IT SYSTEM SECURITY POLICY

APPLICABILITY	All Symbiotec Group of Companies
POLICY ADMINISTRATION	
INITIATED BY (Signature with Name)	BL. Jangir 19/03/24
REVIEWED BY (Signature with Name)	Manish Tare 19/03/24
APPROVED BY (Signature with Name)	RAGHAVENDER R 19/3/24
WITH EFFECT FROM	20/03/2024
REVIEW BEFORE	19/03/2027
VERSION	V1

Table of Contents

Contents

1. Preamble

At SYMBIOTEC, we recognize the critical importance of information technology (IT) security in safeguarding our assets, preserving confidentiality, ensuring integrity, and maintaining the availability of our systems and data. As such, this IT Security Policy serves as a foundational framework to guide our efforts in protecting our digital infrastructure, mitigating risks, and promoting a culture of security awareness and compliance across all levels of the organization.

Our commitment to IT security is rooted in our dedication to maintaining trust with our customers, partners, employees, and stakeholders. By adhering to industry best practices, standards, and regulatory requirements, we aim to:

Protect Information Assets: Safeguard sensitive and confidential information, including customer data, intellectual property, financial records, and proprietary systems, against unauthorized access, disclosure, alteration, or destruction.

Mitigate Cybersecurity Risks: Identify, assess, and mitigate cybersecurity risks associated with emerging threats, vulnerabilities, malware, and unauthorized intrusion attempts targeting our networks and systems.

Ensure Compliance: Align IT security practices with relevant laws, regulations, contractual obligations, and industry standards to uphold legal and ethical responsibilities.

Foster a Secure Environment: Promote a culture of security awareness, accountability, and continuous improvement among employees, contractors, and third-party vendors through training, education, and effective communication of policies and procedures.

Enhance Physical and Environmental Security: Protect physical assets, facilities, and infrastructure housing IT resources from unauthorized access, theft, vandalism, natural disasters, and other physical threats that may compromise security and operations.

Encourage Collaboration: Foster collaboration and information sharing among IT teams, business units, and key stakeholders to address security concerns, implement effective controls, and promote a holistic approach to IT security governance.

By adhering to the principles outlined in this IT Security Policy and supporting policies, procedures, and guidelines, we demonstrate our unwavering commitment to maintaining a secure, resilient, and trustworthy IT environment that upholds the confidentiality, integrity, and availability of our information assets.

2. Purpose

The purpose of our IT Security Policy is to establish a comprehensive framework for safeguarding our digital assets, ensuring the confidentiality, integrity, and availability of information, and mitigating cybersecurity risks. By outlining clear guidelines, responsibilities, and procedures, this policy aims to promote a culture of security awareness, compliance with regulatory requirements, and proactive risk management practices across all levels of the organization. Through effective implementation and enforcement of this policy, we strive to protect sensitive data, maintain trust with stakeholders, prevent unauthorized access, and enhance the resilience of our IT infrastructure against evolving threats and vulnerabilities.

To have a formal structure to address security incidents emanating from natural and manmade events, this could have an impact on the business.

Issues related to compromise of IT Infrastructure and systems need to be addressed formally through a defined structure as the business is technology driven and enabled.

3. Scope and applicability

This policy applies to all employees, contractors, third-party service providers, and entities accessing or utilizing SYMBIOTEC's IT resources, networks, and data, and it is subject to periodic review, updates, and revisions to reflect evolving cybersecurity threats, regulatory changes, and industry best practices.

4. Definitions

I. IT Security: IT security, also known as information security, refers to the measures and practices implemented to protect computer systems, networks, data, and information assets from unauthorized access, theft, disruption, or damage.

II. Vulnerability: A vulnerability is a weakness or flaw in a system, network, application, or protocol that could be exploited by attackers to compromise security, gain unauthorized access, or cause harm.

