Information Technology Policy

Version 3.0
March 2024

LAURUS Labs

Laurus Labs Limited
Hyderabad

Content

1. Introduction

Information technology (IT) is widely used throughout Laurus Labs Limited and is critical to the effective operation of the organization. The Company faces numerous challenges in the IT environment. At the same time, the growing dependence on technology for managing business and to minimize exposes of substantial IT security risks for the organization.

Accordingly, the management of Laurus has identified the need for a comprehensive manual to detail policies and procedures related to Information Technology including Information Security.

The policies prescribed in this document provide a minimum framework for managing the IT function as a whole, thereby inducing consistency in the implementation and governance of the IT function.

The document provides generic guidance. It does not set out to define a single solution appropriate to every process of the IS Department. While there is no universal solution, the document addresses many common processes, which an IS Department might face during its day-to-day operations.

The document would also bring about transparency in the IT Management and Operation process. The Policies and the corresponding Procedures documented here would enable transparent and consistent functioning of the IS Department.

This document is essentially an IT operational policy and not an IT strategy document. The usage of this manual extends to the employees, vendors, and business partners of Laurus. The document is issued under the authority of the Execute Director (ED) and is an Internal Document of Laurus. Access to one or more parts of this document to an employee or Third Party shall be on a "need-to-know" basis and approved by the ED / IT Head / Location IT Manager. Every person in custody of this document has the responsibility for ensuring its confidentiality.

This document has been divided into the following sections

- IT Function at Laurus Labs
- Job Responsibilities
- IT Policies
  - Asset Management Policy
  - Acquisition & Implementation of Packaged Software
  - Change and Problem Management Policy
  - Configuration Management Policy
  - IT Security Policy
  - Capacity Planning and Performance Management Policy
  - Business Continuity Policy

- Third-Party and Outsourcing Services Policy
- Training and Development Policy
- IT Audit Policy
- Exceptions to the Policies

2. IT Function at Laurus:

The Information Systems function is a key enabler and catalyst for the business. Given the increasing dependence upon IT and consequently the increased expectations from an IT Function, the management of Laurus recognizes the need for a robust IT setup including the organization structure and the most up-to-date technology infrastructure, to effectively and efficiently meet its business requirements. The key objectives of the IT Function at Laurus include:

Enterprise Infrastructure and Systems Operations - IS Department shall establish, maintain, and enhance Enterprise Information systems, and Infrastructure services to support Laurus business requirements.

Operational Excellence - IS Department shall implement operational best practices to provide superior availability, reliability, and performance of IS services. This will be done in a partnership approach that emphasizes communication, mutual accountability, and cooperative planning with business units.

Enterprise Security and Disaster Recovery - IS Department shall maintain reliable, secure, confidential, and continuous enterprise operations through policies, procedures, monitoring, risk assessment/planning/mitigation, recovery planning, and periodic testing.

Return on Investment - IS Department shall work with all business units of Laurus to assure that benefits from Enterprise IT investments are optimized while meeting business requirements and managing total cost to the Organization.

Emerging Technologies - IS Department shall identify emerging technologies and evaluate selected ones to determine the potential benefit to Laurus.

The various types of services provided by the IS Department include:

- **Planning services** - Such as advice and guidance on the development of IT strategies.

- **Operational services** - Continuous or regular delivery of services such as access to applications and data, operating computer systems and maintaining networks, and associated customer support facilities

- **Project services** - Such as applications software development.

Currently, the IS Department is primarily responsible for the planning, delivery, and management of operational IT services, and the management of the IT infrastructure across businesses and locations.

The current IT Organization structure may be enhanced/modified to meet changing business requirements. The broad roles and responsibilities of each of the functions are provided in the following section.

3. Roles and Responsibilities

3.1 Executive Director

I. To provide strategic oversight of IS Department.
II. To review and evaluate strategic IT initiatives.
III. To formulate and communicate the Global IT Strategy and Plan.
IV. To manage Information Technology as a business – responsive and sensitive to business needs.
V. To advise Business Functions on technology-enabled business opportunities.

3.2 IT Head

I. To monitor the IT Strategy and Plan.
II. To be responsible for Capital Planning, Investment Management, and Procurement.
III. To be responsible for overseeing the implementation of approved IT Policies including IT Security.
IV. To be responsible for overseeing all IT initiatives.
V. To be responsible for workforce planning and fostering ongoing development of the IT skill base including succession planning.
VI. To be responsible for overseeing the IT operations.

3.3 SAP – Application Manager

I. To take complete ownership of SAP Application from the technical perspective and to continuously review and identify the scope of improvement.
II. To be responsible for the implementation, monitoring, and compliance of the IT policies, procedures, and guidelines including information security in the related domain
III. To provide ongoing inputs and advice to the business team on the ability and feasibility of automating business process requirements using SAP and/or associated solutions.
IV. To approve and validate any new Access to be provided to the System.
V. To ensure compliance to timely application of patches to SAP application including upgrades and to ensure through monitoring and review the design and operating effectiveness of Backup.
VI. To monitor and review all SAP security requirements, periodically.

VII. To liaison with SAP vendor(s) on an ongoing basis and track vendor product and organization developments that may have an impact on Laurus SAP systems.

VIII. To participate in the Business Continuity Planning, testing, and maintenance process relating to SAP as one of the team members along with the business and other team members.

IX. To review, escalate, and manage incidents relating to SAP applications.

3.4 Corporate IT Manager - Network and Infrastructure

I. To be in charge of the entire network & Infrastructure of Laurus offices across India and coordinate with other location IT managers to assist in network and infrastructure-related issues.

II. To understand market trends in technology to leverage it for Laurus.

III. To assess the impact of change in technology for Laurus.

IV. To be the highest point of escalation for any network and Infrastructure related problems.

V. To lead and manage a team responsible for day-to-day operations related to the Server and Network Infrastructure of Laurus.

VI. To lead and manage a team responsible for IT asset management across the organization.

VII. To co-ordinate with the Finance Department / QA Department regarding asset management.

VIII. To work as a Change Manager, Configuration Manager, and Third-Party Manager for Network and Infrastructure related activities.

IX. To be responsible for the implementation, monitoring, and compliance of the IT policies, procedures, and guidelines including information security in the related domain.

X. To be responsible for Incident Management

XI. To ensure a proper Backup process adopted by the team

XII. To assist in developing the technical/managerial skills of subordinates through mentorship, & formal training.

XIII. To review the performance of the function against established performance levels.

XIV. To approve and validate any new access to be provided to the system.

XV. To monitor and review all network and server security requirements, periodically.

3.5 Location IT Manager

I. To be the prime responsible person for all IT-related activities and issues in the respective location.

II. To be responsible for the asset management in the respective location or offices and shall accordingly be the "Asset Manager".

III. To facilitate the asset acquisition as per the local requirement and to coordinate with the corporate IS Department for alignment with a corporate asset acquisition strategy.

IV. Shall also assume role as change manager, configuration manager, and third party manager.
V. To be the initial point of escalation for any ERP, application, network, and Infrastructure related problem in the location.
VI. To be responsible for maintenance and support of any location-specific application that may exist.
VII. To be responsible for the implementation, monitoring, and compliance of the IT policies, procedures, and guidelines including information security for location-specific operations.
VIII. Coordinate and liaison with the corporate IS Department for any major application acquisition or implementation.
IX. To report to the corporate IS Department regarding any local regulatory compliance, Audit, etc., relating to IT.

3.6 System Administrator

I. To manage servers (Application/Database/File/FTP/E-Mail/Proxy etc)
II. To install and maintain servers as per the best practices/installation guides
III. User management
   a. Creation/revocation/change of approved user IDs
   b. Archiving access request/approval trails
   c. Helping network and systems head for access-list validation/Audit
   d. Regular Monitoring of access logs
IV. Backup management
   a. Taking and Archiving backup of all systems as per the backup policy
   b. Backup testing and validation at regular intervals as per the policy
   c. Restoration of systems form backup in case of failure or data loss
V. System performance and capacity monitoring
   a. Monitoring of system resources (disk/memory/CPU) utilization and preparation of reports.
   b. Escalation of the event in case resource utilization goes beyond a defined threshold.
VI. Shall act as a configuration administrator

3.7 Network Administrator

I. To manage all network equipment (Routers/Switches/Firewall/IPS etc)
II. To install routers, switches, and other network-related equipment
III. To upgrade OS and other software for network infrastructure, taking back up & configuration of network equipment and storing it periodically
IV. To manage network connectivity between various Laurus offices
V. Will act as "Asset Manager" and maintain and update asset inventory
VI. Configuration management.
VII. Backup management
   a. To take a backup of all network components before making the changes
   b. To restore systems from backup in case of device failure or data loss

c. To monitor network resources (Network Bandwidth, Hardware CPU/Memory) utilization and preparation of reports

3.8 Security Administrator

I. To adhere to all security best practices as suggested by the Corporate IT Head.
II. To monitor all security logs and to escalate, investigate and resolve any anomaly noticed.
III. To implement and ensure security configurations of Network devices/servers/applications are as per the vendor-provided best practices.
IV. To manage and monitor firewall policy, logs, and generate reports from that periodically.
V. To maintain and monitor Intrusion Detection System rules and logs/alerts.
VI. To maintain and monitor Antivirus and update the software patches as and when required for any components
VII. To monitor any new vulnerabilities and threats published by vendors and inform the operations team about countermeasures.
VIII. To implement all audit recommendations.
IX. Shall act as a configuration administrator.

