all permanent and contract employees.

C. Policy

23.1 Prior to hiring a prospective employee, HR must do a background check, contact references and validate the education testimonial.

23.2 Employees should sign the undertaking accepting responsibility for adherence to security policies.

23.3 HR will ensure that security responsibility is included in the job responsibilities of the employee.

23.4 The Terms and Conditions of employment shall mention the Information Security policy for each employee.

23.5 HR will ensure that segregation of duties and job rotation is implemented, where possible.

23.6 When an employee leaves the employment of the company, HR will ensure that an exit interview is conducted.

23.7 HR will ensure that the person has all computer accounts removed prior to his/her final settlement.

23.8 In the case where employment is terminated without the consent of the employee, he/she should be escorted from the premises.

D. Enforcement

A Policy Violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

HR, System Administrator and Department and IT Manager.

24. Third Party Policy

A. Purpose

This security policy specifies the standard and guidelines for third party and outsourcing.

B. Scope

This policy applies to parties whether they are vendors, contractors, consultants, or outsourced professionals.

C. Policy

24.1 The Risks associated with third party involvement and outsourcing should be identified and appropriate measures taken to address them.

24.2 A non-disclosure agreement is essential before sensitive information is shared with a third party.

24.3 The role and responsibilities of the third party should be clearly defined.

24.4 Third party access to the corporate computer system will be given only after the signing of a formal contract which should contain all security requirements by which the third party is to abide.

24.5 All Third party and external users, if defined on the system, should have a mandatory expiry date.

24.6 Third party or outsourced tasks which require dial-in and dial-up privileges, should be restricted and monitored.

D. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination. For third party it may lead to contract termination.

E. Responsibilities

Department Heads, HR, System Administrator and IT Manager.

25. Equipment Safeguard Policy

A. Purpose

To ensure maximum safekeeping of the Company's Laptop/Devices and Data.

B. Scope

This policy applies to all permanent and contract employees to ensure before their scheduled travel date to include the following equipment and data security safeguards to their travel planning routines.

C. Policy

25.1 Leave your data and/or device at home. The best way to safeguard your data or device is to not bring them on the trip. If you don't need to access data stored on your laptop/device leave your laptop/device in a secure location at home or deposit it back with the company.

25.2 Backup your data. In the case of travelling with laptop/device, the employees should always take backup of their data. In case the employee loses the data along with the device or some malware corrupts the data during the trip, the employee is sure of having a good copy from which the data can be recovered.

25.3 Configure device. The following requirements are critical for foreign travel:

25.3(1) install and update anti-malware software

25.3(2) choose strong passwords

25.4 Do NOT leave your device unattended. Physically having control of your device is the easiest way for someone to access your data. Do not leave your device unattended, lend it to someone you just met or leave it in your checked bag on your flight. If you ever leave your computer, make sure to turn it off instead of just hibernating it or putting it to sleep.

25.5 Do NOT enter your credentials into public computers. Public computers such as hotel business center workstations and internet cafe computers are often poorly managed and provide minimal security protection for its users. If the need to use public computers arises during your travel, avoid entering your credentials at these public computers.

25.6 Connect only to known wifi networks. It's tempting to stay in touch with friends and colleagues as you travel by connecting to wifi networks. However, anyone can create a network and give the network a legitimate sounding name, hoping to lure unsuspecting travelers to connect while capturing personal information transmitted through the network. This is especially prevalent at public cafes, hotel lobbies and airports. When connecting to a network, find out the correct network name from the staff at the business and connect to it.

25.7 Turn off your wifi when not in use. Attackers can easily spoof Wifi network names to connect to devices within range for eavesdropping. To help you avoid accidentally connecting your device to rogue wifi networks at a later time, once you are finished using the network, turn off wifi on your device.

25.8 Practice safe web browsing. The websites you visit online hold valuable data about you. They are also becoming gateways through which hackers can steal your data by infecting reputable or seemingly reputable websites with malware. This threat is magnified during foreign travel as you connect to public networks in hotels, airports, cafes, etc. at your destination.

25.9 Do not click on suspicious links or prompts. Malicious websites commonly craft attacks to exploit a user's curiosity, impatience or to scare them with malware threats. These malicious attacks might come in the form of links or pop-ups that present free offers too good to be true or imminent malware infection if you don't install the product. Think before you click a link or "Yes" to a prompt.

25.10 Clear browsing session information when using devices that do not belong to you. Some web applications do not log you out entirely, even when clicking the logout button or closing the browser. Such behavior allows the next person who uses the device to browse to the same page or click the back button to access your data as if you are still login. To prevent others from accessing your account and data, clear all the web browser session information.

25.11 Take note of credentials you are using during the trip. Regardless of whether you are using them on your device or public computer, they may be compromised. To be safe, take note of the credentials you used so you can change them on a trusted and secure device once you return. Employees need to be mindful that all equipment's which they use or has been issued to them to perform their jobs is owned by organization. It is the individual responsibility of all employees to care for and safeguard the equipment issued to them and keep it in as close as new condition as possible.

25.12 It is the responsibility of the employee to notify the company immediately of loss/damage/theft of the item(s), as to the occurrence and/or explanation thereto. If the item(s) have been stolen, the company also requires the employee to complete an Affidavit at their nearest Police Station immediately and forward the original docket to the company.

25.13 The company may deduct from the employee the cost of equipment lost/stolen within a reasonable time, if the employee committed theft or was negligently responsible for the loss.

D. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination. For a third party it may lead to contract termination.

E. Responsibilities

Department Heads, HR, System Administrator and IT Manager.

26. Personnel Exit Access Policy

A. Purpose

This document specifies the organization policy relating to employees separating from the company and the non-reporting employees who have access to the corporate system, and it discusses in detail the related standards with process to be followed. B. Scope

The scope of this policy includes all employees' and contractors' (henceforth, referred to Ind-Swift Laboratories Ltd. employees) logins, access revocation to corporate systems, example: applications, servers and client systems.

C. Policy

26.1 Managers/Head of Department are responsible for notifying the IT team to disable the credentials and access of an employee separating from the company on or before the employee's last working day in the organization.

26.2 Managers/ Head of Department are responsible for notifying the IT Team for retrieval of any corporate assets (Laptop, Mobile Phone etc.) and client assets.

26.3 Upon termination of employment or a new third-party contractor engagement, the IT team should be immediately informed either by the HR Department or the concerned Department Head.

26.4 All access rights to the organization's systems, networks, and data shall be revoked immediately upon the employee's exit from the organization. Once access is revoked, no exit employee or contractor can access the organization's systems, networks, or data.

26.5 The Delivery Manager is responsible for the particular project or engagement with the respective client and to inform the client about the employee's exit.

26.6 The Delivery Manager will ensure that all client-specific access and credentials associated with the departing employee are revoked and confirm the completion of this process to the client.

26.7 Revocation of access to an application that is not managed by the IT Team must be raised as a separate request with the application asset owner.

26.8 In case of an Account Extension request from the Manager, it must be raised via Helpdesk portal with the approval from Department Head and the following details need to be furnished: a. Purpose of extension

b. Duration

c. Project

26.9 The extension of domain account/System login & email account should not exceed more than 30 days.

26.10 Extension to backup/SharePoint folders should not be more than 90 days.

26.11 If the backup of any data is not requested by the Delivery Manager or Department Head, the IT team would consider it as least important and will wipe the exit user data.

26.12 HR or Department Heads must inform Operations team for disabling the access to Work area.

D. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

Department Heads, HR, System Administrator and IT Manager.

27. Cloud Usage Policy

A. Purpose

This policy establishes the framework for the secure selection, acquisition, use, and exit from cloud computing services. It ensures that all cloud services align with the organization's information security objectives and manage risks associated with cloud computing.

B. Scope

This policy applies to all employees, contractors, and third-party users involved in the use of cloud services for business purposes across the organization. It supports compliance with applicable legal, regulatory, and contractual requirements.

C. Policy

27.1 Selection of Cloud Services

a. Risk Assessment: Conduct information security risk assessment as per ISMS Standards before selecting any cloud service.
b. Due Diligence: Evaluate the cloud provider's compliance with ISO/IEC 27001, SOC 2, GDPR, or other relevant frameworks.
c. Security Controls Review: Ensure the provider has implemented adequate controls for:
    i. Data encryption (at rest and in transit)
    ii. Identity and access management
    iii. Backup and disaster recovery
    iv. Incident response procedures
d. Service Level Agreements (SLAs): SLAs must include:
    i. Uptime and performance guarantees
    ii. Incident notification timeframes
    iii. Data location and residency assurances

27.2 Acquisition of Cloud Services

a. Approval Process: All cloud acquisitions must be approved by the IT Manager and organization management.
b. Data Classification: Cloud services must be matched to the classification level of data they will handle (public, internal, confidential, etc.)

27.3 Use of Cloud Services

a. Access Control: Only authorized users may access cloud services. Access must be role-based and reviewed periodically.
b. Monitoring: Cloud usage must be monitored for unauthorized access, data leakage, or unusual activities.
c. Training: Users must be trained on secure cloud usage and the risks associated with storing sensitive data off premises. (Project Manager will identify the training needs and Trainings will be imparted by CQM Team.
d. Incident Management: Any security incident involving a cloud service must be reported and managed per the organization's incident response policy.