III. Cyber Security: Cybersecurity encompasses the protection of digital assets, including networks, computers, data, and devices, from cyber threats such as hacking, malware, phishing, data breaches, and other malicious activities aimed at causing harm or disruption.

IV. Threats: Threats in the context of cybersecurity refer to potential dangers or risks that can exploit vulnerabilities to compromise the security of IT systems or data. These threats can include malware, phishing attacks, insider threats, denial-of-service (DoS) attacks, and social engineering tactics.

V. Malware: Malware, short for malicious software, is a type of software designed to disrupt, damage, or gain unauthorized access to computer systems and data. Examples of malware include viruses, worms, ransomware, spyware, and trojans.

VI. Unauthorized Access: Unauthorized access refers to the act of gaining entry to a system, network, application, or data without proper authorization or permission. Unauthorized access is often a result of security breaches, weak authentication mechanisms, or exploitation of vulnerabilities.

5. POLICY

5.1 **End Point Security**

5.1.1 Formal security maintenance processes shall be implemented for ensuring adequate security at the end user computing system level. Access to end point computing systems shall be restricted to those people who need the information to perform their business functions on a strictly need to know basis. System documentation shall be protected against unauthorized access. The reference to the word "system(s)" hereafter in this document shall be construed as end point computing systems like desktops, laptops. Wherever required to be stated separately, the same shall be done to elicit a particular detail.

5.1.2 The IT Team shall be responsible for ensuring that systems which are not connected with GxP instrument/ equipment are updated and functional with current operating system patches as per procedure for management of patches/ updates.

5.1.3 Operating system patches on GxP instrument(s) / equipment(s) must be installed based on recommendations from Instrument / Equipment OEM or authorized vendors.

5.1.4 The IT Team shall be responsible for ensuring that systems are updated with latest virus definitions and hardened.

5.1.5 Use of system utilities which may override system or application control shall be done only under authorization.

5.1.6 Each user shall be provided a unique user ID and password. Password management shall be done to ensure that quality and complexity of passwords is maintained. A formal user registration and de-registration process shall be established. The password complexity shall be as stated in the respective SOP.

5.1.7 For critical systems, session time out and connection time out shall be enforced wherever possible. If required login procedures for these systems shall be secure and shall comprise.

5.1.8 Systems shall be configured such that users shall be able to lock their terminals either manually or automatically to prevent unauthorized access.

5.1.9 Changes which impacts on the configuration of the system shall be through a formal change management process.

5.1.10 Suitable tool shall be deployed for managing integrated roll out of OS patches and AV updates and initiate remediation measures to remove inconsistencies in deployment.

5.2 **USB storage / Pen Drive access control.:**

5.2.1 The organization strictly restricts the use of pen drives to prevent data leakage and unauthorized access. Pen drives can only be used with written approval from the respective department head, and all pen drives must undergo scanning by the IT department before use.

5.2.2 USB storage / Pen Drive issued by IT department as per request received on template defined in Annexure-1

5.2.3 **Authorization Process:**

When an employee requires the use of a pen drive for legitimate business purposes, they must submit a written request to their department head as per template define in Annexure-2

The department head evaluates the request and determines its necessity for the intended task.

If approved, the department head forwards the request to the IT department for further processing.

5.2.4 **IT Approval and Scanning:**

Upon receiving the approved request from the department head, the IT department assesses the pen drive for security risks and compatibility with organizational systems.

The IT department performs a thorough scan of the pen drive to detect and remove any malware, viruses, or malicious files.

Only pen drives that pass the IT scanning process are authorized for use within the organization.

5.2.5 **Temporary USB Port Opening:**

Once the pen drive has been scanned and approved by the IT department, a temporary request is made to open the USB port on the employee's device for the designated period as per template defined in Annexure-2.

The IT department opens the USB port temporarily, allowing the employee to use the authorized pen drive for the approved task.

After the designated period or task completion, the USB port is promptly closed by the IT department to prevent unauthorized use or data leakage.