3.9 Database Admin

I. To coordinate, install, or upgrade the database
II. To work on the creation, maintenance, and monitoring of database entities.
III. To maintain all databases and related applications.
IV. To be the single point of contact for all database-related issues.
V. To work on, and resolve all database-related issues and problems.
VI. To have write/update access on the production instance.
VII. To ensure, review, and monitor user management.
VIII. To review and monitor the database capacity and performance.
IX. To ensure version control and maintenance of the configurable items.
X. To move database applications into the production environment with the help of an approved deployment or release Plan.
XI. To take regular backup of the database as per the backup and restoration Policy.

The above-mentioned roles and responsibilities of the various functions within the IS Department should, ideally, be performed independently to maintain segregation of duties. However, due to business and operational constraints should more than one function/role be performed by the same individual. Other roles relating to SAP Application are being mentioned as part of the SAP Maintenance Procedure document. Detailed SAP Maintenance procedure document is being followed to maintain the SAP Application.

4 Asset Management Policy

This policy is aimed at covering Asset Management in terms of –

- Purchase or Acquisition of new Assets
- Asset Ownership and Use
- Asset Classification
- Upgrade of Assets
- Process of Asset Retirement/Disposal and Write-off
- Asset Installation and Qualification

Assets that would a part of this Policy include -

- Computing Devices (Desktop, Laptops, LCD/LED Monitors, etc.,)
- Output Devices (Printers, CD/DVD, Writer, etc.)
- Input Devices (Keyboard, Mouse, Scanners, CD/DVD, etc.)
- Servers
- Application Software (Standard Packaged Software)
- Storage Devices (Personal Storage, Backup device, etc.)
- Network and Communication Applications
- Telephone, Audio, Video equipment, and conferencing devices

4.1 Asset Purchase and Acquisition

I. Information Technology Purchases shall be based on Business Need
II. The IS Department or business user department shall initiate the purchase of any information technology asset.
III. Any asset acquisition initiated by the business user department shall be approved by the business unit head as per the budgets/requirements and recommended by the IS Department
IV. The SCM/Purchasing department shall seek, where required, inputs from the IS Department, in finalizing the list of vendors for IT assets.
V. In case of recurring purchases of a similar asset, SCM shall conduct procurement based on standardized technology guidelines, as provided by the IS Department, from time to time.
VI. Any Asset Purchase and Acquisition contract shall be awarded after following the Vendor Evaluation and Selection process, by the SCM.
VII. Procurement of Software licenses shall be on a need basis, based on requisite prior approval.
VIII. Financial approval for the procurement of IT Assets shall be followed as per the capital asset purchase process of the company.

4.2 Asset Ownership and Use

The ownership of the IT Assets shall be vested with the IS Department. The custodianship of the IT Assets shall be:

a. Individuals in the case of all Personal IT Assets like PCs, Laptops, Personal Printers, Scanners, etc.
b. Administration / Security in-charges in the case of Network printers and common IT equipment like network switches routers etc.
c. The IT Assets provided to individuals shall be for Business/Official Use only.
d. In case of Asset replacement, old assets should be returned to IS Department immediately after the new asset has been provided.
e. Assets in IS Department shall be reissued to new Users, and the details of the same must be maintained.
f. IS Department shall technically review the latest configuration/technology of personal computers/Laptops periodically and recommend a standard configuration to the SCM Department.
g. The User, User Department, and the Local Administration shall be responsible in the event of misplacement or theft of any IT Asset.
h. Employee personal computers should not be connected to the corporate network.
i. Only licensed and approved software (including freeware/shareware/open source) should be installed on IT assets.
j. The IS Department shall have all rights to track and verify the configuration of the hardware and software of the IT Asset, for audit and/or maintenance activities.

4.3 **Asset Allocation**

I. Laptop Allocation

Allocation of laptops to Laurus employees shall be based on business need and laptops shall be allocated to the employees as per the HR policy. For all the other people based on business need with the approval of concerned department Head followed by IT Head or HR Head.

II. Desktop / Thin Client Allocation

Allocation of desktops to Laurus employees shall be based on business needs. Desktop / Thin Client shall be allocated with the approval of the Head of Department / Location Head / IT Head.

III. All other peripheral Devices allocation

Allocation of other peripheral devices shall be done with the approval of the Corporate IT Head / Head of the Department / Head of the Location / Executive Director.

4.4 **Asset Classification & Labelling**

I. All IT assets shall be classified into the following broad categories for grouping (based on homogeneity), identification, and tracking.
   a. Personal Computers (Desktop PC, Laptops,)
   b. Servers
   c. Printers
   d. Application Software
   e. System Software
   f. Networking
   g. Communication (Data / Voice, /video
   h. Security
   i. Power Systems

II. Computer Accessories

III. The IT Assets (shall be uniquely numbered and inventoried in the Asset database maintained by the IS Department and labeled for identification and verification. Access to the Asset database shall be restricted to limited people in the IS Department with prior approval of the Corporate IT Head/ Location IT Manager.

IV. If the IT Assets are being used in the GMP environment/process, labeling will be followed as per the QA numbering procedure.

4.5 **Asset Upgrade**

I. Assets (personal computers/ Laptops) shall not be upgraded within 5 years of the procurement unless approved by the Corporate IT Head/ Location IT manager based on business and applications needs.

II. Software upgrades shall be carried out based on application requirements and support considerations.

III. The Asset Database shall be updated with the upgrade details, by the IS Department.

4.6 **Transfer of Assets**

I. Transfer of PCs from one user to another user or from one location to another location shall be carried out with approval.

II. Transfer of Assets such as Servers, Networking and Telecommunications, Security and Power Systems shall be carried out only upon prior approval of the IS and Finance Departments.

4.7 **Retrieval of Assets**

I. Assets shall be retrieved from the Employees / Temporary Hires / Third Party etc., in case of employee separation or on providing a new asset in place of an existing asset or end of temporary asset requirement.
II. The Asset database details shall be updated in all such cases.
III. The IS Department shall inspect the Asset at the time of retrieval for damage. In case of damage identified by the IS Department as due to negligence / improper use by such user, the IS Department shall recover, from such employee, temporary hire, third party, an appropriate residual amount, for such damages, after considering warranty/insurance cover for such asset. Any deviation shall be approved by the Head of IT / Head HR / Executive Director.

4.8 Asset Retirement and Disposal

I. The IS Department shall retire the IT assets (PCs and Laptops) from use, based on the company's approved Asset Retirement process i.e. timeframe of 5 years. The Corporate IT Head/ Location IT Manager, on a case-to-case basis, determines the retirement of all other IT assets (excluding PCs and Laptops).
II. IS Department may decide to retire the Assets before the life period of the asset for some special reasons listed below
    a. Technology obsolescence
    b. Defective Hardware
    c. The prohibitive cost of maintenance
    d. Damaged or un-repairable condition
III. The retired Assets on retirement may be disposed of in any one of the following ways, as may be decided by the IT Head, and obtain the approval for disposal, as per the organization's asset retirement procedure.
    a. Donation to Charitable / Other institutions
    b. Sold to third parties
IV. The IT Assets for disposal shall be cleansed of any specific licensed / proprietary software and data, by the IS Department.
V. In case the disposed of assets need to be destroyed, the IS Department shall ensure adherence to any location-specific applicable environmental and safety guidelines impacting the disposal of IT Assets and guidelines of QA or EHS Department.
VI. The Asset Database shall be updated upon retirement and disposal of assets, by the IS Department.
VII. The IS Department shall provide a list of all disposed of assets to the finance department.

4.9 Asset Validation

As per the Quality process and SOPs, Validation shall be carried out for the assets used in the cGMP environment.

5 Acquisition & Implementation of Packaged Software Policy

Introduction

This Policy is aimed at covering the Purchase, Acquisition, and Implementation of Standard Packaged Software including Commercial Off the Shelf and Modified Off the Shelf such as ERP Packages, SCM packages, etc. that can be customized and configured to suit the business needs of Laurus.

The purchase and installation of Standard Packaged Software, for office automation that does not require customization (such as MS Office, Internet Explorer, Visio, Operating System Software, and Network Software, etc) shall be covered as part of the Asset Management Policy.

The objective of this policy is to ensure a consistent approach toward the acquisition and implementation of standard packaged software.

Purchases of standard packaged software shall be based on business needs. Any such purchase can be initiated by the IS Department in coordination with the Business User Department or vice-versa.
Detailed business need analysis shall be conducted and a high-level functional requirements specification shall be prepared by the requisitioning user department. The business need analysis shall also include an estimate of the proposed user base. Business Justification of the proposed investment and impact (if any) of the proposed standard packaged software on other applications or functional areas shall be listed as part of the business need analysis.

