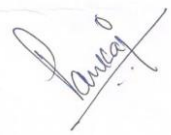
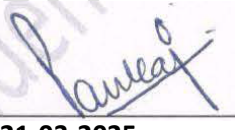
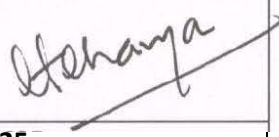


Information Technology and Information Security Policy


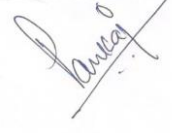
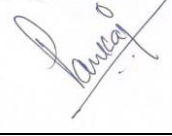
Document No.	IT/POLICY/003
Applicability	INOX INDIA Limited, All Subsidiaries, All Affiliates
	All Manufacturing Units under INOXINDIA Limited
Depots	All Warehouses under INOXINDIA Limited

Version	Revision Date	Revision Description	Author / Process Owner	Sign-Off
1.0	18 th August 2024	First Version Created	CIO	

	<u>Created by</u>	<u>Approved By</u>
	<u>Pankaj Shrivastava</u>	<u>Deeapk V Acharya</u>
	<u>CIO – GM IT</u>	<u>CEO</u>
		
	<u>21-03-2025</u>	<u>21-03-2025</u>

DOCUMENT CONTROL

Author	Chief Information Officer
File Name	INOXINDIA Limited IT Policy Document V.2.0
Created	18 th August 2024
Last Edited	15-03-2025

Version	Revision Date	Revision Description	Author / Process Owner	Sign-Off
1.0	18 th August 2024	First Version Created	CIO	
2.0	23 rd December 2024	Added policies 1. Antivirus management 2. Patch Management	CIO	
3.0	21 st March 2025	Revised all policies as per ISO27001 Standard	CIO	

Targeted Readership: All Stakeholders

TABLE OF CONTENTS

1. INTRODUCTION.....	4
2. ABOUT THE INFORMATION TECHNOLOGY POLICY	4
3. IT FUNCTION	5
4. GOVERNING MECHANISMS.....	5
5. ROLES AND RESPONSIBILITIES	8
6. EQUIPMENT MANAGEMENT POLICY	13
7. PERSONAL COMPUTER (PC) STANDARDS	21
8. INTERNET USAGE POLICY	26
9. INFORMATION SECURITY POLICY	29
10. COMPUTING ENVIRONMENT MANAGEMENT	33
11. NETWORK SECURITY	35
12. WEB SITE SECURITY	40
13. VIRUS MANAGEMENT POLICY	42
14. BACKUP MANAGEMENT	43
15. USER RESPONSIBILITIES / ACCOUNTABILITY	47
16. EMAIL & CHAT POLICY	48
17. SOFTWARE ANALYSIS, DESIGN, DEVELOPMENT IMPLEMENTATION AND USAGE POLICY.....	51
18. ACQUISITION & IMPLEMENTATION OF PACKAGED SOFTWARE POLICY	55
19. INCIDENT MANAGEMENT POLICY.....	60
20. COMPLIANCE	61
21. ADHERENCE TO CONFIDENTIALITY AND PRIVACY LAWS, CYBER LAWS GUIDELINES.....	62
22. ACCEPTABLE USAGE POLICY	63
23. CAPACITY PLANNING AND PERFORMANCE MANAGEMENT POLICY.....	66
24. BUSINESS CONTINUITY PLANNING POLICY.....	67
25. THIRD PARTY AND OUTSOURCING SERVICES POLICY	69
26. IT AUDIT POLICY	73
27. CHANGE MANAGEMENT	74
28. ISSUE MANAGEMENT POLICY.....	81
29. CONFIGURATION MANAGEMENT POLICY	82
30. EXCEPTION	85
31. ABBREVIATIONS	92

INTRODUCTION

- 1.1 "INOXCVA Limited is increasingly relying on Information Technology (IT) to conduct its business operations. With an advanced communication network connecting multiple locations, the IT function has been identified as a critical enabler and catalyst for the business.
- 1.2 However, this growing dependence on technology also introduces significant IT compliance and security risks. Therefore, INOXCVA Limited recognizes the need for a comprehensive IT Policy to establish a framework for managing the global IT function. This policy aims to promote consistency, transparency, and effective governance within the IT function.
- 1.3 This document provides general guidance to all stakeholders and applies to INOXCVA Limited and its entities, including subsidiaries, affiliates, vendors, clients, and third parties utilizing the IT function of INOXCVA Limited. As such, this document is relevant to the employees, vendors, and business partners of INOXCVA Limited (Stakeholders).
- 1.4 Unauthorized duplication and distribution of this document are strictly prohibited. It must not be copied in whole or in part by any means, and no modifications are allowed without formal written approval from the Change Control Board. Every individual in possession of this document is responsible for maintaining its confidentiality

ABOUT THE INFORMATION TECHNOLOGY POLICY

- 2.1 INOXCVA Limited provides and maintains technological products, services and facilities like
Industrial Gas: This division manufactures, supplies and installs cryogenic tanks and systems for storage, transportation and distribution of industrial gases like such as green hydrogen, oxygen, nitrogen, argon, carbon dioxide (CO₂), hydrogen and provides after-sales services.

LNG: This division manufactures, supplies and installs standard and engineered equipment for LNG storage, distribution and transportation as well as small-scale LNG infrastructure solutions suitable for industrial, marine and automotive applications; and

Cryo Scientific: This division provides equipment for technology intensive applications and turnkey solutions for scientific and industrial research involving cryogenic. This Information Technology Policy (IT Policy) is to ensure legal, ethical, compliant use and assure health, safety and security of data and Asset/s. It also provides guidelines for issues like purchase, compliance and IT support.

IT FUNCTION

3.1 *Key Objectives:*

- 3.1.1 Enterprise Application Infrastructure and Systems Operations: To establish, maintain, and enhance enterprise information systems and infrastructure services that support business requirements.
- 3.1.2 Operational Excellence: To implement best practices in operations to ensure superior availability, reliability, and performance of information systems services, fostering communication, mutual accountability, and cooperative planning with business units.
- 3.1.3 Enterprise Application Security and Disaster Recovery: To ensure reliable, secure, confidential, and continuous enterprise operations through the development and implementation of policies, procedures, monitoring, risk assessment, planning, mitigation, recovery planning, and periodic testing.
- 3.1.4 Return on Investment: To collaborate with all business units to optimize the benefits of enterprise IT investments, while meeting business requirements and managing the organization's total costs.
- 3.1.5 Emerging Technologies: To identify and evaluate emerging technologies to determine their potential benefit to INOXCVA

3.2 *Services:*

- 3.2.1 Planning - Advice and guide on development of IT strategies.
- 3.2.2 Operational - Continuous or regular delivery of services such as access to applications and data, operating computer systems and maintaining networks, and associated customer support facilities
- 3.2.3 Project - Such as applications software development

GOVERNING MECHANISMS

4.1 Change management Change Management Policy

4. Roles and Responsibilities

4.1 Executive Management Approves this policy and provides necessary resources for implementation Resolves escalated issues regarding high-impact changes

4.2 Change Advisory Board (CAB)

Reviews, evaluates, and approves/rejects standard and significant changes Consists of representatives from IT, Information Security, Operations, and key business units Meets regularly to review change requests and post-implementation reviews Ensures changes align with business goals and security requirements

4.3 Emergency Change Advisory Board (ECAB):

Smaller subset of the CAB that can convene rapidly Reviews and approves emergency changes

Documents emergency changes for later review by the full CAB

4.4 Change Manager

Administers the change management process Coordinates CAB meetings and documentation

Maintains the change schedule and tracks all changes Provides reports on change management effectiveness Ensures proper communication of change activities

4.5 Information Security Manager

Ensures changes comply with security policies and standards Conducts or reviews security impact assessments for proposed changes Approves changes that affect security controls Monitors implemented changes for security implications

4.6 Change Initiator

Submits properly documented change requests Provides justification and complete information about proposed changes Conducts testing and verification of changes when required Prepares implementation and rollback plans

4.7 IT Operations Staff

Implements approved changes following established procedures Documents the results of implemented changes Executes rollback procedures when necessary

4.8 Policy Requirements

4.8.1 Change Request and Authorization All changes must be formally requested using the approved change request form Changes must be categorized by type, scope, and risk level Authorization requirements escalate based on potential impact:

Low impact: IT Manager approval

Medium impact: CAB approval

High impact: CAB and Executive Management approval

Emergency changes: ECAB approval with post-implementation review

4.8.2 Change Assessment

All change requests must include: Clear description and justification for the change Impact assessment (systems, users, processes affected) Risk assessment and mitigation measures Resource requirements and cost estimates Implementation timeline Testing plan Rollback procedure Security impact assessment must be conducted for changes affecting:

- Authentication systems
- Access control mechanisms
- Network infrastructure

- Encryption implementations
- System configurations related to security
- Introduction of new technologies or systems

4.8.3 Change Planning and Scheduling

Changes must be scheduled to minimize disruption to manufacturing operations Production-impacting changes must be scheduled during approved maintenance windows Changes must be communicated to affected stakeholders with appropriate lead time Change scheduling must consider:

- Manufacturing production schedules
- Critical business periods
- Other planned changes (prevent conflicts)
- Resource availability
- Regulatory compliance requirements