27.4 Identity & Access Management (IAM)

a. Enforce RBAC or ABAC to grant the least privilege necessary.
b. Apply MFA for all access—critical control to prevent credential misuse.
c. Review access permissions at least every 3 months.

d. Remove generic/test accounts and enforce account lockout after repeated failures. (We need to updated this period check list and start preparing the report).

27.5 Data Encryption & DLP

a. Encrypt data at rest and in transit across all providers with cloud-native KMS/HSM services & TLS 1.2 above.
b. Implement data governance frameworks to address compliance across regions, as applicable.

27.6 Network & Perimeter Security

Apply network segmentation and least-access models.

a. AWS: VPCs, Security Groups, NACLs, AWS WAF, Shield
b. Azure: Azure Firewall, Application security groups, Segmentation and routing (As needed)

27.7 Logging & Monitoring

a. Audit Logs & Sign in Logs maintained for last 30 Days.
b. Event logs are maintained for the last 90 days.

27.8 Backup, Recovery & Incident Response

Sustain business continuity and secure recovery.

a. AWS: AWS Backup, S3 Glacier
b. Azure: Azure Backup + Site Recovery
c. Requirement: RTO/RPO & DR tests should be matched Backup and Restoration Plan.

27.9 Exit from Cloud Services

a. Exit Planning: An exit strategy must be defined during the acquisition of new cloud services.
b. Data Migration: Ensure secure transfer of data to internal systems or another cloud provider.
c. Data Sanitization: Verify that all organizational data is permanently deleted from the cloud provider's environment.
d. Access Revocation: Disable all users and administrative access to the cloud service upon exit.
e. Audit & Verification: Conduct a final security audit or assessment to confirm no data or access remnants exist.

D. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

Department Heads, HR, System Administrator, IT Manager, End Users, Legal & ISO.

28. Web Filtering Policy

A. Purpose

This policy defines the configuration and enforcement of web content filtering for users accessing the internet through the organization's network. It aims to ensure appropriate internet use, maintain productivity, and reduce exposure to security threats.

B. Scope

This policy applies to all employees, contractors, and authorized users accessing the internet through the organization's network infrastructure.

C. Policy

28.1 Web Filter Profiles

The following web filter profiles are configured and applied within the network to enforce differentiated access control based on department, risk, or use case:

a. AI Tools block – Restricts access to unapproved AI tools and platforms.
b. LDAP_FULLACCESS – Grants full web access to authenticated LDAP users.
c. Social Sites – Applies restrictions to social networking and media platforms.
d. Wi-Fi Full Access – Grants unrestricted access over wireless networks.
e. default – Default policy profile for general internet usage.
f. Wi-Fi-default – Default profile applied to wireless users with standard restrictions.

28.2 Web Access Categories

Allowed:

a. Business-related content
b. Government and public service websites
c. Educational and training resources
d. Vendor and partner portals Blocked:
a. Malicious sites (phishing, malware, command & control)
b. Adult content
c. Gambling and betting
d. Illegal downloads or torrents
e. Proxy or anonymizer services
f. Cryptocurrency mining sites
g. Hate speech or extremist content
h. Unauthorized cloud storage or file sharing (e.g., personal Dropbox, WeTransfer)

28.3 Categorized Content Monitoring / Restricted

The following web categories are set to Monitor mode, which logs activity but does not block access: a. Web Host Rating

b. Web-based Email
c. Web-based Applications
d. Dynamic Content
e. Advertisements
f. Web Analytics
g. Online Meeting Platforms
h. Social media (e.g., allowed for Marketing, blocked for others)
i. Video streaming (e.g., allowed for certain roles)
j. Shopping and personal email (e.g., Gmail, Outlook.com)

28.4 Exceptions & Whitelisting

a. As per the business requirements custom filter/Blocking policies defined.
b. Business critical exceptions may be requested through IT Security.
c. Requests must be approved by a department head and reviewed by the IT or delegate.
d. Exceptions will be logged and reviewed periodically.

28.5 User Notifications

Users attempting to access blocked websites will receive a block page with the reason.

28.6 Technical Controls

Web filtering enabled via

a. Firewall based URL filtering
b. Endpoint protection software

28.7 Logging & Alerts

Content filtering logs are retained and reviewed by the IT Security team on a periodic basis to detect inappropriate use and maintain compliance.

28.8 Acceptable Usage Policy & User Awareness

All users are expected to adhere to acceptable use standards when accessing the internet. Violations of this policy may result in access restrictions and disciplinary actions. Regular awareness training and mailers related to IT Do's and Don'ts should be delivered.

D. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

Department Heads, HR, System Administrator and IT Manager.

29. Data Masking Policy

A. Purpose

This policy aims to protect sensitive data in non-production or limited-access environments by using various masking techniques, while maintaining data utility and supporting regulatory compliance.

B. Scope

This policy applies to all full-time permanent, temporary, contractors and other third parties who are generating or handling reports of Ind-Swift Laboratories Ltd. containing sensitive data (e.g., PII, financial data, client information). This includes reports shared with internal or external stakeholders where data must be protected through irreversible redaction.

C. Policy

29.1 Method:

a. Sensitive information is permanently redacted in files before distribution.
b. Irreversible: Redacted content cannot be restored.
c. Manual or semi-automated: Redaction can be done via tools (e.g., Adobe Acrobat, LibreOffice).
d. No sensitive data should remain in metadata, comments, or hidden layers. Please refer to the annexure Redaction Guidelines for detailed information.

29.2 Process

a. Identify: Determine which fields in the report contain sensitive information.
b. Redact: Use approved redaction tools to permanently black out or remove sensitive content.
c. Validate: Ensure redacted do not contain the original data in metadata or behind the redaction layer.
d. Archive: Maintain a copy of the redacted version for audit or distribution.
e. Audit Logs: Keep records of redaction actions where required.

29.3 Security & Compliance

a. Store original (unredacted) files securely and restrict access.
b. Ensure redaction tools are correctly configured to remove the underlying text.

c. Review redaction practices annually or during audits.

d. Redacted data must comply with data protection laws (e.g., GDPR, HIPAA, PCI-DSS) by ensuring non-disclosure of sensitive details.

D. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

a. Data Owners: Identify sensitive fields requiring redaction; approve redaction formats.

b. IT/Security Teams: Provide standard redaction guidelines, templates, and ensure consistent application across reports.

c. Report Generators (HR, Finance, Operations, Developers): Apply redaction to sensitive fields before sharing/exporting reports.

d. Auditors: Verify redacted reports and ensure sensitive content cannot be restored from metadata or document history. Department Head/manager must double-check & ensure sensitive content cannot be restored from metadata or document history before sharing the reports.

30. Data Encryption Policy

A. Purpose

This policy defines requirements for encrypting sensitive data in order to protect confidentiality, integrity, and availability of organizational information, both at rest and in transit.

B. Scope

This policy applies to all the employees, contractors, and third-party users of Ind-Swift Laboratories Ltd., all its organizational systems (onpremises, cloud, mobile) and all sensitive data including client information, Employee personal information, financial records, intellectual property, and authentication credentials.

C. Policy

30.1 Encryption Requirements

All data must be classified under one of the following categories:

Sr. No.	Description	Data Classification	Encryption at Rest	Encryption in Transit
1	Strategic backups	Class A	Required (AES-256)	Required (TLS 1.2+)
2	Network Security	Class A	Recommended	Required
3	Asset Inventory	Class C	Recommended	Recommended
4	Incident Management	Class C	Recommended	Recommended

30.2 Encryption at Rest

a. All sensitive data at rest must be encrypted using approved algorithms (e.g., AES-256). b. Encryption must be enforced on:

i. Full disk encryption on all computers, mobile devices, servers. Windows: BitLocker macOS: FileVault Mobile: Native OS encryption ii. cloud storage (for example OneDrive, SharePoint, AWS S3, etc.) as applicable

iii. Removable media (USB Devices) are blocked by default.

Exception - USB Drives or External Storage media are being used by IT in following scenarios:

- Moving the files between the systems which are not connected to Network
- Storing the Backup copy of critical Data
- Creating a installation of recovery drive

c. Considering the above use cases, all External HDDs and USB drives used by IT must be in NTFS or exFAT format and encrypted with AES-256 standards.

OS Platform	Encryption Tool
Windows	BitLocker
MacOS	FileVault
Linux	LUKs

d. Encryption password must comply with Password Policy

e. Encryption key must be stored securely.

30.3 Encryption in Transit

a. All data in transit over public or untrusted networks must be encrypted using TLS 1.2 or higher. b. Encrypted protocols must be used:

i. HTTPS (not HTTP)

ii. Secure SMTP (TLS), IMAPS, SFTP/FTPS

iii. SSL VPNs for remote access iv. Secure IPV4 Tunnels

D. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

Department Heads, System Administrator and IT Manager.