If the software is being used in a cGMP environment, the CSV process will be followed as per the applicable SOPs. Other software will be implemented as per the scope agreed by the vendor and user department.

If it is a packaged solution and multiple processes need to be configured, the Project implementation approach to be followed. The steps involved:

- User Requirements
- Business Blue Print
- Testing (unit/integration)
- User Training
- Cut-over planning
- Data Migration and Go-live
- Post Implementation

6 Change and Problem Management Policy

Introduction

The primary objective of change management is to ensure that changes to systems/applications are applied in a controlled manner so that the stability and security of systems /applications are not compromised. Problem management is aimed at providing

timely and satisfactorily addressing and resolving issues related to the usage of IT resources by end-users.

This policy defines the process for enacting changes on the IT infrastructure including application software, system software, networking resources, and computer hardware.

As a general rule, changes shall be categorized into three major types, the broad definitions of which are given below;

Major changes – Any change request shall be considered as a major change if (but not limited to)

- The change has a cross-functional impact or impacts multiple systems and applications
- The change has an impact on financial processes and applications
- The change requires significant service downtime
- The effort required for making the change is significant

Minor changes-Any other changes that do not have a significant business impact and do not require significant effort, shall be categorized as Minor change.

Emergency Change- Change request that requires immediate execution and which may have a significant business impact if not worked on immediately, shall be considered as an Emergency change.

6.1 Application Change Management

Introduction

This policy is aimed at covering requests for Application Change and Bug Resolution. An Application Change Request is defined as any request for changes to an existing system baseline, due to business requirements. Whereas a bug fix is defined as a record of error or discrepancy found in the system/application after deployment of a system or application.

Policy Statement

I. Change Requests may be initiated by any application user or the application owner.
II. Change Requests shall be processed based on prior approval, linked to the category of change.
III. All change requests shall be analyzed from the perspective of business impact in terms of time and efforts as well as security considerations.
IV. For all changes, the prior approval of the Change Control by Corporate IT Head/designee should be obtained
V. The potential impact of any change on other applications or systems or other modules in the same application shall be assessed from a risk perspective before accepting a change request and recommended the change.

VI. Adequate testing should be carried out in, controlled, and representative environment by the respective business owner before deployed into the production environment
VII. Users impacted by the implemented change shall be notified of the change
VIII. Procedures to roll back/recover from an unsuccessful change are in place where appropriate.

6.2 Emergency Changes

I. Emergency changes can be made only by persons authorized by the Corporate IT Head / Application Owner.
II. Emergency Change Requests shall be carried out upon prior notification to the Corporate IT Head.
III. All emergency changes shall be documented. The change documentation shall be carried out after the change being effected and should include the time and date of changes, commands executed, program or data affected, etc.
IV. The completed documents shall be submitted to the Corporate IT Head for approval.

6.3 Infrastructure Change Management Policy

Introduction

This policy is aimed at covering requests for Infrastructure Change. An Infrastructure Change Request is defined as any request for changes to an existing Infrastructure baseline.

The objective of this policy is to implement and ensure a sound Change Management Approach that maintains the integrity and traceability of Changes incorporated in the following systems –

- Servers and Network and Communication devices (LAN, Wireless Network, Firewall,
  Routers, Switches, etc.
- System Software (OS, Enterprise Database)
- Packaged Software Applications (MS Office, Internet Explorer, etc)

The activities about Infrastructure Change Management include software installation, change of system values, operating system version upgrade, server configuration changes, hardware changes, and changes in database settings. Application of Patches to Application Software like ERP, MS Exchange, etc shall also be part of this Policy. These can be based on

- Updates send by vendors
- Email notifications, or bulletins
- Notifications from website
- Internal vulnerability report

- Security audit report

Computing System (Desktop, Laptop, Palmtop, etc) updates are not covered as part of the Policy and would be discussed as part of Asset Management Policy.

Policy Statement

6.3.1 Change Initiation

I. Any Infrastructure Change Requests can only be initiated by the IS Department.
II. All Infrastructure Change Requests shall be segregated as Normal Requests or Emergency Requests.

6.3.2 Change Impact

I. The potential impact of any change shall be assessed from a risk perspective before accepting a change request
II. Any Changes that shall be carried out must not hamper the security of existing systems or cause any security failure.

6.3.3 Change Approval

I. Change Requests shall be processed based on prior approval, linked to the category of change.
II. Changes regarding security areas (i.e. file permissions, identification and authentication, and discretionary access control) must be approved by the Corporate IT Head/IT Change Manager or designate as per the 'Access Policy', and cannot be implemented as emergency changes.
III. Emergency change requests can be carried out based on notification to the Corporate IT Head/ Location IT Manager.

6.3.4 Change Execution

I. All Changes in the Production environment shall be announced to the intended audience before and after the implementation.
II. A Change Execution/Implementation Plan should be prepared for all Change Requests.
III. For upgrades, patches, and other items provided by 3rd party suppliers, the installation instructions must be followed to implement the change.
IV. Change requests that may have a potentially negative impact on system availability, stability, or performance shall be performed outside normal business hours. Changes that do not impact system availability, stability, or performance can be implemented during work hours.
V. All servers in the Data-Centre must be prevented from automatically updating patches and should instead be scheduled as batch processes following the normal Infrastructure Change Management process.

6.3.5 Testing of Change

Test Plan is to be prepared before implementing any Infrastructure Change if the testing is possible.

Note: Major IT changes are approved through –"Annex -01 IT–Change Request Form".

6.4 Problem Management Policy

Introduction

This policy is aimed at covering Problem and Issue Management for end-users or business users. Any problem or issue that the end-users encounter related to Application availability, access or functionality; Internet & Network availability or access; Computing devices (related to Hardware, Operating System, Packaged Software, Storage, Security, and Others); Printers/Scanners; Communications e.g. IP Phone would be in the scope of this Policy and the corresponding Procedure.

Any Problem / Issue resulting in the Application / Infrastructure Change request shall be managed as per the Change Management Policy for Application and Infrastructure respectively.

The objective of this policy is to implement and ensure a comprehensive Problem and Issue Management Approach that maintains the integrity and traceability of Problems and Issues raised by the end-users.

Policy Statement

I. A helpdesk function shall be maintained for Issue or Problem Resolution.
II. The helpdesk function shall be available during office hours.
III. Any Employee of Laurus can initiate a request for Issue or Problem Resolution.
IV. Request can be raised for self or on behalf of any other employee or department.
V. The requestor needs to submit all details related to the problem while raising the Request.
VI. Periodic exception-based reporting shall be carried out to the Corporate IT Head / Location IT Manager, for monitoring and review.

7 Configuration Management Policy

Introduction

The organization should establish procedures for implementing, managing, and controlling the changes in versions of application systems and customized add-on modules, network and operating system software, interfaces, and utilities including related documentation. This also aims at ensuring uniformity in versions running across the organization and would involve maintaining up-to-date documentation for the entire version change process. The organization should endeavor to implement the tools and utilities for automating the version control procedures and documentation.

Policy Statement

7.1 Configurable Item Identification

I. All individual items of computer hardware and network components, each instance of the system software, and application software including packaged and custom-developed and related Documentation shall be defined as a configurable item, and shall be under the purview of Configuration Management.
II. All Configurable Items (CIs) must be identified and a Configuration List shall be maintained.
III. The Naming of the Configuration Items shall be based on a predefined Naming Convention.

7.2 Document Configuration

I. In the event of the creation or updating of a document that pertains to any of the identified configurable items, the CI List must be updated.
II. The Document History/Revision Trail of the document must be updated with the changes made.
III. A formal review and approval shall be required before releasing any document.
IV. A standard numbering scheme shall be used for all documents.
V. All documents must be archived as per a defined frequency.

7.3 Software Configuration Management

Custom-developed software

I. All software application source codes shall be kept under version control. If version control is not possible, periodic backup need to be maintained
II. The Configuration Manager shall checkout the application source code for changes.
III. The new version of the application code shall be appropriately rolled out at all locations within the agreed time frame if it is being used in other locations as well.

Packaged Application Software

I. The Software Configuration Document must be updated for any changes made to the configuration of the packaged application software (after successful testing and signoff), by the Configuration Manager.
II. In case maintenance of the application, a configuration is possible in an electronic (soft-copy) format, the same shall be subject to check-out and check-in, by the Configuration Manager, as mentioned above.

7.4 Infrastructure and System software

I. All Servers, Network components, and other peripheral devices specifications shall be defined as a Configurable item (CI) as per the requirements.
II. The details for each CI shall include but not limited to –
    a. Hardware specifications
    b. System details (e.g. - version, patch level, etc.)
    c. Configuration details (e.g. – Router, firewall configuration file)

8 IT Security Policy

Introduction

The overall objective of the "Information Security Policy" is to provide guidance and direction for the protection of Laurus information systems against accidental or deliberate damage or destruction.