4.8.4 Testing Requirements

All changes must be tested in a non-production environment before implementation Test plans must verify both functionality and security requirements Testing results must be documented and reviewed before change approval User acceptance testing must be performed for changes affecting business applications For manufacturing systems, simulation testing should be performed when possible

4.8.5 Implementation

Changes must be implemented according to the approved implementation plan Implementation must adhere to predetermined change windows Changes must be implemented by authorized personnel only Implementation activities must be documented in detail Critical manufacturing systems require dual-control principles during implementation

4.8.6 Verification and Post-Implementation Review

All changes must be verified after implementation to ensure:

- The change achieved its intended purpose
- No unintended consequences occurred
- Security controls remain effective

Documentation is updated to reflect the change

Post-implementation reviews must be conducted within two weeks of significant changes Lessons learned must be documented and incorporated into future change processes

4.8.7 Emergency Changes

Emergency changes may bypass standard approval processes only when: Immediate action is required to prevent or address a significant incident Delay would cause substantial harm to the organization The change is required to comply with legal or regulatory mandates Emergency changes must:

- Be documented to the extent possible before implementation
- Be authorized by the ECAB or designated authority
- Undergo comprehensive documentation and review after implementation
- Be reported to the full CAB at the next scheduled meeting

4.8.8 Change Documentation

A comprehensive change log must be maintained containing:

- Change request details
- Approval/rejection information
- Implementation details
- Verification results
- Post-implementation review findings
- Documentation affected by changes must be updated within 5 working days
- System configuration documentation must be updated to reflect all changes

4.8.9 Segregation of Duties

Change management roles must be segregated to prevent unauthorized or unreviewed changes. Personnel who develop changes should not approve or implement those same changes without oversight. Change verification must be performed by someone other than the implementer. For critical manufacturing systems, multiple approvals are required for all changes.

4.8.10 Monitoring and Audit

All changes must be monitored for effectiveness and security compliance. System logs must capture activities related to the change implementation. Periodic audits of the change management process must be conducted. Change records must be retained for at least two years or as required by applicable regulations.

ROLES AND RESPONSIBILITIES

5.1 *Chief Information Officer (CIO):*

5.1.1 Monitor Global IT Strategy and Plan.

5.1.2 Capital Planning, Investment management.

5.1.3 Oversee implementation of approved IT Policies including IT Security.

5.1.4 Oversee all IT outsourcing initiatives.

5.1.5 Workforce planning and foster ongoing development of the IT skill base including succession planning.

5.1.6 To be responsible for overseeing the IT operations.

5.3 *Manager – Application Development & Support:*

- 5.3.1 To continuously review and identify scope of improvement.
- 5.3.2 To implement, monitor and ensure compliance with the IT policies, procedures and guidelines.
- 5.3.3 To advice business team on ability and feasibility of automating business process requirements using application solution.
- 5.3.4 To identify and lead initiatives promoting the “up-take” of application systems, among the user community through necessary upgrade, enhancements, training and change management.
- 5.3.5 To set the KPA’s for subordinates & monitor their performance.
- 5.3.6 To assist in developing the technical / managerial skills of subordinates through mentorship, & formal training.
- 5.3.7 To review the performance of the function relating to application systems against established performance levels.
- 5.3.8 To approve and validate any new Access to be provided to the System.
- 5.3.9 To work as a Change Manager, Configuration Manager and Third Party Manager for application systems related activities.
- 5.3.10 To work as Backup Crisis Management Lead.
- 5.3.11 To ensure compliance to timely application of patches to application systems including upgrades and to ensure through monitoring and review the design and operating effectiveness of Backup.
- 5.3.12 To monitor and review all application systems security requirements, on a periodic basis.
- 5.3.13 To liaison with application systems vendor(s) on an ongoing basis and track vendor product and organization developments that may have an impact on application systems.
- 5.3.14 To participate in the Business Continuity Planning, testing and maintenance process relating to application systems as one of the team members along with the business and other team members.
- 5.3.15 To review, escalate and manage incidents relating to application systems.

5.4 *Manager –Infrastructure:*

- 5.4.1 To coordinate and assist Country IT managers in network and infrastructure related issues.
- 5.4.2 To understand market trends in technology to leverage.
- 5.4.3 To assess the impact of change in technology.
- 5.4.4 To lead and manage a team responsible for day-to-day operations in India related to Server and Network Infrastructure.

- 5.4.5 To lead and manage a team responsible for the IT asset management across the organization, for Indian operations.
- 5.4.6 To co-ordinate with other stake holders regarding asset management.
- 5.4.7 To work as a Change Manager, Configuration Manager and Third Party Manager for Network and Infrastructure related activities.
- 5.4.8 To work as Crisis Management Lead.
- 5.4.9 Implementation, monitoring and compliance of the IT policies, procedures and guidelines.
- 5.4.10 To be responsible for Incident Management.
- 5.4.11 To be responsible for Backup.
- 5.4.12 To set the KPA's for subordinates & monitor their performance and to assist in developing the technical / managerial skills of subordinates through mentorship, & formal training.
- 5.4.13 To review the performance of the function against established performance levels.
- 5.4.14 To approve and validate any new access to be provided to the system.
- 5.4.15 To monitor and review all network and server security requirements, on a periodic basis.

5.5 *System Administrator:*

- 5.5.1 To manage servers (Application/Database/File/FTP/E-Mail/Proxy etc) II.
- 5.5.2 To install and maintain servers.
- 5.5.3 User management, creation/revocation/change of approved user IDs, archiving access request/approval trails, helping network and systems head for access list validation/audit, regular monitoring of access logs etc.
- 5.5.4 Backup management taking and archiving backup of all systems, backup testing and validation at regular intervals. Restoration of systems form backup in case of failure or data loss.
- 5.5.5 System performance and capacity monitoring, monitoring of system resources (disk/memory/CPU) utilization and preparation of reports, escalation of event in case resource utilization goes beyond defined threshold.
- 5.5.6 To act as a configuration administrator.

5.6 *Network Administrator:*

- 5.6.1 To manage all network equipment's (Routers/Switches/Firewall/IDS etc)
- 5.6.2 To install routers, switches and other network related equipments.
- 5.6.3 To upgrade OS and other software for network infrastructure, taking back up of configuration of network equipments and storing it on periodic basis.
- 5.6.4 To manage network connectivity between various locations.

- 5.6.5 To maintain and monitor Antivirus and update the software patches as and when required for any components.
- 5.6.6 To act as “Asset Manager” and maintain and update asset inventory.
- 5.6.7 To manage content filtering and updates for the same.
- 5.6.8 To implement and manage configuration management process, comply with remarks of configuration audits, ensure that the older versions are kept for reference.
- 5.6.9 To take backup and archive backup of all network configuration, IOS image etc., test and validate backup at regular intervals, restore systems from backup in case of device failure or data loss.
- 5.6.10 To ensure network performance and capacity monitoring, monitor network resources (Network Bandwidth, Hardware CPU/Memory) utilization and preparation of reports, escalate event in case resource utilization goes beyond defined threshold.
- 5.6.11 Shall act as a configuration administrator.

5.7 *Security Administrator:*

- 5.7.1 To adhere to all security best practices.
- 5.7.2 To monitor all security logs and to escalate, investigate and resolve any anomaly noticed.
- 5.7.3 To implement and ensure security configurations of Network devices/servers/applications are as per the vendor provided best practices.
- 5.7.4 To manage and monitor firewall policy, logs and generate reports from that on periodic basis.
- 5.7.5 To maintain and monitor Intrusion Detection System rules and logs/alerts.
- 5.7.6 To monitor any new vulnerability and threats published by vendors and inform the operations team about countermeasure.
- 5.7.7 To implement all audit recommendations.
- 5.7.8 Shall act as a configuration administrator.

5.8 *Business Analyst (non ENTERPRISE APPLICATION)*

- 5.8.1 To understand and capture the user requirement.
- 5.8.2 To coordinate between the business users and the technical team.
- 5.8.3 To prepare the functional specifications or the System Requirement Specification (SRS) for the project.
- 5.8.4 To create the user acceptance criteria for application software.
- 5.8.5 To review and approve test plans/cases.
- 5.8.6 To conduct testing.
- 5.8.7 To assist the project manager in the project delivery.

5.9 *Business Analyst (ENTERPRISE APPLICATION):*

- 5.9.1 To understand and capture the user requirement.
- 5.9.2 To coordinate between the business users and the technical team III. To create the user acceptance criteria and test plans.
- 5.9.3 To make configuration changes.
- 5.9.4 To conduct testing.
- 5.9.5 To assist in the project delivery.

5.10 *System Analyst*

- 5.10.1 To understand the Functional Specifications, and to create Technical Specification or System Design document and ensure review and approval of the same.
- 5.10.2 To make required changes to technical specification and review test plans.
- 5.10.3 To work on code review, whenever required.
- 5.10.4 To work on system/integration test of the applications.