31. Data Leakage Prevention Policy

A. Purpose

This policy defines the requirements for Data Leakage Prevention (DLP) to prevent unauthorized disclosure, transmission, or loss of sensitive or confidential data, whether data in transit, at rest or in use. The policy aims to prevent unauthorized transmission or exposure of sensitive data and to monitor and control data flows within and outside the organization. This policy ensures compliance with regulatory and contractual data protection obligations and supports the principles of confidentiality, integrity, and availability of information assets.

B. Scope

This policy applies to all employees, contractors and consultants of Ind-Swift Laboratories Ltd. and to all its organizational assets including laptops, desktops, mobile devices, servers, emails, storage platforms, SaaS applications, cloud services, including all forms of sensitive data (personal data, financial records, intellectual property, and business-critical information).

C. Policy

31.1 Data Classification

a. All data must be classified according to the organization's Information Classification Document.

b. DLP rules shall be aligned with classification levels (Public, Internal, Confidential, Restricted).

31.2 DLP Implementation

a. DLP solutions shall be deployed at the endpoint, email gateway, network, and cloud levels.
b. All internet-facing channels, including web upload, email, and file-sharing applications, must be monitored for sensitive data exfiltration.

31.3 Control Coverage

Data State	Control Measures
Data in Transit	Monitor outbound emails, file uploads, and cloud sync. Encrypt email content when needed.
Data at Rest	Scan servers, databases, file shares, and endpoints for sensitive data. Take corrective actions (e.g., encrypt, isolate, or delete).
Data in Use	Prevent copy/paste, print, screen capture, and USB transfer of protected data on endpoints.

31.3 Acceptable Use Guidelines

Employees must adhere to the following:

a. Do not send sensitive data (e.g., PII, financial info) through unencrypted email or unauthorized tools.
b. Avoid saving confidential files on personal devices or cloud services not approved by IT.
c. Use secure sharing platforms authorized by the organization.
d. Do not bypass or disable DLP controls on managed systems.

31.4 Incident Handling and Reporting

a. All suspected DLP violations must be reported immediately via the Incident Reporting Procedure.
b. Investigations shall be led by the Information Security Officer in collaboration with relevant stakeholders.
c. Root cause analysis will be conducted for confirmed incidents, and appropriate corrective actions will be implemented.

D. Enforcement

A Policy violation will be subject to disciplinary action, which may go so far as employment termination.

E. Responsibilities

Role	Responsibility
Information Security Officer	Define DLP policy, review violations, and ensure compliance.
IT Team	Deploy and maintain DLP solutions, apply updates, and ensure system integrity.
Data Owners	Classify and manage the lifecycle of sensitive data.
Employees/Users	Comply with the DLP policy, avoid sharing sensitive data, and report suspicious activities.

32. Hardware Management Policy

Purpose

This policy establishes requirements for the acquisition, configuration, security, tracking, usage, maintenance, refresh, end-of-life, and disposal of all hardware assets at Ind-Swift Laboratories Ltd., supporting ISO 27001:2022 compliance.

Scope

This policy applies to all laptops, desktops, MacBooks, mobile phones, tablets, servers, switches, firewalls, IoT devices, CCTV systems, external storage media, and any hardware that stores, processes, or transmits company information.

Policy

32.1 Asset Acquisition

- All hardware must be procured only through the IT Department.
- Business justification and management approval are mandatory.
- Only approved vendors and OEM-authorized sources may be used.
- Shadow IT procurement is strictly prohibited.

32.2 Configuration Standards

- All devices must be configured by IT before allocation.
- Mandatory controls include OS hardening, update installation, endpoint protection, disk encryption, removal of default credentials, and disabling unused ports.
- Network devices must follow secure baseline configuration.

32.3 Asset Tracking & Ownership

- IT shall maintain an updated Asset Register with serial number, asset tag, user assignment, warranty, and lifecycle details.
- Every asset shall have an asset tag; users must not tamper with tags.
- Physical verification shall be conducted bi-annually.

32.4 Hardware Security Controls

- All devices must be password/PIN protected and encrypted.
- Laptops must auto-lock after 10 minutes of inactivity.
- Only authorized external devices (by IT) may be used.
- Servers and network equipment must be stored in secure, access-controlled rooms.

32.5 Acceptable Use

- Hardware must be used for official purposes only.
- Unauthorized software installations and configuration changes are prohibited.
- Loss, theft or damage must be reported immediately.

32.6 Patch, Firmware & Update Management

- Critical patches must be applied within 7 days.
- Firmware updates must follow IT maintenance schedules.

32.7 Refresh / Replacement Cycle

- Laptops: 3–4 years
- Desktops: 4–5 years
- Mobile devices/Tablets: 2–3 years
- Network devices/Servers: 5 years

• Exceptions require manager approval.

32.8 Repairs & Maintenance
• All repairs must be performed by IT or authorized OEM partners.
• Data backup and secure wipe mandatory before sending devices for repair.
• Loaner devices may be issued.

32.9 End-of-Life & Disposal
• All EOL hardware must undergo secure data wiping using certified wiping tools.
• Highly sensitive media must be physically destroyed.
• Disposal must be documented and handled via certified e-waste recyclers.

Enforcement
Violations of this policy may result in disciplinary action, up to termination.

Responsibilities
• IT Department – procurement, configuration, tracking, updates, disposal.
• Information Security Team – compliance monitoring.
• Employees – secure and appropriate usage of assigned devices.

33. Internal Service Level Agreement (SLA) Policy

Purpose
This policy defines timelines, responsibilities, and priority levels for handling internal IT service requests raised via email, ensuring timely resolution and consistent service delivery across Ind-Swift Laboratories Ltd.

Scope
This policy applies to all employees, departments, contractors, and IT support staff handling internal IT incidents, service requests, access issues, hardware/software support, and operational IT needs.

Policy

33.1 Communication Method
• All IT support requests must be submitted exclusively through the official IT Support Email.
• Verbal, WhatsApp, SMS, or informal requests are not covered under SLA timelines.

33.2 Priority Definitions and SLA Timelines
Priority 1 – Critical
Description: Major business impact; systems down; no workaround.
Examples: Server outage, ERP failure, production stoppage.
Response Time: 15 minutes
Resolution Time: 4–8 hours

Priority 2 – High
Description: High impact; key operations affected.
Examples: Email failure, VPN issues, laptop failure.

Response Time: 1 hour
Resolution Time: 8–24 hours

Priority 3 – Medium
Description: Work impacted but functioning continues.
Examples: Application errors, printing issues.
Response Time: 4 hours
Resolution Time: 1–3 business days

Priority 4 – Low
Description: No business interruption.
Examples: Software installation, minor issues.
Response Time: 1 business day
Resolution Time: 3–7 business days

Priority 5 – Planned Requests
Description: Scheduled tasks.
Examples: New user creation, system upgrades.
Response Time: Within 2 days
Resolution: As per planned schedule

33.3 Request Handling Workflow
• User sends email request with issue details.
• IT acknowledges request within SLA timelines.
• IT assigns priority, investigates, and resolves.
• User is informed upon resolution.
• IT logs all email-based requests in internal records.

33.4 Responsibilities
IT Support Team:
– Respond and resolve issues as per SLA.
– Maintain internal issue logs.
– Escalate delays to IT Manager.

Department Heads:
– Approve access or special IT requests.
– Ensure employees follow the email request protocol.

Employees:
– Provide complete details when reporting issues.
– Respond to IT queries during troubleshooting.

33.5 Escalation Matrix
Level 1: IT Support Lead – SLA exceeded by 50%
Level 2: IT Manager – High-impact unresolved issues
Level 3: Head – IT – Persistent SLA breaches

Level 4: Senior Management – Critical business impact

33.6 Non-Compliance
Requests not submitted through email will not be SLA-bound. Repeated bypassing of process may be escalated to Department Head or HR.

33.7 Review
This policy will be reviewed annually or when IT support processes undergo significant changes.

Enforcement
Violation of this policy may lead to disciplinary action as per company norms.

Responsibilities
Employees, Department Heads, IT Support Team, IT Manager.

34. Secure Software Development & Secure Coding Policy

Purpose

To ensure that all software developed, modified, or integrated by Ind-Swift Laboratories Ltd. follows secure development practices and meets ISO 27001:2022 controls A.8.25, A.8.26, A.8.27, reducing vulnerabilities and strengthening application security.

Policy Requirements

34.1 Secure Development Framework

• Security must be built into requirements, design, development, testing, and deployment stages.

34.2 Third party Developer must follow Secure Coding Standards

34.3 Security Requirements Documentation

• Security requirements must be documented at the start of each project.
• Requirements must address authentication, authorization, logging, encryption, and data protection.

34.4 Code Review & Security Testing

• Peer code reviews are mandatory for all code deployments.
• Automated and manual security tests must include:
– SAST (Static Analysis)
– DAST (Dynamic Analysis)
– SCA (Software Composition Analysis)
– Penetration testing for major applications

34.5 Third-Party Libraries & Open-Source Components

• Third-party components must be validated for:
– Version vulnerabilities
– Licensing risks

– Known CVEs
• Only approved components may be used.

34.6 Vulnerability Remediation

• All identified vulnerabilities must be logged, risk-ranked, and remediated according to severity.
• Patch cycles must follow the Vulnerability Management Policy.