The objectives of the "Information Security Policy" are:

- To prevent unauthorized disclosure of information stored or processed on Laurus information systems (CONFIDENTIALITY)
- To prevent unauthorized accidental or deliberate alteration of information (INTEGRITY)
- To prevent unauthorized accidental or deliberate destruction or deletion of information necessary for operations (AVAILABILITY)

Policy Sections

- Physical Security
- Logical Access Control
- Computing Environmental Security
- Personnel Security
- Network Security
- Website Security
- Virus Management
- Backup Management
- Incident Management
- Compliance
- Acceptable usage Guideline

8.1 Access Controls

Introduction

Appropriate controls shall be established for all IT assets to ensure physical and environmental exposures (fire, cyclones, water, temperature, and humidity) are adequately controlled. Physical access to critical IT resources shall be ensured through adequate controls.

The Policy defines the minimum controls, which shall be in place to reduce exposure to these physical and environmental threats.

Policy Statements

8.1.1 Physical access control to Data Centre

I. All critical IT equipment (Servers, Routers, Switches, IPS, Firewall, etc) shall be placed in a physically secure and restricted room/Area (Data-center/Server Room).

II. Access to Data-centre shall be restricted to authorized users (Network/System administrator) only.

III. Entry and exit to Data-centre shall be restricted through the use of proximity/swipe card and/or biometric devices or by a lock and key.
IV. The Data-centre shall be under continuous monitoring by IT personnel.
V. Visitors or any third-party guests may be allowed inside the Data-centre with the prior approval of the Head Network and Infrastructure/ Location IT Manager.
VI. A Network/System Administrator shall compulsorily accompany any visitor/housekeeping staff for the duration of the visit to the Data-centre /Server Room.
VII. All instances of access to the Data-Centre shall be logged electronically or physically for periodic review.
VIII. A "Data Center Master Access List" can be maintained in Annex-05, and an Electronic/physical access log and users list shall be reviewed yearly or as when required.
IX. Laurus reserves the right to grant or deny access to the Data Centre to some or all concerned employees, vendors, and visitors at any point of time, as may be decided by the Corporate IT Head / Head Network and Infrastructure/ Location IT Manager.
X. Serving or consumption of food, beverages, or drinks shall not be allowed within the Data Centre, under any circumstances.
XI. Personnel entering the Data-centre shall adhere to basic personal cleanliness standards.
XII. Hazardous and/or combustible materials shall not be allowed within the Data-centre premises.

8.1.2 Fire

I. All computer systems shall be housed in an environment equipped with an adequate fire extinguishing system. For Data-centre / Server room Inert gas-based fire extinguishing systems or any other appropriate fire extinguishing systems shall be used.
II. The fire extinguishers shall be accessible in all areas.
III. Hazardous and combustible materials shall be stored at a safe distance from server rooms and other computer rooms. Computer supplies such as stationery shall not be stored in Data Centre / Server rooms.
IV. All new information-processing sites shall be evaluated and appropriate fire safety controls should be recommended.
V. Functioning and operations of the fire safety devices/equipment installed by Laurus shall be explained to the employees periodically during Internal Training Programs.

8.1.3 Floods and Water Damage

I. Computer and communication rooms shall not be located in areas susceptible to water seepage and flooding.
II. Computer and communication rooms shall be located on raised or elevated floors in flood-prone areas.
III. Adequate drainage provision shall be provided to prevent water damage or flooding.

IV. Electrical equipment, which may have received water damage, shall be checked and dried before being returned to service.

8.1.4 Power Supplies and cabling

I. Uninterrupted Power Supply (UPS) shall be used for continuous running of information processing equipment or to support its orderly close down.
II. The UPS equipment shall be checked at least once in 6 months or following the manufacturer's recommendations to ensure that it regulates the power supply, can handle voltage fluctuations, and can provide necessary battery backup in case of power failure. Location IT manager coordinates with Electrical Maintenance team.
III. All electrical cabling shall have proper earthing to prevent electric surges.
IV. Power and telecommunication lines into information processing facilities shall be laid as per the industry best practice (underground/cable tray).
V. Network cabling shall be protected from unauthorized interception or damage due to environmental hazards e.g. by using conduit or by avoiding routes through public areas.
VI. Power cables shall be separated from communication cables to prevent interference.

8.1.5 Physical Security of Laptops

I. Employees to whom laptop computers are issued shall be responsible for its safe custody.
II. The physical security of laptops, as well as the security of the data residing in these systems, shall be ensured by respective users
III. All laptops shall have a hard disk encryption facility.
IV. Laptops shall not be left on the desk or in the work area or any other visible location overnight. It shall be locked in a secure area at the end of the workday.
V. Laptops shall never be checked in as luggage while traveling. It must always be hand-carried in a briefcase or a laptop carrying case.
VI. All Laptops shall have access to read-only for Mass storage devices
VII. Full Access can be provided for a mass storage device upon receive approval of Concerned HOD's.
VIII. The concerned staff shall file a police report immediately in the event a laptop is stolen. The staff shall also notify the Corporate IT Head/ Location IT Manager and the respective Departmental Head / Legal Head in a day or two, of the theft.

8.2 Logical Access Controls

Introduction

Access to business information and data should be controlled to restrict access to authorized users only. If inappropriate access is granted, unauthorized amendments may be made to application software, information, or data. Therefore, a lack of strong user access management practices could affect the integrity of the computing management.

Formal procedures shall be in place to control the allocation, revocation, and review of access rights to information systems and services. Users shall be granted access based upon the principle of applying the least privilege required in the "IT System User Access Request Form" Annex - 04 for non cGMP users to achieve their desired job function.

This policy aims to ensure secure and effective access to Laurus IS assets remotely or locally. The document shall include detailed procedures and templates for

- Access allocation policies
- Access revocation policies and
- Access review policies

Policy Statements

8.2.1 Access allocation Policy (New ID, Renewal, privilege change)

I. Users shall be granted access to information, data, and applications on a "need to know" basis. Access to information, data, or applications shall be restricted according to the user's requirement or role in the organization and based on least privilege to achieve the desired business function.

II. Access to information services shall be controlled by using unique User Ids so that users can be linked to and made responsible for their actions.

III. **Internet Access-** Access to the Internet shall be given as per the business need and with the approval of the Immediate Superior and HOD.

IV. **E-Mail Access-** Laurus corporate e-mail id shall be allocated to the user as per business need and on approval of immediate superior and HOD.

V. **Packaged Software access-** New user ID for any packaged software (wherever user-based licensing is required) shall be granted with the approval of BU Head and Corporate IT Head/ Location IT Manager.

VI. **Other applications-** Access to any other applications shall be given with the approval of the application owner.
   - Application owners (Business) define the level of access within the application.
   - Only the Application Head and Corporate IT Head/Location IT Manager may be granted "Super-user" access to financial applications on the production system, for emergency use.

8.2.2 Access Revocation

I. Access revocation shall be initiated in the following cases
   a. Employee Separation/Transfer/Promotion
   b. End of temporary Service need
   c. Violation of Acceptable usage guideline

II. In case of Employee separation/transfer, the access revocation request shall be raised by the HR department and sent to the System/Network admin to revoke access

III. All temporary access to resources shall be revoked upon completion of the defined period.

IV. The Corporate IT Head/ Location IT Manager reserves the right to temporarily revoke any access granted to any user on the identification of any suspicious activity that may be detrimental to the interest of the organization.

Note:

1. In case separated Employee having Email access and communication to the external business partner, the Email account will be retained and mails will be forwarded to HOD nominated employee, for a maximum period of 12 months or an extended period approved by the HOD.

2. On receipt of separation intimation, IS administrator will change login credentials (within Five Working Days) and no one will log on to the account / no outgoing emails from this account.

3. As part of the Annual access review, separated employee IDs will be reviewed and necessary action shall be initiated by IS Administrator to close the account or extend the validity, as approved by the HOD.

8.2.3 Authentication

I. User login credentials will be created in the active directory, the same will be used for system and email authentication.
II. Application user login credentials are maintained in the application's local database.

8.2.4 Access review

Access list (user list) review

I. The access privileges, as defined in the system, shall be subject to periodic review, for validity, by the designated business process owners or the Corporate IT Head/ Location IT Manager, as the case may be.
II. Application user's privilege levels shall be reviewed and validated periodically by the business process owner.
III. Email / Domain user accounts shall be reviewed with the employee list, once in a calendar year and maintained in the "Annex-02-Active User List Review Log".
IV. In case employee retired and extends his / her service, shall be treated, as a regular employee, and privileges/access shall be provided, same as previously having.
V. In case employee transferred to Subsidiaries of Laurus Labs Limited, Domain / Email access shall be continued, same as Laurus Labs, as suggested by the HR / HOD.