5.11 *IT Programmer:*

- 5.11.1 To understand the functional and technical specifications.
- 5.11.2 To write code, or make changes in the application code.
- 5.11.3 To prepare test plans and run code self-check.
- 5.11.4 To prepare deployment and release plan

5.12 *Application/ ENTERPRISE APPLICATION Admin:*

- 5.12.1 To ensure, review and monitor user management.
- 5.12.2 To be the single point of contact for all application/ENTERPRISE APPLICATION administration related issues and work on, and resolve all related issues and problems.
- 5.12.3 To ensure version control and maintenance of the configurable items.
- 5.12.4 To have write/update access on production instance.
- 5.12.5 To move applications/configurations into the production environment with the help of approved deployment or release plan.
- 5.12.6 To take regular backup as per the backup.

5.13 *Database Admin:*

- 5.13.1 To coordinate the installation, or upgrade of database.

- 5.13.2 To work on creation, maintenance and monitoring of database entities and to maintain all database and related applications.
- 5.13.3 To be the single point of contact for all database related issues and for resolving all database related issues and problems.
- 5.13.4 To have write/update access on production instance.
- 5.13.5 To ensure, review and monitor user management.
- 5.13.6 To review and monitor the database capacity and performance.
- 5.13.7 To ensure version control and maintenance of the configurable items.
- 5.13.8 To move database applications into the production environment with the help of approved deployment or release Plan.
- 5.13.9 To take regular backup of the database.

EQUIPMENT MANAGEMENT POLICY

6.1 *Objective:*

- 6.1.1 The objective of Equipment Management Policy (EMP) is to capture the maximum outcome or performance required from an Asset in order to deliver (or support) achievement of organisational objectives that is to be derived from the Asset by providing guidance for procurement, usage, maintenance etc., to the Stakeholders. Additionally this Policy informs Stakeholders about organizational and project-level inventory management, rules for allocating & transferring equipment to employees, departments or projects and best practices for all equipment usage and maintenance.

6.2 *Equipment:*

- 6.2.1 The following equipment's are purchased by the organization for official use of the Stakeholders. The list is inclusive and not exhaustive.
 - Computing Devices (Desktop, Laptop, Tablet)
 - Computer Peripherals (Printer, Scanner, Photocopier, Fax Machine, Keyboard, Mouse, Web Camera, Speaker, Modem etc.)
 - Networking Equipment & Supplies (Servers, Router, Switch, Wiring, etc.)
 - Cell phones
 - Biometric Devices
 - Accessories

6.3 *Equipment Purchase and Acquisition:*

- 6.3.1 The Procurement Department procedures & guidelines need to be followed to purchase Equipment/s.

- 6.3.2 Administration Department shall initiate purchase of any Equipment approved by the relevant business head as per business needs within the budgetary approvals of the relevant financial year.
- 6.3.3 The request shall be escalated to the relevant IT Procurement Desk (ITPD) created in this regard who will evaluate best and most cost-effective Equipment for purchase for a particular dept./project/purpose based on the requirement. ITPD will also make sure all standards pertaining to Equipment/s in the IT Policy are enforced during such purchases.
- 6.3.4 In case of recurring purchases of a similar Equipment, ITPD shall recommend procurement of standardized product created and amended in this regard. However, in case of non-standardised Equipment's the requirement shall be routed through the Steering Committee.
- 6.3.5 Financial approval for procurement of Equipment within the budgetary approvals shall be as provided in the Financial delegation of powers, prescribed by the Finance department, from time to time.
- 6.3.6 Equipment Purchase and Acquisition contract shall be awarded in compliance with Vendor Evaluation and Selection Policy of the Purchase Department.

6.4 *Equipment Ownership:*

- 6.4.1 The ownership of the Equipment is vested with the IT Department while the custodianship of the Equipment allotted to individual Stakeholder shall be with such Stakeholder.
- 6.4.2 In case of all other Equipment's installed in the office premises Administration Department shall be the custodian.
- 6.4.3 The Custodian shall be responsible in the event of damage, misplacement or theft of any Equipment.
- 6.4.4 The Equipment shall be insured as per insurance requirements. .

6.5 *Equipment Upgrade:*

- 6.5.1 Equipments shall not be upgraded within 4 years of the procurement, unless approved by the Steering Committee based on urgent business and applications need requisitioned by the business process owner.
- 6.5.2 The Equipment Database shall be updated with the upgrade details, by the IT Department.

6.6 *Compliance:*

- 6.6.1 All Stakeholders shall comply with the IT Policy while purchasing, using and maintaining any Equipment purchased or provided by the organization.
- 6.6.2 Any Stakeholders who notices any deviation in the procurement usage etc; must inform his/her Reporting Manager(s) immediately with a copy to IT contact-desk at sysadmin.in@inoxcva.com or Supportbrd.in@inoxcva.com
- 6.6.3 Inappropriate use of Equipment/s by a Stakeholders will be subject to disciplinary action.

6.7 *Stakeholders Training:*

- 6.7.1 Basic IT training and guidance is provided to all new Stakeholders about using and maintaining Equipment/s, accessing the organization network.
- 6.7.2 Stakeholders can further request for an IT training on a regular or requirement basis.

6.8 *IT Support:*

- 6.8.1 Stakeholders may need support for hardware/software installations or may face technological issues. Support on such issues shall be provided via Ticket System or IT help desk @ sysadmin.in@inoxcva.com only. Any IT support informed or assigned via emails sent on employee email IDs, chats or any other media except the Ticket System or the IT Helpdesk Email ID will not be entertained.
- 6.8.2 The Stakeholders are expected to provide details of their issue or help required in the Ticket raised or Email sent.
- 6.8.3 For major issues like damage, PC replacement, non-working equipment, installation of application software and more, approval from Reporting Manager & HOD is mandatory.
- 6.8.4 After raising a ticket in the Ticket System or sending an Email, employees should expect a reply from the IT Department within 1 working day.
- 6.8.5 The IT Department may ask the employee to deposit the problematic equipment to the IT Department for checking and will inform the timeline for repair/maintenance/troubleshooting/installations or the required work. If the repair time is more than four hours, IT Department. Will provide a replacement machine with the Help of Admin Department for smooth working of the Organisation.
- 6.8.6 If there is no response in 3 working days, a complaint can be raised through an email to the Stakeholder's Reporting Manager and IT Department's personnel designated for this purpose (SPOC).

6.9 *Inventory Management:*

- 6.9.1 IT Department is responsible for maintaining an accurate inventory of all Equipment's purchased by the organization.
- 6.9.2 The Administration Department in HO and IT department in Plants/MRC will maintain a small inventory of standard PCs, software and equipment required frequently to minimize delay in fulfilling critical orders and providing replacement for major repairs.
- 6.9.3 The following information is to be maintained for above mentioned Equipment's in an Inventory Sheet:
- Item
- a) Brand/ Company Name
 - b) Serial Number
 - c) Basic Configuration (e.g. HP Laptop, 500 GB HD, 8GB RAM etc.)
 - d) Physical Location
 - e) Date of Purchase
 - f) Purchase Cost
 - g) Department
 - h) Current Person In-Charge
- 6.9.4 Department wise information about all Equipment must also be maintained and regularly updated in Inventory Sheets by an assigned IT coordinator. When an Inventory Sheet is updated or modified, the previous version of the document should also be retained. The date of modification should be mentioned in the sheet.
- 6.9.5 All Equipment/s of the organization must be physically tagged with codes for easy identification.
- 6.9.6 Periodic inventory audits shall be carried out by the IT Department for validation and to ensure all that all Equipment's are up-to-date and in proper working condition as required for maximum efficiency and productivity.

6.10 Equipment Allocation, De-allocation:

6.10.1 Allocation of Assets by Administration/IT Department:

- 6.10.1.1 New employees shall be allocated a personal computer (desktop or laptop) for office work on the Day of Joining, as per work requirement.
- 6.10.1.2 If required, employees can request their Reporting Manager(s) for additional equipment or supplies like external keyboard, mouse etc.
- 6.10.1.3 Allocation of additional Equipment s to an employee is at the sole discretion of the Reporting Manager(s).

6.10.1.4 No employee is allowed to carry official Equipment electronic devices out of office without permission from Reporting Manager.

6.10.2 De-allocation of Equipment's:

6.10.2.1 The Equipment's must be returned back to the Administration Department by the Stakeholders leaving the organisation.

6.10.2.2 The Administration Department shall inspect the Equipment at the time of retrieval for damage. In case of damage identified by the Administration Department as due to negligence / improper use by such user, the HR & Administration department shall recover, from such employee, temporary hire, third party, an appropriate residual amount, for such damages, after considering warranty/insurance cover for such Equipment.

6.10.2.3 It is the HR department's responsibility to ensure all allocated organizational equipment & other assets have been received back from the Stakeholders who are leaving the organization before settling their dues.

6.10.2.4 The Inventory Sheet shall be mandatorily updated after receiving back all allocated equipment.

6.11 Transfer of Equipment's:

6.11.1 Transfer of Equipment's from one user to another user or from one location to another location or Business Unit shall be carried out with the approval of respective Business Head and Administration department.

6.11.2 Transfer of Equipment's such as Servers, Networking and Telecommunications, Security and Power Systems shall be carried out only upon prior approval of the Steering Committee.

6.11.3 The Asset database shall be updated in all cases of transfer by the Administration Department. Also, where necessary, IT Department shall update other documentation such as Network diagrams, Telecommunication diagrams etc.