34.7 Approved Environments Only

• Development must use secured, segregated environments (dev/test/production).
• Only approved Git repositories, CI/CD tools, and cloud environments may be used.

Responsibilities

Developers, QA Team, IT Security, DevOps/Release Management.

35. Logging, Monitoring & SIEM Policy

Purpose

To ensure proactive detection of anomalies, security events, and system failures by implementing comprehensive logging and monitoring, aligned with ISO 27001:2022 controls A.8.16, A.8.15, A.5.25.

Policy Requirements

35.1 Mandatory Logging

• Logs must be generated for all critical systems, including:
– Servers
– Databases
– Firewalls
– Cloud services
– Endpoints
• Logs must cover security, access, operational events, and configuration changes.

35.2 Log Retention & Protection

• Logs must be retained for:
– 90 days online
– Minimum 1 year archived
• Logs must be protected from deletion or modification.

Responsibilities

IT Security, SOC Team, System Administrators.

36. Backup Security & Retention Policy

Purpose

Ensure secure, reliable, and regulatory-compliant backup and recovery processes aligned with ISO 27001:2022 controls A.8.13, A.8.14.

Policy Requirements

36.1 Backup Encryption

• Backups must be encrypted using AES-256 or equivalent.

36.2 Backup Retention

• Retention periods must align with:
– Legal requirements
– Financial and audit needs
– Business continuity objectives

36.3 Backup Integrity Verification

• Monthly backup integrity checks must be performed.
• Backup failures must be escalated immediately.

36.4 Onsite/Cloud Backup

• At least one backup copy must be stored Onsite or in secure cloud storage.
• Magnetic tapes & stored at security gate in fireproof media safe.

Responsibilities

Backup Administrator, IT Security, Infrastructure Team.

37. Cryptographic Key Management Policy

Purpose

Ensure secure generation, storage, use, rotation, and disposal of cryptographic keys according to ISO 27001:2022 control A.8.24.

Policy Requirements

37.1 Key Generation

• Keys must use approved algorithms (AES-256, RSA-2048+, ECC-256, etc.).

37.2 Key Storage

• Keys must be stored in secure locations:
– Hardware Security Modules (HSM)

– Cloud Key Management Services (KMS)
– Encrypted vaults

37.3 Key Rotation

• Keys must be rotated:
– At least annually
– Immediately after compromise
– When personnel change roles

37.4 Key Access Control

• Access to keys must follow least privilege.
• All access must be logged and monitored.

Responsibilities

IT Security, System Administrators.

38. Vulnerability Management Policy

Purpose

Define consistent detection, assessment, prioritization, and remediation of vulnerabilities, aligned with ISO 27001:2022 controls A.8.8, A.5.27.

Policy Requirements

38.1 Yearly Vulnerability Scanning

• All servers, endpoints, and network devices must be scanned Yearly.

38.2 Vulnerability Remediation Timelines

• Critical: Fix within 30 days
• High: Fix within 45-60 days
• Medium: Fix within 90 days
• Low: Fix as scheduled

38.3 Security Testing

• Annual penetration testing required.
• After major changes, additional scans must be conducted.

38.4 Zero-Day Vulnerability Handling

• Immediate review and mitigation required.
• Emergency patching must be performed for critical zero-days.

Responsibilities

IT Security, Infrastructure Team, Application Owners.

39. Supplier Security Management Policy

Purpose

Ensure suppliers, vendors, and third parties meet organizational security requirements in accordance with ISO 27001:2022 control A.5.19, A.5.20, A.5.21.

Policy Requirements

39.1 Supplier Evaluation

• Review of certifications (ISO 27001, SOC2, etc.).

39.2 Contractual Security Requirements

• All contracts must include:
– Confidentiality
– Data protection
– SLA

39.3 Third-Party Access Monitoring

• Vendor access must:
– Be approved
– Be time-bound
– Be logged and reviewed quarterly

Responsibilities

Procurement, IT Security, Vendor Management Team.

40. BYOD Security Policy

Purpose

Ensure secure management of corporate and BYOD mobile devices aligned with ISO 27001:2022 controls A.6.7, A.8.9, A.8.23.

Policy Requirements

40.1 In case BYOD approved by HR or Top management use of VPN is must.

40.2 Corporate Data Protection

• Corporate data must not be stored on personal devices unless explicitly approved.

40.3 App Usage & Storage Controls

• Only approved applications may be used.
• Data sharing to personal apps (Gmail, WhatsApp, etc.) is based on management approval.

Responsibilities

Employees, IT Security.

41. Incident Response & Forensics Policy

Purpose

To define a structured, timely, and effective approach for identifying, reporting, responding to, containing, analyzing, and resolving information security incidents within Ind-Swift Laboratories Ltd., including the performance of digital forensics where required.
This policy supports ISO 27001:2022 controls A.5.24, A.5.25, A.5.26, A.8.16.

Policy Requirements

41.1 Immediate Reporting of Incidents

• All employees must report cybersecurity incidents, suspicious events, or policy violations immediately to the IT Security team.
• Incidents may include malware infection, data leakage, unauthorized access, phishing, loss of devices, system compromise, etc.

41.2 Incident Classification

• IT Security must classify all incidents based on severity:
– Critical: Impact on critical business systems, large-scale data loss, regulatory impact.
– High: Disruption of major services, confirmed breach of sensitive data.
– Medium: Localized impact on a system or department.
– Low: Minor events with minimal operational impact.
• Classification determines required escalation, response time, and team involvement.

41.3 Incident Response Workflow

Each incident must follow the standard response phases:
• Identification
• Containment (short-term & long-term)
• Eradication
• Recovery

• Lessons learned
• Documentation and closure

41.4 Digital Forensics & Chain of Custody

• IT Security must preserve evidence in a forensically sound manner using approved tools.
• Chain-of-custody documentation must track:
– Who collected the evidence
– Where and how it was stored
– Transfers of custody
– Investigation logs
• Evidence must not be altered during investigation.

41.5 Incident Documentation

• A formal incident report must be completed for every incident, including:
– Root cause
– Impact assessment
– Response actions
– Forensics findings
– Corrective and preventive actions (CAPA)
• Reports must be retained according to the Data Retention Policy.

Responsibilities

• IT Security / IR Team: Lead incident response, forensics, documentation.
• System Administrators: Assist in containment and recovery.
• Employees: Immediately report incidents and support investigation.

42. Disaster Recovery & Technical BCP Policy

Purpose

To establish technical controls to ensure the resilience, restoration, and recoverability of critical IT systems following disruptions.
Aligned with ISO 27001:2022 Controls A.5.30, A.8.13, A.8.4, A.8.5.

Policy Requirements

42.1 RTO and RPO Definition

• Recovery Time Objective (RTO) and Recovery Point Objective (RPO) must be defined, approved, and documented for each critical system.
• Changes to business processes or systems require RTO/RPO updates.

42.2 Disaster Recovery Drills

- Full-scale DR drills must be performed annually.
- Tabletop exercises must be performed semi-annually.
- Findings must be recorded, and corrective actions tracked to closure.

42.3 DR Environment Hardening & Security

- DR systems must be isolated from production to prevent cascading failures.
- DR infrastructure must follow secure configuration standards.
- Access must be controlled using MFA, role-based access, and logging.

42.4 Failover & Recovery Documentation

- Failover and fallback procedures must be documented, tested, and approved.
- Recovery workflows must be version-controlled and stored securely.
- All IT teams must be trained in DR roles and responsibilities.

Responsibilities

- IT Manager: DR governance, approval of plans and drills.
- System Administrators: Maintain DR environment and execute recovery procedures.
- IT Security: Validate DR security posture and risk alignment.

43. Data Retention & Secure Disposal Policy

Purpose

To define secure, compliant, and auditable retention and disposal of electronic and physical data, ensuring regulatory alignment and reduction of information risk.
Aligned with ISO 27001:2022 Controls A.5.34, A.5.28, A.5.29, A.8.10.

Policy Requirements

43.1 Data Retention Requirements

- Retention periods must be based on:
  – Legal and regulatory requirements
  – Quality/compliance needs
  – Operational requirements
- Data must not be retained longer than necessary.

43.2 Secure Disposal of Physical Data

- Confidential physical documents must be:
  – Shredded using cross-cut shredders

– Disposed through certified destruction vendors
• Disposal certificates must be retained.

43.3 Secure Disposal of Electronic Data

• Electronic media must be securely wiped using DoD-approved, NIST 800-88, or equivalent certified tools.
• For highly sensitive media, physical destruction (degaussing, shredding, pulverizing) is mandatory.
• Disposal logs must be maintained.

43.4 Cloud & Application Data Disposal

• Cloud and SaaS platforms must follow the same deletion principles.
• Vendor deletion certificates must be obtained when available.

Responsibilities

• Data Owners: Define retention periods and approve disposal.
• IT Security: Ensure secure methods and maintain records.
• Department Heads: Ensure compliance within units.

44. Secure Configuration Baseline Policy

Purpose

To establish secure configuration baselines for servers, desktops, laptops, network devices, and applications to minimize vulnerabilities and harden the technology environment.
Aligned with ISO 27001:2022 Controls A.8.9, A.8.21, A.8.22, A.8.28.