Access log review of critical servers/ financial applications

I. The Systems Administrator shall review system access violation logs.

II. The respective Application owner within the IS Department shall review application access logs.
III. For all financial applications, adequate logging of user activity shall be enabled.
IV. All-access violation attempts (user and resource authentication) shall be logged and reported by the Systems Administrator / Application owner to the Corporate IT Head/Business Unit Head/ Location IT Manager as deemed appropriate, for necessary action.
V. All system and application logs shall be maintained in a form that cannot readily be viewed by unauthorized persons. A person is unauthorized if he or she:
   - Is not a member of the internal audit staff
   - Is not a member of IS Department staff
   - Does not need to have such access to perform regular duties

Privileged User Access Log Review

Privileged users access logs of the Active Directory Server, shall be reviewed periodically. Based on the log storage size review cycle shall be decided by the Head IT.
A list shall be maintained and reviewed in "Annex- 03 List of User Access Granted By Exception".

8.2.5 Group Policy

All group policies are configured in the Domain controller by creating a different Organization Unit (OU). The Group Policies are being defined in each OU. A new user /system is created in the respective OU to apply the required policies. These Policies can not be changed by the Local Admin.

8.2.6 User ID Rules

I. There shall be a one-to-one relationship between user Ids and individuals, except group ids.
II. Any group ID (E-mail) required for a specific business purpose shall be created with the approval of the Departmental Head and Application head/ Location IT Manager
III. User Ids shall follow a standard naming convention for all computer systems to facilitate user identification. Naming conventions shall cover all end users, contractors, consultants, auditors, and vendors.
IV. All user accounts created in all systems & applications should contain the complete details of individuals like Full name, business unit details, department, employee id, etc.
V. All "Default" user-ids that are shipped with the application shall be deactivated if not used.
VI. Inactive users shall be logged off from applications after a predefined inactivity time.
VII. Generic Login ID details issued to Finance, SCM, BD, IS and SAP Departments, shall be maintained " Annex-03 List of Users – Access granted on Exception".
VIII. User ID shall be locked after a predefined number of failed login attempts.

IX. Generic login IDs are being provided to logon to the Windows Operating system as a process:
- Instrument / equipment connected systems /
- Teams working in shifts /
- Department-specific Users in Plant operations departments, to have a common communication based on the approval of Department HOD / Designee
- Instrument/equipment, application level, individual logins

8.2.7 Password Management

I. The minimum password length is 8 characters and a mix of alphanumeric characters, maximum password age is 90 days, history of 8 passwords is maintained, the system locks after 5 failed log-in attempts and a password history file is maintained to prevent the reuse of passwords for atleast 3 cycles.
II. Easy to guess passwords shall not be used.
III. Passwords shall never be displayed in clear text or stored in readable form in batch files in automatic login scripts, in terminal function keys, in computers

without access control, or in other locations where unauthorized people might discover them.

IV. Vendor supplied and default passwords are changed immediately upon installation.

V. First Time password

a) Systems that allow users to change the password after the first logon may have a standard predefined 1st-time password and users shall be forced to change the password after the first login.

b) Wherever system/process does not force/allow users to change the password after the first login, the password generated by the administrator should be unique and shall be communicated to the user in a secured manner. Conveyance of passwords through unprotected (clear text) electronic mail messages shall be avoided.

VI. In the event a staff member who has privileged access is terminated or has resigned, the password for privileged access shall be changed.

VII. System files holding authentication data or passwords shall be protected from unauthorized access.

VIII. All users shall keep passwords confidential.
Note: 1. Employees working outside the Laurus Labs LAN cannot reset the password directly, the administrator should set the password or set the password policy age without expiry to such users. 2. Service Users password policy age without expiry, shall be maintained.

8.3 Personnel Security

Introduction

The employees are the most valuable assets. However, careless, uninformed, undisciplined employees may cause significant problems relating to information security. At the same time, associates are ultimately responsible for controlling the dissemination of confidential information. Therefore, human resource security policies must be implemented to address the risks of human error, theft, fraud, or misuse of facilities and assist all personnel in creating a secure computing environment.

Policy Statements

8.3.1 Security during Hiring, Transfer, and Termination

I. All employee and contract staff of the IS Department shall be subject to a formal pre-employment screening, which shall include the following:
- Availability of satisfactory references
- Appropriate background check
- Appropriate identity checks (passport or similar document)

II. All employees shall sign a confidentiality or nondisclosure agreement upon initiation of employment.

III. All employees shall acknowledge the organization policies and Acceptable Use policy.

IV. In case of employee separation/termination, formal clearance shall be obtained from IS Department before being formally relieved.

8.3.2 User Responsibilities / Accountability

I. Reporting security Incidents -Any personnel who becomes aware of any loss, compromise, or possible compromise of the information systems, or any other incident which has security implications on the information systems, shall immediately report the incident to the IS Department, or corresponding Business Unit Head.

II. A formal disciplinary process shall be established for employees violating Information Security Policies and Procedures. Such a process would act as a deterrent to employees who might be inclined to disregard security procedures. Additionally, it would ensure correct and fair treatment for employees who are suspected of committing serious or persistent breaches of security.

8.3.3 Security Awareness and Orientation Session

I. The Security Awareness Orientation program shall include the following areas:

- Introduction to Information Security
- Password Guidelines
- E-mail system
- Internet Usage
- Desktop / Laptop Security
- Data Backup
- Virus Controls
- Physical Security
- Reporting of Security Incidents

II. IT Policy shall be placed in the Intranet for employees' review.

8.4 Network Security

Introduction

Network security forms an integral part of the overall Information Security and is important to all users. Network security assumes importance to Laurus when viewed in light of the following:

- Networks change frequently as new users and devices are added and newer data communication technology is introduced
- Usage of various networking, communications, and computing technologies to effectively meet the user needs

Policy Sections

The Policy consists of the following sections:

- Servers/OS
- Router

- Firewall
- IPS
- Switch
- Wireless
- Internet Security
- E-mail Security
- VPN Security

8.4.1 Server Control

I. The purpose of each server on the network shall be identified and how the server would be used.

II. The network services, software, and other applications or utility software, installed on a server, shall be identified.

III. All critical parameter settings, scripts, and configuration files used during the installation of a network operating system shall be maintained.

IV. The following issues shall be considered while deploying a network server:
- The categories of information that shall be stored on the server
- The security requirements for that information
- The network services that shall be provided by the network server
- The security requirements for the network services

V. Operating System shall be hardened through the following:
- The latest approved hotfixes / Patches shall be applied
- Configure security policies for authentication and access control
- All unnecessary users (e.g. guest) shall be disabled
- Default passwords shall be changed as part of the installation process.
- Inactive terminals shall be set to a timeout of 15 minutes wherever applicable.

VI. Password policy shall be configured as per the Standard password policy defined.

8.4.2 Routers

Best practices from router OEM shall be used for the configuration of a router. This shall include -

I. Unnecessary services of Routers shall be disabled

II. Remote and local access to routers shall be restricted to limited users.

III. Appropriate ACLs (access control lists) shall be applied to allow the desired services only.

IV. Time out for all modes of access sessions to the Routers (Telnet, Console, Aux) shall be set to a time out of 15 minutes.

8.4.3 Firewall

I. A Firewall should be appropriately implemented to segregate the networks into different network segments. The following should be considered during the implementation of a firewall system-
- Specific security guidelines as specified by the firewall vendor should be configured.

II. The firewall /Gateway system shall deny all inbound and outbound services unless specifically permitted.

8.4.4 Intrusion Prevention System (IPS) / Monitoring

I. IPS shall be deployed for the critical segments of the network.
II. IPS logs shall be monitored and reviewed.

8.4.5 Switch/LAN

I. Access to all switches shall be restricted as per the access policy
II. Various network segments shall be segregated through the implementation of VLAN.
III. Critical segments of the network (DMZ, Internal Servers, etc) shall be segregated from other network segments.

8.4.6 Wireless Access Points

I. Wireless Access Points default password shall be changed.
II. An appropriate encryption mechanism shall be configured for wireless LAN communication.
III. The SSID of the Access point shall be changed from the factory default to prevent easy access.

8.4.7 Database

I. The database server shall be placed behind a firewall and IPS shall be used to detect any intrusion attempts.
II. The database server process should run as a user with minimum required privileges and never as an administrator.
III. Default database users not required should be disabled.
IV. The database server should not be assigned publicly accessible IP, and access to the database should be allowed only from the Web Server/Application server on a particular port only.
V. Direct access to backend database servers (production) shall be strictly restricted to the authorized person.

8.4.8 Internet Security

I. Access to the Internet shall be given as per responsibility requirements.
II. All Internet connections shall pass through a firewall and\or a proxy server.
III. Guest internet access will be provided to the visitors on a seperate VLAN.
IV. Internal users shall be prohibited from accessing Web Sites that are deemed inappropriate.
V. The Systems and Network Head/ Location IT Manager shall define the protocols/services/sites to be allowed for use.
VI. Monitoring World Wide Web activity shall ensure that users are not accessing sites containing inappropriate material and shall ensure that proper levels of security are used.

8.4.9 E-Mail Security

VII. Corporate E-mail access shall be given to users as per the access policy or on a business need basis with the approval of the Department HOD.