6.12 Retrieval of Assets:

- 6.12.1 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, with the approval of Respective site specific Functional Head, Unit Head and respective units IT department.
- 6.12.2 The Asset database details shall be updated in all such cases.
- 6.12.3 The site specific IT Administration Department shall inspect the Asset at the time of retrieval for damage. In case of damage identified by the site specific IT Administration Department as due to negligence / improper use by such user, then HR & Administration 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.

6.13 Equipment Retirement and Disposal:

- 6.13.1 If necessary, Steering Committee shall retire the Equipment's based on the company's approved Asset Retirement timeframe prevalent at the time.
- 6.13.2 Steering Committee may decide to retire the Equipment's before the life period for some special reasons listed below;
- Technology obsolescence
 - Defective Hardware
 - Prohibitive cost of maintenance
 - Damaged or un-repairable condition
- 6.13.3 The retired Equipment's on retirement may be disposed by the Administration Department / commercial department to sold off to certified e waste agencies.
- 6.13.4 The Equipment's for disposal shall be cleansed of any specific licensed / proprietary software and data.
- 6.13.5 In case the Equipment's need to be destroyed, the IT Department with the help of EHS Department, shall ensure adherence to countries specific applicable environmental and safety guidelines impacting such disposal.
- 6.13.6 The retired GxP Assets on retirement should not be disposed as they may be required for future reference
- 6.13.7 The Asset Database shall be updated upon retirement and disposal of assets, by the Administration Department and list of such disposed Assets shall be provided to Finance Department.

6.14 Installation Qualification (IQ):

- 6.14.1 Corporate System and network administration team shall be responsible for ensuring the Installation qualification process for servers and other network devices, if applicable.
- 6.14.2 The installation qualification process shall;
 - Confirm that the System specifications meet the User Requirement Specification.
 - Conforms to the manufacturer's technical description and installation requirements.
 - Confirm that appropriate licenses and documents exist to enable the system to be operate and maintained in compliance, safely, effectively and consistently.
- 6.14.3 Ensure that all required system software and server support application software are provided.
- 6.14.4 Ensure that the backup software or devices required are properly installed for backup.
- 6.14.5 To ensure that the System is in a satisfactory condition for the Computer OQ to be started.
- 6.14.6 The Installation qualification test shall be recorded.
- 6.14.7 All installation qualification reports shall be submitted to the Steering Committee.
- 6.14.8 The installation qualification process shall not be applicable on Personal Computing device.

6.15 Operational Qualification (OQ):

- 6.15.1 If applicable, Corporate CSV-retention requirement Team shall under the guidance of Steering Committee, ensure operational qualification is being performed for IT system before going to production environment.
- 6.15.2 The Operation Qualification testing shall;
 - Verify the operational aspects of the Server that are deemed critical to its satisfactory performance.
 - Ensure that adequate security controls are in place as per the security best practices of the component.
 - Ensure that the system does what it is supposed to do.
 - Ensure that the system can produce the required level of performance, through stress/load testing.
 - Ensure that the system does have the required level of capacity.

6.15.3 The operational qualification testing team shall comprise of members from

- One of the member of Steering Committee
- System and network administration
- Application owner
- Security expert

6.15.4 The operational qualification test shall be recorded and all operational qualification reports shall be submitted to Steering Committee for review.

6.15.5 The operational qualification process shall not be applicable in certain exceptional cases like Personal Computing device.

6.16 Equipment Usage, Maintenance and Security:

6.16.1 It is the responsibility of all Stakeholders to ensure careful, compliant, safe and judicious use of the equipment & other assets allocated to and/or being used by them.

6.16.2 Proper guidelines or safety information must be obtained from designated staff in the IT Department before operating any equipment for the first time.

6.16.3 Report of any observed malfunction, error, fault or problem while operating any equipment owned by the organization or assigned to the Stakeholders must be immediately escalated to IT Helpdesk.

6.16.4 Any occurrence of improper or careless use, misuse, wastage of supplies or any such negligence/offense compromising the safety or health of the equipment and Stakeholders using them, will be subject to disciplinary action.

6.16.5 If the Stakeholder's assigned Asset is malfunctioning or underperforming and needs to be replaced or repaired, such Asset shall be submitted to the IT Department for checking, maintenance or repair after the approval of Reporting Manager. The IT Department staff person will give a time estimate for repair/maintenance and if the repair time is more than 4 hours will provide a suitable replacement.

6.16.6 The Reporting Manager can be informed about excessive delay or dissatisfaction about the repair or maintenance performed by the IT Department. The issue will then be resolved by the Reporting Manager in consultation with the SPOC.

6.17 Phone Usage Policy:

6.17.1 Landline phone systems are installed in the organization's offices to communicate internally with other employees and make external calls. The landline phones should be strictly used to conduct official work only. As far as possible, no personal calls should be made using landline phones owned by the organization.

- 6.17.2 Long distance calls should be made after careful consideration of the business needs since they incur significant costs to the organization.
- 6.17.3 The Admin. Department is responsible for allotting/installing/maintaining telephone connections in offices. For any problems related to telephones, the Stakeholders shall immediately mail to hrassist@INOXCVA.com.
- 6.17.4 Stakeholders should remember to follow telephone etiquette and be courteous while representing themselves and the organization using the organization's phone services.

PERSONAL COMPUTER (PC) STANDARDS

7.1 *Objective:*

- 7.1.1 The main aim of this policy is to maintain standard configurations of PC hardware and software purchased by the organization and provided to Stakeholders for official work. The hardware standards will help maintain optimum work productivity, computer health & security, inventory management and provide timely and effective support in troubleshooting PC problems. The software standards will ensure better system administration, effective tracking of software licenses and efficient technical support.

7.2 *General Guidelines:*

- 7.2.1 It is the responsibility of the IT Department to establish and maintain standard configurations of hardware and software for PCs owned by the organization. The standard, can however, be modified at any point in time as per specific business needs on the approval of Steering Committee in consultation with the relevant department heads.
- 7.2.2 Multiple configurations shall only maintained in consultation with the Department/Project Head wherein there are different requirements of various departments and projects in the organization.
- 7.2.3 Only in exceptional cases, when none of the standard configurations satisfy the work requirements, can an employee request a non-standard PC configuration. Valid reasons need to be provided for the request and written approval of the Reporting Manager(s) is required for the same.

7.3 *Network Access:*

- 7.3.1 All PCs used in the organization are enabled to connect to the organization's Local Area Network as well as the Internet.
- 7.3.2 Network security is enabled in all PCs through Firewall, Web Security and Email Security software.
- 7.3.3 Stakeholders are expected to undertake appropriate security measures as enlisted in the IT Policy.

7.4 *Data Backup Procedure :*

- 7.4.1 Data Backup is setup during installation of Operating System in a PC. As an additional security measure, it is advised that Stakeholders keep important official data on the server. Data can only be transferred to any external storage device on urgent business needs by Stakeholders having an authority to do so or unless authorised by the Head of the Department.
- 7.4.2 File Backup System:
 - 7.4.2.1 Organization has installed a file server for backing up data of all Stakeholders. All Stakeholders are expected to keep official data on the file server.
 - 7.4.2.2 Stakeholder's Reporting Manager or the SPOC will have access to that data.
 - 7.4.2.3 All employees will login to the file server through user ID and password.
- 7.4.3 Server backup:
 - 7.4.3.1 IT Department shall maintain an incremental or Full backup of all servers with at least 3 copies of all servers.
 - 7.4.3.2 Replica mode or Backup of all running servers will be offline and it should maintain backup every twenty-four hours.
 - 7.4.3.3 The hard disk of every server should be in the RAID.

7.5 Antivirus Management Policy

7.5.1 Purpose

This policy establishes requirements for the implementation, maintenance, and monitoring of antivirus software across all information systems within INOXCVA to protect the organization's assets from malware threats in accordance with ISO 27001:2013 requirements, specifically control A.12.2 (Protection from malware).

7.5.2. Scope

This policy applies to:

- All computing devices owned, managed, or operated by or on behalf of the organization
- All servers, workstations, laptops, mobile devices, operational technology (OT), and Industrial Control Systems (ICS) connected to company networks
- All employees, contractors, vendors, and third parties who access the organization's information systems

7.5.3. Policy Statements

7.5.3.1 General Requirements

1. All information systems and computing devices within the organization must be protected by approved antivirus/anti-malware software.
2. Systems that cannot support conventional antivirus solutions (e.g., certain ICS/OT systems) must be protected through alternative security controls approved by the Information Security Officer.
3. Antivirus software and virus definition files must be kept up-to-date according to the update procedures defined in this policy.
4. Users are prohibited from disabling, modifying, or uninstalling antivirus software without explicit authorization from the Information Security Officer.

7.5.3.2 Implementation Requirements

1. The IT Department shall maintain a standard approved list of antivirus/anti-malware solutions appropriate for different system types within the manufacturing environment.
2. Antivirus software deployment must include:
 - Real-time scanning of files upon access
 - Scheduled full-system scans at least weekly
 - Automatic update mechanisms for virus definitions
 - Logging and alerting capabilities
3. Special consideration for manufacturing systems:
 - Antivirus scanning and updates for ICS/OT environments must be tested in a non-production environment prior to deployment
 - Scanning schedules for production systems must be configured to minimize operational impact
 - Application whitelisting should be implemented where feasible

7.5.3.3 Update Management

1. Virus definition files must be updated at least daily on standard IT systems.
2. For manufacturing control systems (OT/ICS):

- Updates must be applied according to a risk-based schedule established with operations management
 - Updates must be tested in a non-production environment before deployment
 - Updates should be applied during scheduled maintenance windows when possible
3. Exceptions to the update schedule must be documented and approved by the Information Security Officer.