5.2.6 **Laptop Drive Encryption:**

To enhance data security and protect sensitive information, all laptop drives must be encrypted. This measure ensures that any data stored on these devices is safeguarded against unauthorized access. Compliance with this policy is mandatory for all users.

5.2.7 **Laptop Issuance Process**

Laptops will be issued to employees only upon the approval of the respective HOD and the CTO.

5.3 **Information Security Incident Management**

5.3.1 Any compromise of confidentiality, availability or integrity of information is considered as an information security incident.

Confidentiality related incidents are as stated bellow but not limited to

- Theft of information
- Unauthorized use of information
- Unauthorized transfer of information

Integrity related incidents are monitored by IT Dept. by reviewing cases such as:

- Server Events logs
- Inaccurate/Incomplete data.

5.3.2 IT Dept. carry out system monitoring and logs reviews to detect information security incidents. Events of unauthorized access attempts to the company's information systems resources, internet etc. are reviewed by the IT dept. on a regular basis based on network settings and policies configurations.

5.3.3 Users and managers are also encouraged and accountable to promptly inform any information security lapses/weaknesses to the IT Dept. occurring in their respective areas.

5.3.4 In order to understand as to how this policy shall manifest, it is imperative that one understands the meaning of what an Incident or Event is the explanation is provided as under:

- An event is defined as an identified occurrence in a system, service or network indicating a possible breach of security, procedures and safeguards a previously unknown situation that shall be relevant from the security point of view.
- An incident is defined as a single or a series of unwanted or unexpected events that have a significant probability of compromising business operations and threatening security. A crisis shall manifest out of an incident, if it threatens the safety of the staff, and impacts business continuity. Anything else shall be construed/deemed as incidents/events.

5.3.5 Once the incidents are detected or informed based on the above mechanisms an Incident Report as given template in Annexure-3 is initiated. The form can be initiated by any employee. Following information is required to be investigated and reported in the report:

5.3.6 Mechanism of identification of the information security incident to be documented with respect to various logs monitoring, user activity monitoring, data loss etc.

5.3.7 The detail of the incident is documented with respect to what went wrong and the impact of the incident on confidentiality, integrity and/or availability of the information/information assets. The option of high, medium or low impact is attributed based on the criticality and value of the information affected by the incident. The criticality or value is based on the classification of information. High impact should be considered for "Company Confidential" information, Medium Impact should be considered for "Internal Use" information and Low Impact should be considered for information classified as "Publicly Available" information.

5.3.8 The investigation of incident is done with respect to potential or actual causes using brainstorming and reviewing of the logs/evidence.

5.3.9 The actions are identified for the detected case of incident with respect to damage control and recovery for the information affected.

5.3.10 The long-term actions for avoiding the reoccurrence of the incident are also identified using the review and strengthening of controls.

5.3.11 Any preventive actions for similar information or information assets are also identified as learning from the incident.

5.3.12 The effectiveness of the actions taken above are also assessed after 3 months using the effectiveness scale provided in the Information Security Incident Report as per Annexure-3.

5.3.13 Before initiating any work, both the information security vendor and the customer are required to sign a Non-Disclosure Agreement (NDA). This agreement serves to protect confidential information exchanged during the course of the engagement. The agreement lays out with each party who is responsible for handling, sharing, and safeguarding sensitive data and intellectual property. Signing it shows that both parties understand the importance of keeping things confidential and agree to maintain high standards of information security during their work together.

5.3.14 Security audits shall be conducted on an annual basis to ensure data security.

5.3.15 Based on the security audit outcomes the risk assessment shall be prepared.

6. CONTINUOUS IMPROVEMENT

The organization continuously reviews and improves the pen drive usage procedure based on feedback, audit findings, and emerging security threats.
Updates to the procedure are communicated to all relevant stakeholders to ensure ongoing compliance and data protection.