VIII. Users shall have to adhere to E-Mail access guideline as defined in the "acceptable use guideline".

IX. Every user shall be provided with a fixed quota of disk space for email purposes wherever applicable.

X. The maximum filesize for email attachments shall be restricted to a fixed size for security reasons.

XI. An E-mail content filtering mechanism shall be deployed at the gateway level.

XII. All e-mails shall carry the following standard footer banner.

"DISCLAIMER
The information contained in or accompanying this e-mail is intended only for the use of the stated Recipient and may contain information that is confidential and/or privileged. If the reader is not the Intended recipient thereof, you are hereby notified that any dissemination, distribution, or copying of this e-mail is strictly prohibited and may constitute a breach of confidence and/or privilege. If you have received this e-mail in error, please notify us immediately. Any views or opinions presented are solely those of the author and do not necessarily represent those of LAURUS Labs Limited. There may be an attachment(s) to this e-mail that may contain software viruses that could damage your computer system. While LAURUS Labs Limited has taken every reasonable precaution to minimize this risk, it cannot accept liability for any damage that you may sustain as a result of software viruses. You should carry out your virus checks before opening the attachment(s)".

8.4.10 VPN Security

I. Strong user authentication shall be implemented to ensure the privacy of client-to gateway communications. The authentication methods deployed may include traditional username/password authentication.

II. VPN Server rules shall state those machines which users should have access to System Administrator / In-charge must set rules at VPN Server for outbound traffic such as limiting use by user/group, time of the day and should filter out any unwanted content using plug-in filters.

III. VPN access shall be provided to the Employees / Vendors based on the request received from the User with HOD/Designee approval or HR or Departmental HOD / Designee. The request can be sent through the mail to IS department or "**Annex-04 - Access Request Form**".

IV. VPN users access is reviewed with Active employees once in every calendar year.

8.5 Web Site Security

Introduction

Recognizing the importance of the corporate website as a means of communicating with the stakeholders and communities, at large, integrity and availability of the same is paramount. This policy discusses the standards applicable for Laurus websites and shall also be applicable for any other website hosted by subsidiaries and affiliates across the globe representing Laurus. The following controls shall also be used for website security, wherever applicable.

Policy Statement

8.5.1 Domain Name Security

I. Use of any website to be hosted representing Laurus shall be authorized by the Corporate IT Head/Location IT Manager. Any authorization by the Business shall be routed through the Corporate IT Head / Location IT Manager for final hosting.

II. Access to domain name registration information shall remain with the Corporate IT Head/ Location IT Manager. The Corporate IT Head/ Location IT Manager shall do any changes to domain name registration information only upon authorization.

III. The Corporate IT Head/ Location IT Manager in consultation with the Corporate Communications Department and the Business Units shall identify possible domain names representing the Laurus brand and shall take appropriate initiatives to proactively take control of these domains, to prevent any misuse of Laurus brand name.

IV. Any known and reported instance of the public website(s) causing harm (through its content or domain name) to the public image of Laurus, once brought to the notice of the Corporate IT Head/ Location IT Manager, shall be communicated to the Corporate Communications Department and Legal department for necessary action.

8.5.2 Web Site hosting

I. The Corporate IT Head/ Location IT Manager shall formally approve web site hosting location and platform.

II. Appropriate security controls as mentioned below shall be implemented as part of website hosting.

III. Perimeter Security-

- Public web servers shall be placed in a demilitarized zone (DMZ) secured behind a firewall and IDS/IPS.
- Firewall, IDS/IPS, and Routers shall be configured as per the best practices defined.
- The firewall shall filter traffic between the Internet, Intranet, and DMZ section and shall allow only the minimal required protocols/Services.

IV. Host Security-

- The operating system on which the website shall be hosted shall be hardened/secured as per vendor-suggested best practices.
- The operating system shall enable the required logging. Web Server access and security logs shall be analyzed daily.

8.5.3 Content upload and management

I. Any content uploading/modification/change to the public website shall be done with prior approval from the Corporate Communications Department and the Corporate IT Head/ Location IT Manager.

II. Access to the webserver shall be restricted to the user on a "need-to-do" basis and should be as per access policy.

III. The latest content and configuration of the webserver shall be uploaded to the configuration management database as per the configuration management policy.

IV. Content of websites shall be backed up as per the approved backup policy.

8.5.4 Third-party hosting

I. Selection of third-party hosting services shall specifically include security requirements as per business needs. The organization should be able to showcase its process maturity in terms of security.

II. In case of third party hosting, appropriate contract and SLA shall be followed

8.6 Virus Management Policy

Introduction

All workstations (desktops and laptops), servers, and other information processing equipment under Laurus shall be adequately protected against all viruses/Worms/Trojans.

Policy Statement

I. Anti-virus software, approved by the IS Department, should always be kept running on all desktops/laptops/servers without exception.

II. User systems shall be configured to download the latest virus protection signature files from Internet sites/Intranet servers after confirmation of IS Department.

III. Virus scanning should be done on all software/files supplied by a third party in the form of CDs/DVDs/USB drives or any other removable media before loading it into the system.

IV. The users each time any file is copied from any source including network drives and any removable media shall perform virus scanning.

V. All information or files downloaded from the Internet and all mail attachments shall be scanned for viruses automatically.

VI. In case a virus outbreak alert is received, the IT Help desk and Head Network and Systems/ Location IT Manager shall inform all the users immediately about the ways and means to protect against the virus attack.

VII. If a virus attack is suspected, the following shall be observed:
   a. Suspected tape / CDs / disk shall be isolated
   b. Affected server / PC / laptop shall be isolated

VIII. Gateway antivirus shall be implemented for the E-mail server. All incoming and outgoing mails shall be scanned for viruses automatically.

IX. Virus affections should be recorded as "incident" events and the Systems Administrator shall duly maintain a log of the same.

X. Anti-Virus updated to the systems based on their groups. The groups are being classified and updated as follows:
- End-User Systems – Pushed centrally based on the updates released by OEM
- Instrument Connected Systems - Tested in one of the instrument systems and pushed to other GMP application connected systems.
- Server – updated based on the testing

8.7 Backup Management

Introduction

All software and data shall be backed up regularly to ensure that each application and its data can be recovered in the event of operations failure, loss of service, or loss/corruption of data.

Policy Statement

I. The IS Department shall maintain documented backup and recovery plan and procedures for the following-
- Application Data
- Data in the File Servers
- Electronic Mails
- System Software like Operating Systems
- Parameter and Configuration files/information of network devices
- Projects Data

II. The backup plan shall include
- Folders/files to backup for each server
- Frequency/interval of backup
- Media of backup
- Frequency/Interval of backup testing
- Labeling standards/convention

III. The backup procedure for each application and end-user data will be transferred to the backup server daily. Data from the backup server will be transferred to data tapes weekly. Project-level backup will be done monthly.

IV. The Corporate IT Head/ Location IT Manager shall approve the backup and restoration plan.

V. All users are responsible for all information residing on their respective desktops or laptops. Users can secure critical business information by performing online backups to an identified central storage area approved by IS Department.

VI. Access to backup media shall be restricted on a 'need to know, need to do' basis.

VII. All backup media shall be identified, labeled, and logged.

VIII. The backup media especially magnetic media like DLTs and DATs shall be periodically tested, as per the testing frequency defined, to ensure the ability to restore backed-up data on a sampling basis.

IX. Periodic Backups shall be taken in two sets, one for on-site storage and one for offsite storage.

X. Off-site storage of backup shall be done in a facility that is physically in a separate area within the same city/town or in another city/town.

XI. The on-site backup media should be stored in a fireproof cabinet in an area outside the Data Center / Server Room, with access being restricted to employees with requisite approval.

XII. Offsite backup storage areas shall have baseline physical security, to ensure the safety and security of the backup media.

XIII. Backups of systems are tested at least monthly/quarterly to ensure they can be relied upon in an emergency and meet the needs of business continuity plans and business requirements.

8.8 Compliance

Introduction

The operation and management of information systems may be subject to contractual and regulatory requirements. Accordingly, appropriate policies should be defined and followed to ensure such compliance, on an ongoing basis. The objective for ensuring compliance is to avoid breaches of any regulatory or contractual requirements resulting in civil or criminal prosecution.

The policy consists of the following sections:
1 Use of authorized Software
2 Adherence of Privacy laws, Cyber laws guidelines

Policy Statements

8.8.1 Use of authorized Software

I. Only licensed and approved software shall be used at the Laurus IT network. Software licenses should be controlled and maintained by the IS Department to ensure protection against default or contractual and/or other limitations and liabilities.

II. Software license conditions, including those applying to limited use, should be observed at all times. Accordingly, no user shall make or use unauthorized copies of software or applications.

III. Users are permitted to use only approved software. Use of any other software, without authorization from IS Department, is strictly prohibited.

IV. Products licensed to run on a specific computer or at a particular site should not be copied onto another computer or another site without written authorization from the vendor, except for backup.

V. The IS Department shall conduct periodic reviews of software usage on Laurus PCs, Laptops, and Servers to ensure that no unauthorized software is being used. All software found in violation will be removed immediately.