7.5.3.4 Monitoring and Response

1. The IT Department shall implement centralized monitoring of antivirus status across the organization.
2. Malware detection alerts must be responded to according to the organization's Incident Response Plan.
3. Monthly reports on antivirus status, threats detected, and remediation actions shall be provided to the Information Security Officer.
4. Systems repeatedly infected with malware must undergo security reassessment.

7.5.3.5 Air-gapped Systems

1. For isolated or air-gapped systems, the IT Department shall establish a procedure for regular, controlled updates of antivirus definitions.
2. Portable media used to update air-gapped systems must be scanned on secure systems before use.
3. A log of all updates to air-gapped systems must be maintained.

7.5.3.6 Removable Media Control

1. All removable media (USB drives, external hard drives, etc.) must be scanned before connection to any organizational system.
2. Automatic scanning of removable media upon connection must be enabled where technically possible.
3. The use of removable media in manufacturing environments must be strictly controlled according to the organization's Removable Media Policy.

7.5.3.7 Training and Awareness

1. All employees shall receive security awareness training that includes malware threats, social engineering techniques, and proper use of antivirus software.
2. Manufacturing staff shall receive specialized training on malware risks to industrial systems.
3. Security awareness refresher training shall be conducted annually.

7.5.4. Roles and Responsibilities

7.5.4.1 Information Security Officer

- Overall responsibility for antivirus protection strategy
- Approving exceptions to this policy
- Reviewing antivirus status reports and ensuring compliance with this policy

7.5.4.2 IT Department

- Selection, implementation, and maintenance of antivirus solutions
- Monitoring system compliance with this policy
- Responding to malware incidents
- Maintaining centralized management of antivirus software

7.5.4.3 OT/ICS Team

- Collaborating with IT on appropriate antivirus solutions for manufacturing systems
- Scheduling and implementing updates for manufacturing systems
- Implementing compensating controls where standard antivirus solutions cannot be used

7.5.4.4 All Users

- Complying with this policy and related procedures
- Reporting suspected malware infections immediately
- Not interfering with antivirus operations

7.5.5. Compliance and Exceptions

1. Compliance with this policy shall be verified through periodic audits conducted by the Information Security Officer or designated third parties.
2. Non-compliance may result in disciplinary action in accordance with the organization's HR policies.
3. Exceptions to this policy must be:
 - Documented with clear business justification
 - Approved by the Information Security Officer
 - Reviewed at least quarterly
 - Accompanied by compensating controls where appropriate

7.5.6. Related Documents

- Information Security Policy
- Incident Response Plan
- Acceptable Use Policy
- Removable Media Policy

- Change Management Policy
- Risk Assessment Procedure

7.5.7. Review and Update

This policy shall be reviewed annually and updated as needed to reflect changes in the organization's risk environment, technology infrastructure, or regulatory requirements.

7.5.8. References

- ISO/IEC 27001:2013, specifically Annex A.12.2 (Protection from malware)
- ISO/IEC 27002:2013 implementation guidance
- IEC 62443 (Industrial network and system security)

7.5.9. Definitions

- **Malware:** Software designed to infiltrate, damage, or obtain unauthorized access to a computer system
- **Antivirus Software:** Programs designed to detect, prevent, and remove malware
- **ICS:** Industrial Control Systems that manage and control industrial processes
- **OT:** Operational Technology that monitors and controls physical devices and processes in the manufacturing environment

INTERNET USAGE POLICY

8.1 Objective:

- 8.1.1 The Internet Usage Policy provides guidelines for acceptable use of the organization's Internet network so as to devote Internet usage to enhance work productivity and efficiency and ensure safety and security of the Internet network, organizational data and the Stakeholders.

8.2 General Guidelines:

- 8.2.1 The organization has installed an Internet Firewall to assure safety and security of the organizational network. Any employee who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary.

- 8.2.2 Internet is a paid resource and therefore shall be used only for office work. The organization reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the organization's network.
- 8.2.3 The organization has systems in place to monitor and record all Internet usage on the organization's network including each website visit, and each email sent or received. The IT Department can choose to analyse Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy.
- 8.2.4 Restricted websites likes Social media , News, Gambling, Online Shopping, Video Streaming or any inappropriate website should be blocked and open only after HOD approvals.

8.3 *Internet Login Guidelines:*

- 8.3.1 All Stakeholders may be provided with a Username and Password to login to the Internet network in the office for their individual official usage.
- 8.3.2 Stakeholder can also get a local static IP address for internet and intranet use. All Stakeholders will be responsible for the internet usage through this local static IP.
- 8.3.3 The IT Department has defined guidelines for issuing new passwords or allowing Stakeholder to modify their own passwords. Username and password for a new employee must be requested by the HR Department.
- 8.3.4 Sharing the Username and Password with another employee, visitor or guest user is prohibited.
- 8.3.5 A visitor or guest user who wants to use the office Internet will be given a Guest Username and Password but Guest system should have updated Antivirus and all Windows related Security patches
- 8.3.6 Any password security breach must be notified to the IT helpdesk immediately.
- 8.3.7 Username and password allotted to an employee will be deleted upon resignation/termination/retirement from the organization.

8.4 *Password Guidelines:*

- 8.4.1 The following password guidelines shall be followed to ensure maximum password safety.

8.4.1.1 Choose a password with 8 or more characters which does not contain easily identifiable words (e.g. your username, name, phone number, house location etc.) with at least one numeric and one special character apart from letters.

8.4.1.2 Combine multiple unrelated words to make a password.

8.4.2 Keep your Password Safe:

8.4.2.1 Do not share your password with anyone.

8.4.2.2 Make sure no one is observing you while you enter your password.

8.4.2.3 As far as possible, do not write down your password. If you want to write it down, do not display it in a publicly visible area.

8.4.2.4 Change your password periodically (every 3 months is recommended).

8.4.2.5 Do not reuse old passwords. If that is difficult, do not repeat the last 5 passwords.

8.5 *Other Security Measures:*

8.5.1 Ensure your computer is reasonably secure in your absence.

8.5.2 Lock your monitor screen, log out or turn off your computer when not at desk.

8.6 Online Content Usage Guidelines:

8.6.1 Stakeholders are solely responsible for the content accessed and downloaded using Internet facility in the office. If they accidentally connect to a website containing material prohibited or considered inappropriate by the organization, they should disconnect from that site immediately.

8.6.2 During office hours, employees should not access news, social media and other websites online, unless required for office work.

8.6.3 Stakeholders are not allowed to use Internet for non-official purposes using the Internet facility in office.

8.6.4 Stakeholders should schedule bandwidth-intensive tasks like large file transfers, video downloads, mass e-mailing etc. for off-peak times.

8.7 *Inappropriate Use:*

8.7.1 The following activities are prohibited on organization's Internet network. This list can be modified/updated anytime by the IT Head as deemed fit.

8.7.2 Appropriate disciplinary action (including legal action or termination) can be taken against an employee involved in the activities mentioned below:

- 8.7.2.1 Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth.
- 8.7.2.2 Downloading images, videos and documents unless required for official purpose.
- 8.7.2.3 Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of inflammatory, pornographic or sexually explicit material unless explicitly required for office work.
- 8.7.2.4 Accessing pirated software, tools or data using the official network or systems.
- 8.7.2.5 Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the HR department.
- 8.7.2.6 Engaging in any criminal or illegal activity or violating any law.
- 8.7.2.7 Invading privacy of co-workers.
- 8.7.2.8 Using the Internet for personal financial gain or for conducting personal business.
- 8.7.2.9 Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.
- 8.7.2.10 Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the organization's reputation.

INFORMATION SECURITY POLICY

9.1 Objective:

- 9.1.1 Information security means protection of the organization's data, applications, networks and computer systems from unauthorized access, alteration and destruction. The Information Security Policy provides guidelines to protect data integrity based on data classification and secure the organization's information systems.
- 9.1.2 The objectives of the "Information Security Policy" are;
 - 9.1.2.1 To prevent unauthorized disclosure of information stored or processed (Confidentiality).
 - 9.1.2.2 To prevent unauthorized accidental or deliberate alteration of information (Integrity).
 - 9.1.2.3 To prevent unauthorized accidental or deliberate destruction or deletion of information necessary for operations (Availability).

9.2 General Guidelines:

- 9.2.1 Various methods like access control, authentication, monitoring and review will be used to ensure data security in the organization.
- 9.2.2 Security reviews of servers, firewalls, routers and monitoring systems to be conducted on a regular basis. These reviews should include monitoring of access logs and intrusion detection software logs.

- 9.2.3 Appropriate training to be provided to data owners, data users, and network & system administrators to ensure data security.

9.3 *Data Classification:*

- 9.3.1 The organization classifies data into three categories:

- 9.3.1.1 **High Risk:** It includes information assets which have legal requirements for disclosure and financial penalties imposed for disclosure. E.g. Payroll, personnel, financial, biometric data.
- 9.3.1.2 **Medium Risk:** It includes confidential data which may or may not directly impose losses on the organization if disclosed but are of strategic importance, but is also not publicly available. E.g. Agreement documents, trade secrets, unpublished reports, intellectual property, financials, client/vendor list, pricing etc.
- 9.3.1.3 **Low Risk:** It includes information that can be freely disseminated. E.g. brochures, published reports, other printed material etc.