Policy Requirements

44.1 Use of Industry Baselines

• All systems must apply CIS Benchmarks, DISA STIG, or organization-approved secure configuration standards.
• Baselines apply to:
– OS (Windows/macOS/Linux)
– Databases
– Network devices (firewalls, routers, switches)
– Servers and endpoints

44.2 Configuration Approval & Exceptions

• Any deviation from baseline standards must be approved by IT Security.
• Exceptions must document:
– Risk justification
– Compensatory controls
– Expiry date

44.3 Hardening Checklists & Documentation

• Checklists must be maintained for each platform and reviewed annually.
• Settings include:
– Disabling unnecessary services
– Blocking default ports
– Disabling default accounts
– Enforcing password and MFA policies
– Applying secure logging configurations

44.4 Monitoring Configuration Drift

• Automated tools (CSPM, EDR, SCCM, MDM, vulnerability scanners) must monitor devices for drift.
• Non-compliant systems must be corrected or quarantined.

Responsibilities

• System Administrators: Implement baselines and maintain configuration integrity.
• IT Security: Approve baselines, monitor drift, enforce compliance.
• Cloud Teams: Apply secure baselines to cloud workloads.

45. Remote Work & Teleworking Security Policy

Purpose

To ensure secure remote access to Ind-Swift Laboratories Ltd. systems, prevent unauthorized disclosure of information, and maintain the confidentiality, integrity, and availability of organizational data during remote work, outside premises or teleworking activities.
This policy aligns with ISO 27001:2022 controls A.6.7, A.5.10, A.8.9, A.8.21, A.8.23.

Scope

This policy applies to:

- All employees, contractors, and consultants working remotely
- All company devices used for remote access
- Personal devices approved under the BYOD policy
- All access to corporate systems, cloud platforms, email, and applications from remote locations

Policy Requirements

45.1 Use of Approved Devices Only

• Only company-approved laptops, desktops, or secure BYOD devices (pre-approved by HR) may be used for remote work.
• Devices must have the following pre-installed:
– EDR / Antivirus

– Firewall
– Endpoint hardening controls
• Use of personal, family-shared, or public devices is prohibited unless explicitly approved.

45.2 Mandatory Use of VPN and MFA

• All remote connections must use the official Corporate VPN with enforced encryption (AES-256/IPSec or SSL-VPN).
• MFA (Multi-Factor Authentication) is mandatory for:
– VPN
– Email (only for Admin user)

• Direct, unsecured internet access to corporate apps is strictly prohibited.

45.3 Secure Home / Remote Network Requirements

• Personal or home Wi-Fi must meet minimum security standards:
– WPA2 or WPA3 encryption
– Strong, unique router password
– No default router credentials
• Public Wi-Fi (cafes, airports, hotels) must not be used unless connected through VPN and IT-approved secure hotspots.

45.4 Protection of Confidential Information

• Confidential or sensitive data must not be printed at home unless explicitly authorized.
• Local storage on personal devices is strictly prohibited.
• Files must only be stored on approved cloud drives or corporate systems.
• Screens must be protected from shoulder surfing; auto screen-lock must be enabled.

45.5 Physical Security of Remote Work Environment

• Devices must not be left unattended in cars, public places, shared accommodations, or open environments.
• Remote workers must ensure:
– Safe storage of devices
– Restricted access by family members or visitors
– Use of privacy screens when needed

45.6 Prohibited Activities

Remote workers must not:
• Disable firewall, antivirus, or EDR protections
• Use unauthorized remote access tools
• Download or install unapproved software
• Connect USB storage devices without authorization
• Use personal email or social media for work purposes
• Forward work emails to personal accounts

45.7 Patch & Update Compliance

• Remote devices must stay updated with security patches for:
– Operating system
– Browsers
– VPN
– Antivirus/EDR
• Devices not patched within required timelines may be automatically blocked from connecting.

45.8 Secure Communication Practices

• Corporate communication channels (Teams, Skype, corporate email, approved messaging apps) must be used for all work-related interactions.
• Confidential discussions must not occur in public places or through unapproved apps.

45.9 Incident Reporting

Remote employees must immediately report:
• Lost or stolen devices
• Suspicious activity on devices
• Unauthorized access attempts
• Accidental exposure or sharing of confidential data

All incidents follow the Incident Response & Forensics Policy.

Responsibilities

Employees

• Follow secure remote work protocols
• Maintain device security
• Report security incidents immediately
• Ensure confidential information is protected at all times

IT Security

• Maintain secure VPN, MFA, and endpoint protection controls
• Monitor remote access activity via SIEM
• Provide guidance and training on remote work security
• Enforce compliance and take corrective actions

46. Information Transfer Policy

Purpose

To ensure that all information transferred within Ind-Swift Laboratories Ltd. or to external parties is securely protected against unauthorized access, interception, disclosure, alteration, or loss. This includes transferring information via electronic, physical, or verbal methods.

This policy supports ISO 27001:2022 requirements for information transfer, communication security, encryption, access control, and monitoring.

Scope

This policy applies to:

- All employees, contractors, consultants, and third parties.
- All forms of information transfer, including:
  - Email
  - SFTP/FTPS
  - VPN communication
  - Secure cloud sharing
  - Removable media (USB, HDD, SSD)
  - Printed documents
  - Instant messaging (only approved tools)
  - Verbal communication involving confidential data

Policy Requirements

46.1 Approved Secure Transfer Channels

• Only company-approved, secure transfer methods may be used to send or receive information.
• Approved channels include:
– Encrypted email (TLS 1.2+)
– Secure File Transfer Protocol (SFTP/FTPS)
– VPN-based communication
– Approved cloud platforms
• Unapproved channels such as WhatsApp, personal email, and public file-sharing sites are strictly prohibited.

46.2 Encryption for Sensitive Information

• Sensitive, confidential, or regulated information (PII, financial data, R&D data, quality data) must be encrypted during transfer.
• Encryption standards must follow approved algorithms such as AES-256 and TLS 1.2+.
• Passwords or decryption keys must be shared through a different secure channel (not the same email).

46.3 Authorization Before External Sharing

• All external information sharing must be authorized by:
– Data Owner
– Department Head, OR
– IT Security (if high sensitivity)
• Before sharing externally, employees must confirm:
– Identity of the recipient
– Business need and legal basis
– Whether an NDA is in place
• All external transfers must be logged and may be reviewed.

46.4 Validating Recipient Identity

- External recipients must be validated before sending any sensitive data.
- Verification methods:
  – Confirming corporate email domain
  – Cross-checking vendor contact list
  – Telephonic or official email verification
- Sensitive data must never be sent to generic email IDs (e.g., info@, support@) unless approved.

46.5 Integrity Protection During Transfer

- Where applicable, checksums or hash verification (e.g., SHA-256) must be used for large file transfers.
- Logs of file uploads/downloads must be maintained for audit purposes.
- Systems must maintain transmission records, versioning, and tracking of changes.

46.6 Use of Removable Media

- Removable media may only be used with explicit approval.
- All removable devices must be encrypted and malware-scanned.
- Unauthorized devices must be blocked by endpoint protection tools.
- Lost or stolen media must be reported immediately as a security incident.

46.7 Physical Transfer of Documents

- Confidential physical documents must be:
  – Sealed in envelopes or locked bags
  – Clearly labeled “Confidential”
  – Transported via approved secure courier services
  – Not left unattended at any time
- Physical copies must be securely shredded when no longer needed.

46.8 Cloud-Based Information Sharing

- Only company-approved cloud platforms may be used for data transfer.
- Mandatory controls for cloud sharing:
  – Link expiry dates
  – Restricted access (no “public link” sharing)
  – Activity logs enabled
- Data residency and regulatory requirements must be followed.

46.9 Monitoring & Logging of Information Transfers

- All external transfers must be logged by IT systems or users.
- Suspicious transfers or repeated failures will trigger a security investigation.
- Logs must be retained according to the Data Retention Policy.

46.10 Incident Reporting for Transfer Failures

Any of the following incidents must be reported immediately:
• Sending information to the wrong recipient
• Unencrypted transmission of sensitive data
• Unauthorized external sharing
• Data leakage through misconfiguration
• Any attempt to bypass secure channels

Incidents must follow the Incident Response & Forensics Policy.

Responsibilities

Employees

• Use only authorized channels and secure methods for information transfer.
• Validate recipients and protect confidentiality.
• Report accidental or unauthorized transfers immediately.

Department Heads / Data Owners

• Approve external sharing requests.
• Ensure proper classification and handling of information.
• Verify compliance within their departments.

IT Department / IT Security

• Provide secure transfer tools (email encryption, SFTP, VPN, cloud).
• Maintain security configurations and logs.
• Monitor suspicious transfers and enforce controls.
• Conduct periodic audits of information transfer practices.