VI. Users found contravening Laurus software compliance policy shall be subjected to disciplinary action.

8.8.2 Adherence of Privacy laws, Cyber laws guidelines

Laurus shall ensure adherence to applicable Data Privacy laws, Cyber laws, and related guidelines that are in force. It shall be the responsibility of the Corporate IT Head/ Location IT Manager, to identify applicable location-specific regulatory requirements relating to data privacy, electronic transactions and ensure adherence to the same.

8.9 Acceptable Usage Policy for Laurus employees

Purpose of the Acceptable Usage Policy

The following section outlines the policy for use of the computing systems and facilities located at or used by Laurus. The definition of the Laurus information systems and facilities shall include any computer, server, or network provided, supported, or used by the Laurus. The "user" of the system is the person using the Laurus computing systems to perform work in support of the Laurus program. The purpose of these guidelines is to ensure that all Laurus users (users, support personnel, and management) use the computing facilities in an effective, efficient, ethical and lawful manner.

8.9.1 Internet and Email Usage Policy

Following is a list of activities (not limited to as this list is not exhaustive), which are considered improper and hence prohibited:

I. Using any words, images, or references that could be viewed as obscene, derogatory or racially, sexually, ethnically, or otherwise offensive to colleagues, customers, suppliers, or competitors.

II. Creating, accessing, downloading, or transmitting messages or images that might be considered inappropriate in the workplace, including, but not limited to, messages or images that are lewd, obscene, or pornographic and messages or images that might be considered offensive or harassing due to their reference to race, sex, age, marital status, religion, national origin, physical or mental disability or another such protected status.

III. Accessing and/or trying to access IT systems for which the user does not have any access.

IV. Using e-mail, the Internet, or any other communication tool/media to harass, intimidate or annoy other persons including co-workers.

V. Spreading "chain mail" and other such frivolous communications.

VI. Users shall not use official mail ID for registering with websites (e.g. news sites)

VII. Accessing any software for online computer games.

VIII. Using the computer equipment and software to conduct personal business/transactions.

IX. Downloading, copying, or transmitting software and/or documents protected by copyright. Any employee with a question concerning a copyright issue should contact the IS Department.

X. Downloading any other software or materials (such as online publications) unless Laurus IS team has approved such download and has taken appropriate permissions and/or have subscribed for organization-wide use.
XI. Introducing computer viruses, worms, or Trojan horses.
XII. Using the system to solicit for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.
XIII. Using the IT systems to create any offensive or disruptive messages.
XIV. Using the IT systems to send or receive copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.
XV. Using a code, access a file, or retrieve any stored information unless authorized to do so.
XVI. Accessing message(s) to which an employee is not the intended recipient or sending the message(s) under someone else's name.

8.9.2 Desktop Usage Guideline

I. PCs / Laptops are provided to the users for business purposes and for enhancing their productivity and effectiveness in discharging their duties.
II. PCs should be protected by passwords and should be logged off when left unattended.
III. Unauthorized software should not be installed on the system from any source such as the Internet, or personal CDs, floppies, etc.,
IV. Caution should be exercised before opening e-mail messages from unknown or unidentified external sources. Such messages may contain computer viruses or malicious code, which can cause substantial damage to the Laurus computing system or even spread to other systems on the network.
V. Computing systems should be shut down at the end of the day's work for security reasons and also to save power.
VI. Users should refrain from using Laptops/Desktops for personal use including, but not limited to, storage of personal data such as family photos, songs, or videos.
VII. Users shall never disable Antivirus software, backup, or asset software.
VIII. If users suspect any infection to the system by virus or malicious contents, they must immediately shut down the computer, disconnect it from the network, and report the same to the IS Helpdesk.

8.9.3 Portable computing/Laptop Security

I. Portable computers and software are issued for business purposes only.
II. Users shall be responsible for the equipment and software until properly returned to Laurus.
III. Users shall allow the Administrator towards periodical system maintenance and back up
IV. The user shall be responsible for regularly backing up data at the Office. Loss of data due to theft or device malfunction shall be the user's responsibility.
V. Upon the request from Laurus at any time, for any reason, the user shall immediately return any portable computer equipment and all software to Laurus.

VI. The equipment and software are to be returned in good working order (unless it is being returned because of a malfunction) along with all documentation, software, and configurations.

8.9.4 Password Security

It shall be the responsibility of the individual users to secure their password, to avoid access to the Laurus Information system, by unauthorized users. Users shall

I. Always create a strong password as per the password policy
II. Never use easy to guess passwords
III. Never write password or store in clear text
IV. Never share or give the password to anyone.
V. Change the initial password immediately after the first login.
VI. Change Password at regular intervals.
VII. Never use the option of saving the password.
VIII. Be responsible for any transaction made through their IDs. Laurus may initiate necessary legal action if the damage is caused through the inappropriate use of such IDs.

8.9.5 General Usage guideline

I. The computer systems, messaging systems, and e-mails are the property of Laurus and are not the private property of any employee.
II. Laurus shall own the intellectual property rights on any work products, documents, and files arising from the work of employees, during and after his tenure of employment with Laurus. Hence all files of any nature residing in the PCs/Laptops are the property of Laurus.
III. The company's IT systems are to be used by the employees strictly for official business purposes. The company reserves the right to revoke the privilege of use of the computing systems temporarily or permanently in the interest of the organization.
IV. Laurus reserves the right to monitor and record all information relating to the usage of its computer systems. If it is found that the computing systems have been intentionally, or otherwise misused or attempted to have been misused, tampered with, or manipulated, the Organization shall initiate appropriate actions on those individuals.
V. No user shall engage in any activity that is explicitly prohibited and is considered an improper act within this policy.
VI. The IT Assets provided to individuals shall be for Business/Official Use, and would have to be returned to the IS Department during separation from the organization, or transfer or whenever a new asset is provided to the Users.
VII. All files should be secure at all times. When users leave the work area it is recommended to:
- Clear all classified information from desktop
- Use a screen Lock on PC or Laptop

- Lock up any other valuables the user may have
- Users shall lock up their paper files, log off the computer and make sure the laptop is secure either by locking it in a drawer or taking it with them when leaving for the night.

Any non-compliance with these requirements shall constitute a security violation and shall be reported to the management of Laurus and shall result in short-term or permanent loss of access to Laurus information systems followed by suitable disciplinary action.

8.10 Data Center Access

Introduction

Data Center access to the restricted and allowed to only authorized users. The Data Center should have access control.

Policy Statement

8.10.1 Access to the data center to the employees/members of the Management Team, IS, E & M, HR and Security Department.

8.10.2 Access to the Data Center shall be provided, based on the need and approval of the Departmental HOD and IT Head.

8.10.3 A "Annex 05 - List of Authorized Users to Data Center Door Access Control" shall be maintained.

8.10.4 A register shall be maintained to record the external service vendor visited "Data Center - Physical Access Register". Entry to the Data Center should be accompanied by the authorized IS Team member.

8.10.5 Data Center Access reviewed once in a Calendar year "Annex 06 - Data Center Access Log Review".

8.11 Data Transmission Procedure

Formal agreements that include non-disclosure and confidentially clauses must be in place for data sharing prior to the data transfer and no personal or confidential information is to be transferred unencrypted.

Information that is transferred should be checked for virus/malware before being sent or before being opened when received.

a) Preferred Transfer Method

The preferred transfer method is through a secured file sharing portal(Amazon Docs/onprime owncloud) or Email.

8.12 Patch Management

Operating system/application patches are updated frequently to protect from known vulnerabilities, including all desktops, and laptops owned and managed by Laurus.

Desktops and laptops that are in the company's network must be configured to get updates from the centralized patch management system. Patching is done fortnightly through the centralized patch management system.

Note: GMP systems shall be updated as per the supplier/vendor. These systems are not included in centralized patch management systems.

Monitoring
IT Team is required to compile and maintain reporting metrics that summarize the outcome of each patching cycle.

9 Business Continuity and Disaster Recovery

In recent years, added emphasis has been placed on the continuation of business functions in the face of potential disasters. Such disruptive acts may be natural disasters such as earthquakes, severe storms, flooding, etc., or deliberately caused by man (bombings, riots, and theft) or technical glitches like virus attacks, server crashes, etc. Whenever they occur, they could lead to significant disruption of business, if recovery measures are not planned. The objective of this policy is to provide guidelines to facilitate the recovery of business operations to reduce the overall impact of such an event, while at the same time resuming the critical business functions within a predetermined period. But, a separate Business Continuity Plan has to be prepared to cater to the operational aspect of Crisis Planning. The Business Continuity Planning aspects discussed in this policy consider the availability of the IT infrastructure, including facilities and personnel for respective locations.

10 Third-Party and Outsourcing Services Policy

Introduction
This policy is aimed at providing a framework and guidelines in the identification and management of Third Party and Outsourcing Services employed by the IS Department. This shall include (but not limited to) outsourcing of IT services, annual maintenance contract (AMC), IT Audit engagements, outsourced software development, and implementation, etc.