- The system should have all the required restrictions and controls.
- Users should not have permission to add remove the program.
- A restriction for sharing large files over email should be in place.
- File sharing large file over emails should be in place.
- File sharing lock should be active for all users.
- Access to the server room should be through door access control for authorized users only.

7. ENFORCEMENT

7.1 Any employee found to violate this policy shall be escalated to IT.

7.2 Management's interpretation of the clauses in this policy will be final and binding. Management reserves the right to alter or amend any clause in this policy at any time as per its discretion.

7.3 Exceptions and deviations to this policy shall be documented and approved by the Respective Head. The business need for the same shall be detailed.

7.4 The evidence to be maintained are as given under:

- Incident Reports
- Communication methodology for recording of incidents.
- Feedback provided to stakeholders.
- Corrective and Preventive Action Plan.
- Incident Resolution Reports.
- Learning from Incidents.

8. EXCEPTION

8.1 Exceptions to the End Point System Security Policy shall not be universal but shall be granted by the IT Committee on a case-to-case basis These may arise, for example, because of local circumstances, conditions or legal reason existing at any point of time.

8.2 Exceptions to the End Point System Security Policy may have to be allowed at the time of implementation or at the time of making any update to this document or after implementation on an ad-hoc basis based on business or a specific and a peculiar manifestation of circumstances which could be of temporary or permanent in nature.

8.3 All exceptions during implementation shall be submitted by the concerned person responsible for implementation.

8.4 Exceptions shall not be universal but shall be granted by the IT Committee on a case-by-case basis, upon an official request made by the information owner. All Exceptions granted by the IT Committee must have a definite end date. These may arise, for example, because of local circumstances, conditions or legal reasons existing at any point of time.

8.5 All exceptions during implementation shall be submitted by the concerned person responsible for implementation. These shall be submitted through an Exception Form and sign-off on the same shall be maintained including ad-hoc requests.

8.6 The System Administrator shall review all exceptions periodically for validity and continuity.

9. VIOLATIONS AND DISCIPLINARY ACTION

9.1 In case of violations either by employee or third party shall be escalated to IT.

9.2 Violations by third parties shall also come under the purview of the Information Security Framework and action shall be taken accordingly.

10. AMENDMENTS

The Company reserves the right to amend or modify this Policy in whole or in part, at any time without assigning any reason whatsoever. However, this policy, in whole or in part, shall stand modified/amended from time to time, without any further action on the part of the Company, as and when there would be any statutory modification(s) / amendment(s) / revision(s) to the applicable provisions to it.

ANNEXURE – 1

Request for USB storage Issuance

Location: **Rau** □ **SEZ** □ **Subsidiary Unit** □ ____________

User Name	:	
Employee Code	:	
Department	:	
Purpose	:	
Requirements Type	:	**Temporary** □ **Permanent** □

Requested by:
User
(Sign & Date)

Approved by
User HOD / Designee:
(Sign & Date)

USB storage issued by Administrator (IT):

Remark: ____

Issued by:
Name & (Sign & Date)

ANNEXURE - 2

REQUEST FOR DISABLE / ENABLE USB RESTRICTION

Location: Rau □ SEZ □ Subsidiary Unit □ ____________

System ID	:	
Department	:	
Reason for Enable / Disable USB Restriction	:	

Remark: ____

____

Requested by:
User
(Sign & Date)

Approved by
User HOD / Designee:
(Sign & Date)

Enable / Disable USB restriction by Administrator (IT):

Done by:
Name & (Sign & Date)

ANNEXURE - 3

Information Security Incident Report

Date:

Incident No. -

Identification Method for Incidence:

Details of Incidence (What went wrong):

Investigation (Reasons):

Details

Impact on CIA	Confidentiality	Integrity	Availability
High			
Medium			
Low			

Action for above case:

Details

Responsibility	Planned Date	Completion Date	Effectiveness Rating	Status/Remarks

Corrective Actions (To avoid in future):

Details