47. Cloud Monitoring & Cloud Assurance Policy

Purpose

The purpose of this policy is to ensure that all cloud services used by Ind-Swift Laboratories Ltd. are continuously monitored, assessed, secured, and governed in alignment with ISO 27001:2022 Controls A.5.23, A.8.16, A.8.9, A.5.30, and industry best practices.
This policy establishes a framework for:

- Monitoring cloud operations
- Ensuring provider compliance
- Identifying security gaps
- Ensuring reliability, performance, and data protection
- Managing cloud lifecycle and exit strategies

Policy

47.1 Cloud Governance & Assurance Framework

• All cloud services must be approved by IT Security and Management before use.
• A Cloud Risk Assessment must be completed for all SaaS, PaaS, and IaaS onboarding.
• Cloud vendors must meet minimum security certifications (ISO 27001, SOC 2, PCI DSS where applicable).
• Ownership must be assigned to a Cloud Service Owner for each cloud application.
• Critical cloud systems must undergo annual Business Impact Assessment (BIA).

47.2 Quarterly Cloud Usage Review

• Cloud service consumption, user activity, permissions, and billing must be reviewed quarterly.
• Quarterly review must validate:
– User access appropriateness
– Resource utilization
– Licensing compliance
– Data storage locations and residency
– Misconfigurations or unused services
• Review results must be documented and approved by IT Management.

47.3 Continuous Cloud Monitoring & Log Analysis

• All cloud environments must generate logs for:
– Access events
– Authentication and MFA failures
– Data modifications
– Administrative actions
– API interactions
– Network and firewall events
• Logs must be:
– Retained for minimum 180 days (or regulatory requirement)
– Sent to SIEM for real-time monitoring
– Reviewed weekly for anomalies, suspicious behavior, or threats
• Alerts must be configured for:
– Unauthorized access attempts
– Data exfiltration
– High-risk API calls
– Privilege escalations
– Abnormal resource utilisation

47.4 Cloud Configuration & Security Baselines

• All cloud platforms must follow secure configuration standards (CIS Benchmarks).
• Mandatory baselines include:
– Encryption at rest and in transit
– Zero Trust configuration for network access
– Secure API authentication

– Firewall, NSG, or security group hardening
• Configuration drift must be monitored via automated tools.

47.5 Annual Cloud Security Audit

• A formal cloud audit must be performed at least annually to verify:
– Compliance with security requirements
– Access control effectiveness
– Backup integrity and DR readiness
– Patch and update compliance
– Vendor adherence to SLA and uptime guarantees
• Audit results must be documented, and corrective actions tracked to closure.

47.6 Cloud Data Protection & Backup Assurance

• Cloud-stored data must be encrypted (AES-256 or provider equivalent).
• Backup schedules must be defined, tested, and monitored for failures.
• Data residency must comply with regulatory requirements (India DPDP Act, global regulations if applicable).

47.7 Cloud Incident Monitoring & Response Integration

• Cloud incidents must follow the Incident Response Policy.
• Cloud security alerts must integrate with SIEM and SOC monitoring.
• Cloud provider notifications must be monitored and responded to within SLA.
• Post-incident forensic evidence must be preserved.

47.8 Cloud Vendor Management & SLA Monitoring

• Vendors must provide:
– Uptime SLA
– Security commitments
– Data protection obligations
– Compliance certifications
• Vendor performance and SLA adherence must be reviewed annually.
• Any service gaps must be escalated to vendor and internal management.

47.9 Cloud Exit Planning & Migration Assurance

• All cloud services must have a documented Exit Plan, including:
– Data export procedures
– Data deletion methodology
– Temporary access during migration
– Vendor lock-in mitigation
• Exit Plans must be:
– Tested every two (2) years
– Validated for completeness and reliability
• All data must be securely deleted after migration, with provider-issued Certificate of Data Deletion (if available).

47.10 Continuous Compliance & Improvement

• Compliance with cloud controls must be reviewed annually.
• Improvements must be implemented based on:
– Audit findings
– Threat intelligence
– Industry updates
– Cloud provider changes

Responsibilities

• Cloud Owner: Ensure operational compliance and quarterly reviews.
• IT Security: Monitor logs, enforce security baselines, analyze threats.
• System Administrators: Maintain configurations, backups, identity controls.
• Management: Approve cloud onboarding, budgets, and risk treatments.
• Third-party Providers: Adhere to contractual security and compliance commitments.

48. Outsourced Development Security Policy

Purpose
Ensure that all outsourced software development activities meet the security, quality, and compliance requirements of ISO 27001:2022 and Ind-Swift Laboratories Ltd.

Scope
This policy applies to all third-party vendors, contractors, freelancers, and partners engaged in software development, customization, integration, or maintenance.

Policy

48.1 Vendor Qualification & Approval
• All outsourced development partners must be evaluated for security capability.
• Contracts must include confidentiality, IP protection, data protection, and security clauses.
• Only approved vendors from the Vendor Master List may be engaged.

48.2 Security Requirements for Outsourced Development
• Vendors must follow secure coding standards.
• Development must occur only in approved and controlled environments.
• Access to source code and systems must be restricted and monitored.
• Vendors must not use personal systems or cloud services without approval.

48.3 Data Protection & Access
• Access to Ind-Swift data must be minimum necessary and time-bound.
• Sensitive data must be anonymized or masked wherever possible.
• All access must be logged, reviewed, and revoked after project completion.

48.4 Deliverable Security Assurance
• All deliverables must undergo security testing (SAST/DAST).
• Code review must be performed before acceptance.
• Vulnerabilities must be remediated by the vendor at no additional cost.

48.5 Intellectual Property & Confidentiality
• All source code, documentation, and deliverables remain the property of Ind-Swift Laboratories Ltd.
• Vendors must sign NDA and IP protection agreements.

48.6 Monitoring & Compliance
• Vendor development activities may be audited at any time.
• Non-compliance may lead to termination of the contract.

Responsibilities
IT Security, Procurement, Vendor Management, Software Development Partners.

49. Threat Intelligence Policy

Purpose

To define a structured process for collecting, analyzing, validating, and disseminating cybersecurity threat intelligence relevant to Ind-Swift Laboratories Ltd. This ensures proactive defense, early detection of emerging threats, and alignment with ISO 27001:2022 control A.5.7 Threat Intelligence.

Policy Requirements

49.1 Threat Intelligence Sources

IT Security must subscribe to multiple trusted sources, including:
• CERT-In advisories
• OEM vendor advisories (Microsoft, Adobe, Cisco, etc.)
• Security threat feeds (AlienVault, MISP, Abuse.ch)
• Industry ISAC/Pharma security alerts
• SOC & EDR threat feeds
• Cloud provider alerts (AWS/Azure/GCP Security Bulletins)

49.2 Threat Intelligence Review & Analysis

• Monthly threat intelligence review meetings must be conducted.
• Critical threat alerts (zero-days, active exploits, ransomware campaigns) must be reviewed within 24 hours.
• Impact assessment must consider:
– Affected assets
– Vulnerability severity
– Exposure level
– Exploitation likelihood

49.3 Distribution of Actionable Intelligence

• Processed and validated intelligence must be distributed to:
– IT Infrastructure
– SOC Team
– Application Owners
– Senior Management (for high-risk threats)
• Immediate notification required for critical threats.

49.4 Threat Intelligence Log Management

• A Threat Intelligence Log must be maintained, capturing:
– Threat description
– Source
– Date identified
– Affected systems
– Actions taken
– Closure date
• Logs must be reviewed during internal audits.

49.5 Integration With Incident Response & Vulnerability Management

• Relevant threat intelligence must trigger vulnerability scans, patching, or containment steps.
• Threat intelligence must be used to update detection rules in SIEM/EDR.

Responsibilities

• IT Security: Gather, analyze, distribute intelligence.
• SOC Team: Monitor, correlate SIEM/EDR alerts, update detection rules.
• IT Infra: Apply mitigation steps, patches, and configuration updates.

50. Privileged Access Management (PAM) Policy

Purpose

To ensure secure control, monitoring, and governance of privileged accounts, preventing misuse, unauthorized access, and breaches.
Aligned with ISO 27001:2022 controls A.5.18, A.8.2, A.8.3, A.8.21.

Policy Requirements

50.1 Separation of Accounts

• All administrators must maintain separate user and admin accounts.
• Admin accounts must not be used for daily/non-admin work.

50.2 Mandatory MFA for Privileged Accounts

• MFA must be enforced for all privileged accounts including:
– Cloud Admin
– Firewall/Network Admin

50.3 Privileged Access Vaulting

• All privileged credentials must be stored securely.

50.4 Privileged Access Review

• All privileged accounts must be reviewed on regular basis.
• Inactive, unused, or unauthorized privileged accounts must be disabled immediately.

50.5 No Shared Administrative Credentials

• Shared admin passwords are strictly prohibited.
• Unique credentials must be used for each privileged user.

50.6 Monitoring & Session Recording

• Administrative sessions must be logged and monitored via SIEM.
• High-privilege sessions must have session recording if supported.

50.7 Emergency Access Management

• Break-glass accounts must follow:
– Restricted use
– Audit logging
– Password rotation after each use

Responsibilities

• IT Security: Define PAM controls, monitor privileged activity.
• System Administrators: Manage and maintain privileged accounts.
• Management: Approve privileged access where required.