Policy Statement

10.1 **Vendor Evaluation and Selection**

I. Any Third Party and Outsourcing Services Contract shall be awarded after completion of the Vendor Evaluation and Selection process.

II. Security requirements shall be considered while finalizing any vendors and if required the vendor shall be audited for their security practices.

III. The formal Contract document shall be prepared and signed by both parties after the generation of the Purchase Order (PO) by SCM.

IV. The Approval for granting the Project to a certain Third Party and Outsourcing Services provider shall be as per the Delegation of Authority in the Financial Policy.

10.2 **Contract**

I. A formal contract shall be signed with Third Party and Outsourcing service provider before the commencement of any service. The contract can be Time based (for a fixed period) or Project/Deliverable based.

II. A Third Party Manager shall be identified, who would coordinate with the Third Party and Outsourcing service provider. The Responsibility of ensuring the signoff of Contract, SLA, etc by Laurus and the Third Party and Outsourcing service provider shall rest with the Third Party Manager.

III. The formal contact shall list down the Scope of Work, Roles and Responsibilities, Security Requirements, Escalation mechanism, availability of services to be maintained in the event of a disaster, etc.

IV. Applicable Statutory regulations shall be documented and compiled as applicable to the place of location & nature of services provided and added as part of the Contract.

V. The formal contract must be reviewed and approved by the Legal Department and the Third-party manager. For outsourcing of major IT services, approval of the Corporate IT Head/Location IT Manager shall also be obtained.

VI. Laurus shall have the right to audit the contractual responsibilities of the Third Party and Outsourcing Services provider at any given point of time during the period of the contract.

VII. The Third Party and Outsourcing Services provider must take explicit permission of the Third-party Manager to involve any subcontractors for the fulfillment of the contractual responsibility.

VIII. Laurus shall reserve the right to any intellectual property arising from collaborative work with the Third Party and Outsourcing Services provider like the development of software etc.

10.3 **Contract Expiry**

I. Contract Closure details must be documented on expiry of the Contract. A closure meeting must be conducted with all relevant stakeholders.

II. The Corporate IT Head/Location IT Manager shall review the Contract Closure details.

III. The SCM department shall be communicated on the expiry of the Contract.

11 Vulnerability Management

I. Vulnerability Assessment

I. Internal assets:

Vulnerability assessment will be conducted half yearly by the external vendor for all internal servers including end-user systems, network devices, and Printers.

Mitigate the identified vulnerabilities in respective systems, except application systems and servers. We will harden these systems by blocking the ports and external traffic.

II. External Assets:

Externally hosted servers will scan regularly by 3rd party tool and mitigate the critical vulnerabilities based on application compatibility.

II. Penetration Testing

PT will be conducted half yearly for externally hosted servers.

Both internal and external activities shall be performed as separate engagements.

12 IT Audit Policy

Introduction

The scope of this policy is to establish a mechanism for facilitating Information Systems Audit at Laurus, periodically, to ensure the following: –

- Safeguarding of Information System Assets/Resources
- Maintenance of Data Integrity
- Compliance with policies and procedures

Defining the exact Audit process, methodologies and the review areas is not in the purview of this document, and can only be finalized by the IS Department after consultation with the Senior Management and the Audit(s).

Policy Statement

I. An external or independent internal authority shall conduct an IT Audit as may be determined on an annual basis or as and when the Corporate IT Head/ Location IT Manager perceives any such need.

II. Information Systems Security Audit shall be budgeted as a separate line item in the overall IT Budget.

III. The Corporate IT Head/ Location IT Manager or the IT Steering Committee shall decide on the mode of audit (external or independent internal authority)

IV. If the Audit is to be conducted by external agencies, then Auditor Selection, Contract, and all other processes shall apply as per the 'Third Party and Outsourcing Services Policy'.

V. If the Audit is to be conducted by internal authority, then the Auditor(s) shall be independent of the IT Function.

VI. The various types of Information Systems Security Audit shall include the following:
   a. IS Strategy & Policy
   b. IT Security Policy
   c. Application Systems
   d. Vulnerability Analysis and Penetrative Testing of Laurus Networks
   e. Technology & Infrastructure Audit
   f. Business Continuity Planning including Demonstrated Recovery
   g. General Computer Controls Environment

VII. The Corporate IT Head/ Location IT Manager or designate shall be responsible for Coordinating with the Auditor(s) for the Audit.

VIII. System audit tools can be used for Audit. Any System Audit Tool that is used shall be adequately protected to prevent any misuse.

IX. Audit of any operational systems shall be conducted in such a way as not to disrupt normal operations. Any potential disruption expected as a result of the audit shall be communicated to all relevant stakeholders.

X. The IT Audit results and findings should be documented and submitted to the Corporate IT Head/ Location IT Manager. Corporate IT Head/ Location IT Manager, in turn, shall present the audit findings to the IT Steering Committee.

XI. The Corporate IT Head/ Location IT Manager shall be responsible for ensuring the implementation of corrective actions for gaps identified by the Audit. A roadmap defining the timeframe for closing all gaps must be prepared and presented to the IT Steering Committee within a month of the submission of the Audit Report.

XII. The IT Steering Committee shall review the compliance status of agreed remedial action to close the gaps identified in the Audit.

XIII. All Audit Reports shall be stored for retention requirement

13 Exceptions to the Policy

Introduction

This document defines the policy that will be followed by Laurus IT personnel to identify any exceptions to policies that must occur to successfully complete the business transaction. The "exceptions to policy" will take effect only upon obtaining the prior approval of the concerned authority.

Policy Statement

There may be instances where there is a justifiable business need to perform actions that conflict with Laurus-approved IT Policies and Procedures. Laurus IT Leadership recognizes that policies cannot be created and enforced in all circumstances at all times. To provide flexibility in these instances, there is an "Exception to Policy" standard that details the actions that are required to obtain a waiver from compliance to a specific policy.

I. Requests for exceptions to policies must have a justifiable business case documented and must have the necessary approvals to be considered valid. Exceptions must be approved and signed by the Corporate IT Head/ Location IT Manager. Once approved, exceptions to policy will be valid for a pre-decided period after which it must be re-evaluated and re-approved.
II. If policy exceptions are likely to circumvent existing internal controls then "Mitigating Controls" or "Compensating Controls" must be implemented and followed. The Corporate IT Head/ Location IT Manager shall be convinced and approve the arrangements to put in place the mitigating or compensating controls.
III. Exceptions to Policy approvals shall be reported to the IT Steering Committee, for information.

14 Oversight and Review

Laurus Labs will periodically review and monitor the IT Policy as necessary and appropriate. This Policy is subject to review on a needed basis, but at least once in three (3) years ± 3 months.

15 Annexures

The following are annexure to the IT Policy:

- Annex 01 IT – Change Request Form
- Annex 02 Active User List Review Log
- Annex 03 List of User Access Granted By Exception
- Annex 04 User Access Request Form (Create / Remove)
- Annex 05 List of Authorized Users to Data Center Door Access Control
- Annex 06 Data Center Access Log Review

16 Abbreviations

IT	INFORMATION TECHNOLOGY
IS	INFORMATION SYSTEMS
QA	QUALITY ASSURANCE
FTP	FILE TRANSFER PROTOCOL
CPU	CENTRAL PROCESSING UNIT
CD	COMPACT DISC
DVD	DIGITAL VIDEO DISC
SCM	SUPPLY CHAIN MANAGEMENT
PC	PERSONAL COMPUTER
LAN	LOACL AREA NETWORK
OS	OPERATING SYSTEM
MS	MICROSOFT
SOP	STANDARD OPERATING PROCEDURE
IP	INTERNET PROTOCOL
VPN	VIRTUAL PRIVATE NETWORK
HR	HUMAN RESOURCES
DNS	DOMAIN NAME SERVER
OEM	ORIGINAL EQUIPMENT MANUFACTURER
ACL	ACCESS CONTROL LIST
IDS	INTRUSION DETECTION SYSTEM
DMZ	DEMILITARIZED ZONE
UPS	UNINTERRUPTED POWER SUPPLY
SDLC	SOFTWARE DEVELOPMENT LIFE CYCLE
SLA	SERVICE LEVEL AGREEMENT
NDA	NON DISCLOSURE AGREEMENT
WAN	WIDE AREA NETWORK

17 Revision Log

Revision No.	Reason for revision	Effective Date
0.0	First issue	16.05.2016
1.0	Modification of access revocation of separated employee defined and minor modification and cosmetic error correction	27.09.2019
2.0	Modification of access revocation more specifically and also introduced periodic user review policy and annexures to meet the audit response.	02.06.2021
3.0	Minor modification and cosmetic error correction and also added the Vulnerability Management.	Effective from date of approval of this document

18 Approval:

Prepared By

Signature:	Date: 25/03/2024
Print Name: KONERU RAJESH	Title and Department: DGM, IS

Reviewed By

Signature:	Date: 25/03/2024
Print Name: VIVEK DIGUMARTI	Title and Department: VP-1, IS & SAP

Approved By

Signature:	Date: 25-3-24
Print Name: RAVI KUMAR VV	Title and Department: ED