- 9.3.2 Different protection strategies must be developed by the IT department for the above three data categories. Information about the same must be disseminated appropriately to all relevant Stakeholders.

- 9.3.3 High risk data must be encrypted when transmitted over insecure channels.

- 9.3.4 All data must be backed up on a regular basis as per the rules defined by the IT Department.

9.4 *Access Control*

- 9.4.1 All critical IT equipment's (Servers, Routers, Switches, IDS, Firewall etc.) shall be installed in a physically secure and restricted room/Area (Data centre/Server Room) and access shall be restricted to authorize users only.

- 9.4.2 All instances of access to the Data Centre shall be logged electronically or physically for periodic review of the Steering committee along with user list.

- 9.4.3 Serving or consumption of food, beverages or cold drinks is strictly prohibited in the Data Centre.

- 9.4.4 Hazardous and / or combustible materials is strictly prohibited within the data centre.

9.4.5 Formal procedures shall be in place to control the allocation, revocation and review of access rights to information systems and services achieved by individual logins and shall require strong authentication by way of passwords, biometrics etc.

9.4.6 All users of systems which contain high or medium risk data must have a strong password as defined in the IT Policy.

9.4.7 Default passwords on all systems must be changed after installation.

9.4.8 Access to information, data or application shall be restricted according to the user's requirement or role in the organisation. A list of designated approvers shall be maintained for various types of access and access to information services shall be controlled by using unique User Id.

9.4.9 Remote access to Information system shall be given to the Stakeholder with approval of HOD through secured VPN channel authenticated via password authentication or public/private keys with strong pass-phrases.

9.4.10 Designated network Administrator/s shall be responsible to maintain the system level user accounts i.e. root with separate account for regular administration. System Administrator shall logon as themselves, using a normal User Id when performing regular work duties. Logging in as the Supervisor/Administrator shall be limited to administrative activities only.

9.4.11 Third party user's access on special approval from the IT Head shall be granted for defined time frame only for the specific purpose subject to such third party agreement to our policies.

9.4.12 Access revocation shall be initiated in the following cases:

- Employee Separation/Transfer/Promotion
- End of temporary Service need
- Violation of Acceptable usage guideline

9.4.13 Application user's privilege levels shall be reviewed and validated periodically by the business process owner.

9.4.14 The Systems Administrator shall review system access violation logs on a daily basis. All access violation attempts (user and resource authentication) shall be logged and reported by the Systems Administrator Steering Committee for necessary action.

9.5 *User Id Rules*

- 9.5.1 There shall be a one-to-one relationship between user Ids and individuals, except group ids.
- 9.5.2 Access to computing resources (e.g. Internet, E-mail, Applications) via shared User Ids/Generic ID is strictly prohibited.
- 9.5.3 Any group ID (E-mail) required for specific business purpose shall be created with approval of the Departmental Head and Application head/ Country IT manager. Business justification for the use of such ID shall be documented.
- 9.5.4 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.
- 9.5.5 All user accounts created in all systems & application should contain the complete details of individuals like Full name, business unit details, department, employee id etc.
- 9.5.6 All "Default" user-ids that are shipped with the application shall be deactivated if not used.
- 9.5.7 Inactive users shall be logged off from applications after a predefined inactivity time.
- 9.5.8 User ID shall be locked after a predefined number of failed logon attempts.

9.6 *Password Management:*

- 9.5.9 The minimum password length, maximum password age, history of passwords, failed log-in attempts etc, shall be set as per the Password Standards defined.
- 9.5.10 Easy to guess passwords shall not be used. 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 computer without access control, or in other locations where unauthorized people might discover them.
- 9.5.11 Systems shall force users to change password after first logon, however, in case where system/process does not force/allow users to change password after first logon, the password generated by the administrator should be unique and shall be communicated to user in secured manner. Conveyance of passwords through unprotected (clear text) electronic mail messages is prohibited.
- 9.5.12 Authentication codes/passwords transmitted across the network shall be encrypted.
- 9.5.13 The User Id and password for highly privileged users e.g. Supervisor/Administrator shall be stored in a sealed envelope and placed in a secure location.

9.7 *Virus Prevention:*

- 9.5.14 Virus prevention for personal computers and email usage has been described previously.
- 9.5.15 Apart from that, all servers and workstations that connect to the network must be protected with licensed anti-virus software recommended by the vendor. The software must be kept up-to-date.
- 9.5.16 Whenever feasible, system/network administrators must inform users when a virus/ other vulnerability has been detected in the network or systems.

9.8 *Intrusion Detection:*

- 9.8.1 Intrusion detection must be implemented on all servers and workstations containing high and medium risk data.
- 9.8.2 Operating system and application software logging process must be enabled on all systems.
- 9.8.3 Server, firewall and critical system logs must be reviewed frequently.

COMPUTING ENVIRONMENT MANAGEMENT

10.1 *Objective:*

- 10.1.1 The objective of this policy is to provide effective management of the computing environment to ensure the correct and secure operation of information processing facilities.

10.2 *Documented Operating Procedures:*

- 10.2.1 Clear documented operating/management procedures shall be prepared for all operational computerized systems specifying the correct instructions for detailed execution of each job including the following;
 - 10.2.1.1 System restart and recovery procedures for use in the event of system failure;
 - 10.2.1.2 Instructions for handling errors or other exceptional/emergency conditions.
 - 10.2.1.3 Support contacts in the event of unexpected operational or technical difficulties.
 - 10.2.1.4 Scheduling requirements, including interdependencies with other systems.
 - 10.2.1.5 Batch and background job execution and review requirements.

10.2. System specific documented procedures shall also be prepared for system housekeeping functions associated with computer and network management such as computer start-up and closedown procedures, back up and equipment maintenance by the concerned administrator.

10.2.3 All such documents shall be reviewed by the Steering Committee.

10.3 Authentication and Account Management:

10.3.1 To enhance the security and pre-empt cyber attacks the organisation uses Multi factor authentication (MFA) for authenticating users.

10.3.2 The multifactor authentication shall use a combination of:

10.3.2.1 Password or PIN

10.3.2.2 Official Laptop/PC

10.3.2.3 OTP

10.3.3 The Company also uses Risk-based Authentication. Adaptive Authentication to analyze additional factors by considering context and behavior when authenticating and often uses these values to assign a level of risk associated with the login attempt. For example: From where is the user when trying to access information? When you are trying to access company information? What kind of device is used? Is it the same one used yesterday? Is the connection via private network or a public network?

10.3.4 The credentials of privileged admin accounts shall be secured in a repository

(a vault) to reduce the risk of those credentials being stolen. Once the System administrators go through the PAM system to access their credentials, they shall be authenticated and their access logged. When a credential is checked back in, it shall be reset to ensure administrators go through the PAM system next time they want to use the credential.

10.3.5 Unnecessary accounts/groups shall be periodically monitored and deleted.

10.4 Segregation of Duties:

10.4.1 Management or execution of certain duties or areas of responsibility shall be segregated, in order to reduce opportunities for misuse of information or services.

10.4.2 The same Stakeholder (except at supervisory level) shall not carry out any two or more of the following functions;

- Transaction data entry
- Database administration
- System development and maintenance
- Security administration
- System administration
- Network administration
- SAP Functional Consultant
- Security audit.

10.4.3 Clear security boundaries shall exist between development and production environments and accordingly Developers shall not have access to production systems (excepting display access) or data except during support in emergencies.

10.4.4 If due to business exigencies, functions cannot be segregated, alternate controls such as monitoring of activities and audit trails and management supervision shall be implemented.

10.4.5 It is important that security audit shall remain independent.

10.5 Disposal of Data Storage Media:

- 10.5.1 Data Storage Media like Hard Disk drives, Removable disks, DATs, cassettes, Optical storage media, Magnetic tapes etc; shall be disposed of securely and safely when no longer required.
- 10.5.2 Media containing sensitive information (Restricted or Confidential) shall be disposed of securely and safely when it is no longer required e.g. by incineration or destroyed by securely deleting.
- 10.5.3 The contents of any re-usable media that are to be disposed shall be erased in such a way so that it cannot be recovered.

NETWORK SECURITY POLICY

11.1 Objective:

- 11.1.1 Network security forms an integral part of the overall Information Security, and is important to all users. Network security assumes importance as usage of various networking, communications and computing technologies though effectively meet the user needs but also transmits Sensitive data over networks.
- 11.1.2 The network services software and other application or utility software, installed on a server, shall be identified and documented.