51. Endpoint Security & Hardening Policy

Purpose

Ensure secure configuration, monitoring, and protection of endpoints to reduce cyber risks, aligned with ISO 27001:2022 controls A.8.9, A.8.21, A.8.22, A.8.23.

Policy Requirements

51.1 Endpoint Hardening & CIS Compliance

• All laptops, desktops, and workstations must follow CIS Benchmarks.
• Hardening must include:
– Disabling unnecessary services
– Secure browser configuration
– Disabling macros unless approved
– Enforcing BIOS/UEFI passwords

51.2 Full Disk Encryption

• Disk encryption on all endpoints (if required)
– BitLocker for Windows

51.3 Security Controls on Endpoints

• All endpoints must have:
– Endpoint Detection & Response (EDR)
– Antivirus/NGAV
– Host firewall enabled
– USB restrictions based on role
• Unauthorized USB devices must be blocked.

51.4 Patch Management Manully

• Monthly patching is mandatory for all endpoints.
• Critical OS patches must be deployed within 14 days.

51.5 Software Installation Control

• Only approved software may be installed.
• Local admin rights must be restricted to authorized personnel.
• Unauthorized software must be automatically blocked/removed.

51.6 Endpoint Monitoring & Compliance Enforcement

• All endpoint activity (USB usage, malware alerts, login attempts) must be monitored.
• Non-compliant endpoints must be quarantined.
• Regular compliance audits must be performed by IT Security.

Responsibilities

• IT Security: Define standards, monitor compliance.
• IT Support: Implement updates, hardening, and troubleshooting.
• Employees: Use endpoints responsibly and report issues.

52. Patch Management Policy

Purpose
To define mandatory requirements for timely identification, assessment, testing, deployment, and verification of security patches and updates for all IT assets to reduce cyber risk and comply with ISO 27001:2022 (Control A.8.8).

Scope
This policy applies to all servers, network devices, endpoints, cloud services, virtual machines, applications, databases, mobile devices, and third-party systems used within Ind-Swift Laboratories Ltd.

Policy

52.1 Patch Management Governance
• IT Security and Infrastructure teams jointly own patch lifecycle management.
• Patch Management Schedule must be maintained.
• Only authorized IT personnel may perform patch deployment.

52.2 Patch Identification
• Patch notifications must be enabled for firewall, network devices, and cloud services.
• CERT-In advisories must be reviewed and logged as part of threat intelligence.

52.3 Patch Classification
All patches must be classified based on severity:
• Critical — Exploit exists, or asset is internet-facing → Deploy within 7 Days.
• High — Significant risk but no active exploit → Deploy within 15 days.
• Medium — Functional improvements/security fixes → Deploy within 30 days.
• Low — Cosmetic/non-security updates → Deploy within 45 days.

52.4 Patch Testing
• Patches must be tested in a staging environment prior to production rollout.
• Tests must include: application compatibility, rollback verification, system performance, and integration checks.

52.5 Patch Deployment
• Deployment must follow the Change Management Policy.
• Production patching must be scheduled during maintenance windows.
• Emergency patching is allowed only for critical vulnerabilities and must be documented and approved by IT Manager.

52.6 Patch Verification
• Post-deployment validation must include: system reboot confirmation, service/application verification, log review, and monitoring alerts.
• Failed patches must be rolled back immediately using documented rollback procedures.

52.7 Cloud Patch Management
• All cloud services (O365) must use automated patching features.
• Cloud dashboards and security centers must be reviewed monthly.

52.8 Network & Security Device Patching
• Firewalls, switches, routers, WAF, VPN appliances must have firmware updates applied within 15–30 days depending on severity.
• Configuration backup must be taken before any update.

52.9 Endpoint Patching
• All laptops/desktops must receive OS and application patches automatically.
• Endpoint protection/EDR must receive signature updates daily.

52.10 Third-Party / Vendor Patch Compliance
• Outsourced/support vendors must provide monthly patch compliance reports.
• Contracts must include patch SLAs aligned with this policy.

52.11 Patch Exceptions
• Exceptions must be documented, risk assessed, and approved by IT Security and the asset owner.
• Compensating controls (network isolation, firewall rules, monitoring) must be applied.

52.12 Reporting & Compliance
• Monthly Patch Compliance Report must be submitted to IT Manager and ISO Team.
• Patch compliance target: 100% for critical systems, 95% for non-critical systems.
• Non-compliance must be escalated as per IT escalation matrix.

52.13 Logging & Monitoring
• All patching activities must be logged.
• SIEM must monitor vulnerabilities and patch status.
• Regular VAPT must validate effectiveness of patching.

Enforcement
Violations of this policy may lead to disciplinary action, up to and including termination.

Responsibilities
IT Security Team – classification, monitoring, compliance.
Infrastructure Team – testing, deployment, validation.
Application Owners – approval, functional testing.
Third-Party Vendors – timely patching & reporting.

53. ICT Readiness for Business Continuity Policy

Purpose
To ensure Information and Communication Technology (ICT) systems supporting critical business operations at Ind-Swift Laboratories Ltd. remain available, resilient, and recoverable during disruptions, in compliance with ISO 27001:2022 Control A.5.30.

Scope

This policy applies to all critical IT systems, applications, servers, networks, cloud services, communication systems, and supporting infrastructure.

Policy

53.1 ICT Business Continuity Governance
• IT Manager and ISMS Manager jointly oversee ICT continuity planning.
• Business Impact Assessment (BIA) must identify critical systems and acceptable downtime.
• ICT continuity requirements must be documented and reviewed annually.

53.2 RTO and RPO Requirements
• Recovery Time Objective (RTO) and Recovery Point Objective (RPO) must be defined for all critical systems.
• High-criticality systems must target:
– RTO: ≤ 4 hours
– RPO: ≤ 1 hour
• RTO/RPO values must be approved by system owners and IT management.

53.3 IT Infrastructure Continuity Controls
• Redundant power, UPS, and generator backup must be maintained.
• Network redundancy (dual links, failover routing) must be implemented.
• Redundant storage and mirrored servers must be used for critical systems.
• Cloud workloads must have multi-zone resilience configuration.

53.4 Application Continuity Controls
• All critical applications must support backup, restoration, and failover.
• Cloud-based applications must enable high availability (HA) and fault tolerance.
• Offline operating procedures must exist for business-critical applications.

53.5 Backup & Data Protection
• Backups must be encrypted, tested, and stored in offsite or cloud DR locations.
• Full disaster recovery tests must be conducted at least once annually.
• Backup retention must meet legal and regulatory requirements.

53.6 Communication Continuity
• Emergency communication channels (alternate email, phone, WhatsApp groups, or satellite communication if applicable) must be defined.
• Contact lists for IT, management, and emergency support must be updated quarterly.

53.7 DR Drills & Testing
• Annual disaster recovery drills are mandatory.
• Tabletop exercises must be conducted twice yearly to test readiness.
• Issues identified during drills must be recorded and corrective actions implemented.

53.8 Change Management Integration
• ICT continuity implications must be evaluated for every major change.
• Systems affecting continuity must undergo impact analysis before approval.

53.9 Outsourced and Vendor Continuity Requirements
• Vendors hosting business-critical systems must provide evidence of their DR capabilities.
• Contracts must mandate:
– DR readiness
– Maximum downtime commitments
– Incident reporting SLAs

53.10 Monitoring & Incident Response Integration
• ICT continuity risks must be monitored through SIEM and monitoring systems.
• Business continuity incidents must trigger immediate reporting to:
– IT Manager
– CISO / ISMS Manager
– Senior Management (for major disruptions)

53.11 Documentation Requirements
• ICT Continuity Plans (ICT-BCP) must include:
– System inventory
– Recovery procedures
– DR environment details
– Failover workflows
– Contact lists and escalation matrix
• Plans must be updated annually or after major changes.

Enforcement
Non-compliance with this policy may result in disciplinary measures and increased operational risk. Repeated failures to follow DR procedures may result in escalation to senior leadership.

Responsibilities
• IT Manager – Owns ICT continuity architecture and readiness.
• ISMS Manager – Ensures ISO 27001 compliance and risk assessments.
• System Administrators – Maintain DR environments and backups.
• Application Owners – Validate application-specific recovery procedures.
• Vendors – Ensure contractual continuity requirements are fulfilled.

54. PII (Personally Identifiable Information) Protection Policy

Purpose
To ensure the lawful, ethical, secure, and compliant processing of Personally Identifiable Information (PII) within Ind-Swift Laboratories Ltd., aligned with ISO 27001:2022, DPDP Act 2023, and global privacy standards.

Scope
This policy applies to all forms of PII processed by employees, contractors, applications, servers, cloud systems, mobile devices, and authorized third parties.

Policy

1. Lawful and Purpose-Based Collection of PII
• PII must be collected only for legitimate, lawful, and documented business reasons.
• Collection must be linked to activities such as HR operations, regulatory compliance, vendor verification, and business transactions.
• Hidden, unauthorized, or excessive data collection practices are prohibited.

2. Classification and Labeling of PII
• All PII must be classified as "Confidential" users responsibility.
• Systems storing PII must reflect the classification in labels, access rules, and data handling methods.