- 11.1.3 All critical parameter settings, scripts and configuration files used during installation of a network operating system shall be documented.
- 11.1.4 The following issues shall be considered while deploying a network server:
- 1) The categories of information that shall be stored on the server
 - 2) The security requirements for that information
 - 3) The network services that shall be provided by the network server
 - 4) The security requirements for the network services.
- 11.1.5 Operating System shall be hardened through the following;
- a. All unused ports shall be blocked
 - b. Only required services shall be enabled
 - c. Latest approved hot fixes / Patches shall be applied
 - d. Configure security policies for authentication and access control
 - e. All unnecessary users (e.g. guest) shall be disabled
 - f. Default passwords shall be changed as part of the installation process.
 - g. A warning banner shall be displayed at login.
 - h. Inactive terminals shall be set to a timeout of 5 minutes wherever applicable.
- 11.1.6 Password should be set and managed as per password policy.
- 11.1.7 All unsuccessful login attempts shall be recorded and reviewed by the System Administrator on a daily basis.
- 11.1.8 Availability of Network servers shall be monitored/logged and escalated through centralized network management server.

11.2 Server Control:

- 11.2.1 The specification/configuration and purpose of each server on the network shall be identified and how the server would be used shall be documented.
- 11.2.2 The network server shall be dedicated to a single network service wherever applicable (e.g. DNS, ftp and http services).
- 11.2.3 All critical parameter settings, scripts and configuration files used during installation of a network operating system shall be documented.
- 11.2.4 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
- 11.2.5 Operating System shall be hardened through the following;
- All unused ports shall be blocked

- Only required services shall be enabled
- Latest approved hot fixes / 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.
- Wherever possible a warning banner shall be displayed at login.
- Inactive terminals shall be set to a timeout of 5 minutes wherever applicable.

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

11.2.7 All unsuccessful login attempts shall be recorded. The System Administrator shall review this on a daily basis.

11.2.8 Availability of Network servers shall be monitored/logged and escalated through centralized network management server.

11.3 Routers:

11.3.1 Remote and local access to routers shall be restricted to limited users and unnecessary services of Routers shall be disabled. Appropriate ACLs (access control lists) shall be applied to allow the desired services only.

11.3.2 Time out for all modes of access sessions to the Routers (Telnet, Console, Aux) shall be set to a time out of 5 minutes.

11.3.3 All critical events including login attempts, configuration changes, access violation messages generated by Access Control Lists (ACL's), system error messages of routers shall be logged and these logs shall be reviewed daily by Systems Administrator (s).

11.4 Firewall:

11.4.1 Firewall shall be appropriately implemented to segregate the networks into different network segments.

11.4.2 The following shall be considered during the implementation of a firewall system:

11.4.2.1 If a software firewall is used, the host on which the Firewall is installed should be secured.

11.4.2.2 Specific security guidelines as specified by the firewall vendor should be configured.

11.4.2.3 The firewall should be configured for full logging and a mechanism for generating alerts on suspicious activity.

11.4.2.4 The firewall system shall deny all inbound and outbound services unless specifically permitted.

11.4.2.5 The firewall administrator or a monitoring system shall review log files on a daily basis and investigate any unusual activity.

11.4.2.6 Defined change control procedures shall be followed when making changes to the firewall system.

11.4.2.7 Internet facing firewall rules shall be periodically reviewed to ensure there is no loophole that allow malicious inbound. traffic,

11.4.2.8 Changes to firewall system shall include

- Modification of ACL for the firewall system
- Upgrades or modifications to the firewall operating systems
- Upgrades or modification of the firewall application
- Addition of new firewall system hardware

11.5 Intrusion Detection System (IDS) / Monitoring:

11.5.1 IDS shall be deployed for the critical segments of the network and IDS logs shall be monitored and reviewed on daily basis.

11.5.2 IDS signature files shall be updated on regular basis.

11.6 Switch/LAN:

11.6.1 Access to all switches shall be restricted as per the access policy.

11.6.2 Various network segments shall be segregated through implementation of VLAN.

11.6.3 Critical segments of the network (DMZ, Internal Servers etc) shall be segregated from other network segments.

11.6.4 Internet facing server and IP range shall be frequently scanned to find potential exposure.

11.7 Wireless:

11.7.1 Wireless Access Points default password shall be changed and appropriate encryption mechanism shall be configured for wireless LAN communication.

11.7.2 The SSID of the Access point shall be changed from the factory default to prevent easy access.

11.7.3 Access points should disable broadcast SSID feature.

11.8 Database:

11.8.1 The database server shall be placed behind a firewall and IDS shall be used to detect any intrusion attempts.

11.8.2 The database server process should run as a user with minimum required privileges and never as administrator.

- 11.8.3 Default database users not required should be removed and 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.
- 11.8.4 Depending upon importance of data, fine grained record/row level auditing should be considered.
- 11.8.5 Direct access to backend database servers (production) shall be strictly restricted.

11.9 Internet Security

- 11.9.1 Access to Internet shall be restricted and as per need.
- 11.9.2 All Internet connections shall pass through a firewall and/or a proxy server.
- 11.9.3 Dial up internet access is strictly prohibited.
- 11.9.4 Users should adhere to Internet usage guideline as defined in acceptable user guideline and are prohibited from accessing Web Sites that are deemed inappropriate.
- 11.9.5 World Wide Web activity shall be monitored to ensure that proper levels of security are maintained.
- 11.9.6 The Systems Administrator shall define the protocols/services/sites to be allowed for use.
- 11.9.7 All access to Internet services shall be logged and shall be review by the System Administrator on a weekly basis.

11.10 VPN Security:

- 11.10.1 Strong user authentication shall be implemented to ensure the privacy of client-to-gateway communications.
- 11.10.2 The authentication methods deployed may include traditional username/password authentication, RADIUS (Remote Authentication Dial-in User Service) or TACACS/TACACS+ servers, LDAP-compliant directory servers, X.509 digital certificates, and two-factor schemes such as those involving hardware tokens and smart cards.
- 11.10.3 All VPN user login shall be logged and maintained for future reference.
- 11.10.4 VPN Server rules shall state those machines which users should have access to.

- 11.10.5 System Administrator 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.

WEBSITE SECURITY

12.1 Objective:

- 12.1.1 This policy discusses the standards applicable for web-sites across globe. The following controls shall also be used for website security, wherever applicable.

12.2 Domain Name Security:

- 12.2.1 Use of any website shall be authorized by the Change Control Board.
- 12.2.2 Access to domain name registration information shall remain with CIO. Any changes in the domain name registration information shall only be upon authorization of the CIO.
- 12.2.3 The CIO in consultation with the Business Units shall identify possible domain names representing the brand and shall take appropriate initiatives to proactively take control of these domains, so as to prevent any misuse of the brand name.
- 12.2.4 Any reported instance of a website(s) causing harm (through its content or domain name) to the public image shall be communicated to the Legal department for necessary action.

12.3 Web Site hosting:

- 12.3.1 CIO shall formally approve web site hosting location and platform.
- 12.3.2 Appropriate security controls as mentioned below shall be implemented as part of website hosting:
- 12.3.2.1 Public web servers shall be placed in a demilitarized zone (DMZ) secured behind firewall and IDS/IPS.
- 12.3.2.2 Firewall, IDS/IPS and Routers shall be configured as per the best practices defined.
- 12.3.2.3 The firewall shall filter traffic between Internet, Intranet and DMZ section and shall allow only the minimal required protocols/Services.

12.4 Host Security:

- 12.4.1 The operating system on which the website shall be hosted shall be hardened/secured as per vendor suggested best practices.
- 12.4.2 The operating system shall enable the required logging. Web Server access and security logs shall be analyzed daily.
- 12.4.3 Host based IDS shall be implemented wherever applicable.

12.5 Application Security:

- 12.5.1 The web application server shall be hardened and adequate logging shall be enabled on the application server.
- 12.5.2 Application code developed shall be reviewed to check against common security flaws like SQL injection and cross-site scripting.
- 12.5.3 Database server used by web site should never be accessible directly from Internet.
- 12.5.4 Websites should undergo regular vulnerability assessment, penetration testing and audit as per the audit policy.

12.6 Content upload and management:

- 12.6.1 Any content uploading/modification/change to the public web site shall be done with prior approval from the Change control Board.
- 12.6.2 Access to the web server shall be restricted to user on a “need-to-do” basis and should be as per access policy.
- 12.6.3 Latest content and configuration of web server shall be uploaded in the configuration management database as per the configuration management policy.
- 12.6.4 Content of websites shall be backed up as per the approved backup policy.

12.7 Third party hosting:

- 12.7.1 Selection of third party hosting services shall specifically include security requirements as per business needs. The organization should be able to show case their process maturity in terms of security. This may include Industry standard certifications like ISO27001 etc.

- 12.7.2 In case of third party hosting, appropriate contract and SLA shall be signed as per the “Third party and outsourcing policy”.
- 12.7.3 The SLA in this case shall explicitly include the security requirements and appropriate penalties in case of violations thereof.

VIRUS MANAGEMENT POLICY

13.1 Objective:

- 13.1.1 All Assets to be adequately protected against all viruses/Worms/Trojans.

13.2 General Conditions:

- 13.2.1 Anti-virus software, approved by the IT Department, should always be kept running in all desktops/laptops/servers without exception.
- 13.2.2 User systems shall be configured to download the latest virus protection signature files from Internet sites/Intranet servers after confirmation of IT department.
- 13.2.3 Virus scanning should be done on all software/files supplied by third party in the form of CDs/DVDs/USB drives or any other removable media before loading it into the system.
- 13.2.4 The users shall perform virus scanning each time any file is copied from any source including network drives and any removable media.
- 13.2.5 All information or files downloaded from the Internet and all mail attachments shall be scanned for viruses automatically.
- 13.2.6 In case a virus outbreak alert is received, the IT Help desk and System Administrator shall inform all the users immediately about the ways and means to protect against the virus attack.
- 13.2.7 If a virus attack is suspected, the following shall be observed;
- Suspected tape / disk shall be isolated
 - Affected server / PC / laptop shall be isolated
- 13.2.8 Gateway antivirus shall be implemented for E-mail server. All incoming and outgoing mails shall be scanned for virus automatically.