3. Access Control and Least Privilege
• Access to PII must follow the principle of Least Privilege.
• Only authorized roles may access, modify, export, or process PII.
• Access must be approved, logged, periodically reviewed, and revoked when no longer required.

4. Security of PII in Storage and Transmission
• Encryption must be used for PII stored on cloud.
• TLS 1.2+ encryption must be used for data transfers, APIs, and integrations.
• PII must never be transmitted via unsecured channels, personal emails, or unapproved cloud services.

5. External Sharing Restrictions
• PII must not be shared with third parties without:
– Documented business need
– Legal basis
– Management approval
– Signed NDA
• Sharing PII outside India must follow legal safeguards.

6. PII Breach Detection and Notification
• Any PII breach—suspected or confirmed—must be reported immediately to IT Security.
• Incidents must follow the Incident Response Policy and include:
– Containment
– Impact analysis
– Notification (internal and external if required)
– Corrective actions

7. Retention and Data Minimization
• PII must be retained only for the legally required and business-justified duration.
• Retention schedules must be documented by Data Owners.
• Outdated or unnecessary PII must be securely deleted.

8. Secure Deletion and End-of-Life
• Secure wipe tools must be used to erase PII from systems at end-of-life.
• For highly sensitive PII, physical destruction of storage devices is required.
• Cloud deletion must follow vendor-specific secure wipe standards.

Responsibilities
• Data Owners: Define purpose, classification, retention, and disposal methods.
• IT Security: Implement technical controls, encryption, monitoring, and breach handling.
• Employees: Follow approved procedures for storing, accessing, and sharing PII.

55. Privacy Policy

Privacy Policy
By accessing this website, you consent to the terms of this Privacy Policy. By submitting your information to Ind-Swift Group, you agree to the collection, processing, storage, and use of such information as outlined herein.

1. Introduction
At Ind-Swift Group, we respect your privacy and are committed to protecting the personal and sensitive data of all our website visitors, customers, healthcare professionals, and stakeholders.

This Privacy Policy explains how we collect, use, store, and share your information in compliance with:

The Information Technology Act, 2000 – Section 43A

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

We uphold a “Privacy by Default” principle, ensuring that all user data is handled with confidentiality and care.

2. Scope
This policy applies to all visitors who browse, interact with, or submit information via www.indswiftgroup.com.

3. Information We Collect
We collect the following types of data when you visit or interact with our website:

3.1 Personal Information
Information that may identify you personally, including:

Name

Contact number

Email address

Company name

Designation

Uploaded documents (e.g., CVs, inquiry forms)

3.2 Sensitive Personal Data or Information (SPDI)
Only where necessary and voluntarily submitted:

Passwords

Payment or bank account details

Medical information (if any for sample requests)

Any combination of personal information that may be used for authentication or identity purposes

Note: Information available in the public domain or disclosed under the RTI Act is not treated as sensitive.

4. Purpose of Collection
We use your data for the following legitimate business and service-related purposes:

Responding to product, business, or partnership inquiries

Processing job applications or product sample requests

Sending newsletters, updates, or marketing communications (only if opted-in)

Improving website content and user experience

Fulfilling legal or contractual obligations

Conducting analytics to improve our services

5. Use of Cookies
Our website may use cookies and third-party tools like Google Analytics to:

Track user behavior and preferences

Improve performance and speed

Personalize the browsing experience

You may disable cookies in your browser settings if desired.

6. Data Storage & Security
Ind-Swift Group maintains reasonable and appropriate security standards to protect your personal data. We implement:

Technical safeguards (encryption, access controls)

Managerial procedures (authorized access, data minimization)

Periodic audits and reviews

Your information is retained only as long as necessary for business or legal purposes.

7. Sharing & Disclosure
Your information may be shared under the following conditions:

With trusted third-party vendors under strict confidentiality (e.g., IT, legal, logistics)

When required by law, regulation, or government authority

With internal business units of Ind-Swift Group for legitimate use

We do not sell or trade your personal information to external parties for commercial gain.

8. Access, Correction & Consent Withdrawal
You may request to:

Access or update your personal data

Withdraw previously given consent

Raise concerns regarding misuse or correction

Contact our Data Privacy Officer at the email provided below.

9. Third-Party Links
This website may contain links to third-party platforms (e.g., NSE, TradingView, partner websites). Ind-Swift Group is not responsible for the privacy policies or content of external websites.

10. Changes to this Policy
We may update this policy from time to time. Any changes will be reflected on this page with a revised "Effective Date."

11. Contact Us
For privacy-related queries, access requests, or feedback, please contact:

Data Privacy Officer
Ind-Swift Group
Email: support@indswiftgroup.com
Phone: 0172-5061850
https://www.indswiftgroup.com

56. Server Room Temperature Monitoring Policy

Purpose
To ensure continuous monitoring and control of Server Room environmental conditions to maintain optimal operating

temperature, protect IT infrastructure, prevent overheating-related failures, and ensure uninterrupted business operations and information security.

Scope

This policy applies to:

• All servers, storage devices, network equipment, backup systems, and supporting IT infrastructure housed in the Server Room.

• All employees, IT personnel, Engineering/Facilities staff, and authorized Security personnel involved in temperature monitoring, maintenance, or access control to the Server Room.

Policy

1. Environmental Control Requirements

• The Server Room must operate within safe temperature limits to ensure availability and performance of IT assets.
• Recommended operating temperature range: 18°C to 27°C.
• Ideal control range: 20°C to 24°C.
• Humidity controls, where available, must follow OEM/environmental standards.

2. Monitoring Devices & Calibration

• The Server Room must be equipped with a Digital Temperature Display Unit and/or automatic temperature sensors/hygrometers.
• All monitoring devices must be maintained in good working condition.
• Calibrated annually or as per internal calibration procedures, if applicable.

3. Access Control and Authorized Personnel

• Only authorized IT, Engineering, and Security personnel may access the Server Room.
• Security staff must verify identity and ensure restricted entry in alignment with access control policies (ISO 27001 A.5.15).
• All access events must be logged as per the access management process.

4. Monitoring Frequency

• Temperature shall be documented twice daily during general shift (Morning & Evening).
• During weekends or holidays, Security personnel shall record temperature if IT staff are unavailable.
• IT personnel must review and verify holiday/weekend temperature logs on the next working day.

5. Temperature Recording Requirements

Temperature readings must be recorded in the Server Room Temperature Monitoring Log Sheet, including:

• Date and Time
• Temperature Reading (°C)
• Recorded By / Verified By (Sign & Date)
• Location (if multiple sensors installed)
• Remarks (e.g., fluctuations, abnormal readings)

6. Deviation Handling & Corrective Actions

If Server Room temperature exceeds the defined threshold:

1. Notify the IT Head and Engineering/Facilities team immediately.
2. Engineering must inspect HVAC/AC units and initiate corrective actions.
3. IT must take protective steps, such as:
   – Switching to backup AC units
   – Reducing non-critical server loads
   – Triggering automated cooling alarms (if available)
4. Document the deviation in the monitoring log and raise an Incident Report/Deviation Form as per QMS/ISMS procedures.
5. Verify and record temperature normalization after resolution.

7. Preventive Maintenance Requirements

• HVAC/AC units supporting the Server Room must undergo monthly preventive maintenance or as per SOP No. 14050.
• Temperature sensors and hygrometers must be:
– Inspected periodically
– Calibrated as per the calibration SOP (if applicable)
– Replaced immediately in case of malfunction

8. Logging, Review & Retention

• All temperature monitoring logs must be retained as per the ISMS document retention schedule.
• Logs must be reviewed monthly by IT to identify trends, risks, or recurring deviations.
• Any anomalies must be escalated through the risk assessment or incident management process.

9. Policy Review

This policy shall be reviewed annually or earlier under the following conditions:
• Change in Server Room infrastructure or equipment
• HVAC upgrades or environmental control changes
• Internal/External audit recommendations
• Updates to legal, regulatory, or ISO 27001:2022 requirements

Acknowledgement of IT Policy Understanding

Document No.: ISLL/IT/P/01
Issue Date: 20-08-2025

This is to acknowledge that I, the undersigned employee of Ind-Swift Laboratories Ltd. Services Pvt. Ltd., have read, understood, and agreed to comply with the organization's IT Policy.

I understand that the IT Policy outlines the responsibilities, acceptable use of IT resources, security requirements, and my role in safeguarding organizational information assets. I agree to:

1. Adhere to all IT security protocols, policies, and procedures.
2. Maintain confidentiality and integrity of company information and systems.
3. Report any observed or suspected IT security incidents promptly.
4. Accept that non-compliance with the IT Policy may result in disciplinary action, up to and including termination.

By signing below, I confirm my commitment to comply with the IT Policy and contribute to maintaining a secure and responsible IT environment at Ind-Swift Laboratories Ltd..

Employee Details

- Employee Name: _____
- Employee ID: _____
- Department: _____
- Designation: _____
- Date of Joining: _____

Acknowledgement

I hereby acknowledge that I have received, read, and understood the IT Policy.

Employee Signature: _____
Date: _____

Authorized By (HR/IT Dept.): _____
Date: _____