- 13.2.9 Virus affections should be recorded as “incident” events and the Systems Administrator shall duly maintain a log of the same. (Refer Incident management procedures).

14. Backup & Restore Policy

14.1 Objective:

14.1.1 1. Purpose

This Backup and Restore Policy establishes the requirements for the backup and restoration of information systems and data within [Organization Name] to ensure business continuity, minimize data loss, and comply with ISO 27001:2013 requirements, specifically control objective A.12.3 (Information Backup).

14.2. Scope

This policy applies to all information systems, applications, and data repositories owned, operated, or managed by [Organization Name], including cloud-based services and outsourced IT functions. It applies to all employees, contractors, consultants, temporary staff, and other workers at [Organization Name] who administer or maintain these systems.

14.3 Roles and Responsibilities

14.3.1 Information Security Officer (ISO)

- Overall responsibility for this policy
- Regular review and update of this policy
- Monitor compliance with this policy

14.3.2 IT Department

- Implementation of backup and restore procedures
- Monitoring and verification of backup success/failure
- Testing of restore procedures
- Management of backup infrastructure and media
- Documentation of backup configurations and restoration procedures

14.3.3 System and Application Owners

- Define data classification and retention requirements
- Approve backup schedules and retention periods
- Validate restoration procedures for their systems

14.3.4 All Staff

- Ensure that business-critical data is stored in designated locations that are included in backup schedules
- Report any suspected data loss or corruption immediately

14.5. Backup Requirements

14.5.1 Data Classification and Backup Frequency

Backup frequency shall be determined based on data classification:

Classification	Description	Backup Frequency	Retention Period
Critical	Essential for business operations, significant financial or legal impact if lost	Daily full backup	7 years
High	Important for business operations, moderate impact if lost	Daily incremental, weekly full backup	3 years
Medium	Normal operational data, limited impact if lost	Weekly full backup	1 year
Low	Non-essential data, minimal impact if lost	Monthly full backup	3 months

14.5.2 Backup Storage Requirements

14.5.2.1 On-site Backups

- On-site backups must be stored in a secure location with appropriate environmental controls
- Access to backup media and backup systems must be restricted to authorized personnel
- Backup media must be clearly labeled with content, date, and classification

14.5.2.2 Off-site Backups

- Critical and high classification data must maintain off-site backups
- Off-site storage facilities must provide appropriate physical security, environmental controls, and access restrictions
- Transport of backup media must be conducted securely by authorized personnel or trusted third parties

14.5.2.3 Cloud-based Backups

- Cloud backup providers must be assessed and approved by the Information Security Officer
- Cloud backup solutions must use encryption for data in transit and at rest

- Access controls must be implemented to restrict access to authorized personnel only

14.5.3 Backup Technology and Methods

14.5.3.1 Backup Types

- Full Backup: Complete backup of all selected files
- Incremental Backup: Backup of files changed since the last backup
- Differential Backup: Backup of files changed since the last full backup

14.5.3.2 Encryption Requirements

- All backup data containing sensitive or confidential information must be encrypted
- Encryption keys must be managed according to the organization's Cryptographic Controls Policy
- Minimum encryption standard: AES-256

14.6. Restoration Procedures

14.6.1 Restoration Testing

- Restore capabilities shall be tested at least quarterly for critical systems
- Restore capabilities shall be tested at least semi-annually for high classification systems
- Restore capabilities shall be tested at least annually for medium classification systems
- Results of restoration tests shall be documented and reviewed

14.6.2 Restoration Requests

- Business unit managers may authorize data restoration requests for their department
- The IT Department shall document all restoration requests and outcomes
- For emergency restores, the IT Manager or Information Security Officer may authorize the restore

14.6.3 Restoration Priorities

In the event of a major incident requiring multiple restores, the following priority shall be followed:

1. Systems supporting health and safety functions
2. Systems supporting critical business operations
3. Systems containing customer data
4. Systems supporting financial functions
5. Other business systems

14.7. Backup Monitoring and Reporting

14.7.1 Monitoring Requirements

- All backup jobs shall be monitored for successful completion
- Failed backup jobs shall trigger automated alerts to IT staff
- Backup systems shall be monitored for capacity and performance

14.7.2 Reporting Requirements

- Monthly backup status reports shall be generated and reviewed by the IT Department
- Quarterly compliance reports shall be provided to the Information Security Committee
- Any backup failures that could result in data loss shall be reported as security incidents

14.8. Data Retention and Disposal

14.8.1 Retention Periods

- Backup retention periods shall comply with legal, regulatory, and business requirements
- Retention periods shall be defined in the Data Classification and Handling Policy
- Special retention requirements may be implemented for legal holds or investigations

14.8.2 Media Disposal

- All backup media shall be securely disposed of at the end of its retention period
- Physical media shall be destroyed in accordance with the Asset Management Policy
- Cloud-based backups shall be securely deleted and verification obtained from the provider

14.9. Business Continuity and Disaster Recovery

14.9.1 Integration with Business Continuity

- This policy shall be aligned with the organization's Business Continuity Plan
- Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) shall be defined for each system
- Critical systems shall have documented restoration procedures as part of the Disaster Recovery Plan

14.9.2 Disaster Recovery

- In the event of a disaster, backups shall be used to restore systems according to the Disaster Recovery Plan
- Backup and restoration procedures shall be tested as part of disaster recovery exercises
- Alternate restoration sites and procedures shall be documented and tested

14.10 Related Documents

- Information Security Policy
- Data Classification and Handling Policy

- Asset Management Policy
- Business Continuity Plan
- Disaster Recovery Plan
- Incident Management Policy

USER RESPONSIBILITIES / ACCOUNTABILITY

15.1 Reporting security Incidents:

- 15.1.1 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 IT Help Desk and corresponding Business Unit Head.

15.2 Security Awareness and Orientation Session:

- 15.2.1 Each new employee and contract staff of IT Department is required to attend an information security awareness orientation session.
- 15.2.2 The Security Awareness Orientation program shall include 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

15.3 Compliance:

- 15.3.1 It is the responsibility of all Stakeholders to ensure careful, compliant, safe and judicious use of the equipment & other assets allocated to and/or being used by them. All stakeholder shall at all times abide by all the Code of Conduct, Company Policies including this IT Policy as well as all applicable laws.
- 15.3.2 Any violation of the Code of Conduct, Company Policies including this IT Policy as well as all applicable laws is construed as a major misconduct and disciplinary/legal

process shall be initiated against any Stakeholders found in violation of any of the above.

EMAIL & CHAT POLICY

16.1 Objective:

- 16.1.1 This policy provides information about acceptable usage, ownership, confidentiality and security while using electronic messaging systems and chat platforms provided or approved by the organization. The policy applies to all electronic messages sent or received via the above mentioned messaging systems and chat platforms by all official employees of the organization.

16.2 General Guidelines:

- 16.2.1 The organization reserves the right to approve or disapprove which electronic messaging systems and chat platforms shall be used for official purposes.
- 16.2.2 It is strictly advised to use the pre-approved messaging systems and platforms for office use only.
- 16.2.3 Every user shall be provided with a fixed quota of disk space for email purpose wherever applicable.
- 16.2.4 The maximum file size for email attachments shall be restricted to fixed size for security reasons.
- 16.2.5 E-mail content filtering mechanism shall be deployed at gateway level.
- 16.2.6 An employee who, upon joining the organization, is provided with an official email address should use it for official purposes only. It is important to immediately create a standardised email signature with the disclaimer provided by the Company.
- 16.2.7 Any email security breach must be notified to the IT helpdesk immediately.
- 16.2.8 Upon termination, resignation or retirement from the organization, the organization will deny all access to electronic messaging platforms owned/provided by the organization.
- 16.2.9 All messages composed and/or sent using the pre-approved messaging systems and platforms need to comply with the company policies of acceptable communication.

- 16.2.10 Electronic mails and messages should be sent after careful consideration since they are inadequate in conveying the mood and context of the situation or sender and might be interpreted wrongly.
- 16.2.11 All email signatures must have appropriate designations of employees and must be in the format approved by the HR Department.

16.3 Ownership:

- 16.3.1 The official electronic messaging system used by the organization is the property of the organization and not the Stakeholder. All emails, chats and electronic messages stored, composed, sent and received in the official electronic messaging systems are the property of the organization.
- 16.3.2 The organization reserves the right to intercept, monitor, read and disclose any messages stored, composed, sent or received using the official electronic messaging systems.
- 16.3.3 The organization reserves the right to alter, modify, re-route or block messages as deemed appropriate.
- 16.3.4 IT Administrator can change the email system password and monitor email usage of any employee for security purposes.

16.4 Confidentiality:

- 16.4.1 Proprietary, confidential and sensitive information about the organization or its employees should not be exchanged via electronic messaging systems unless pre-approved by the Head of the Department.
- 16.4.2 Caution and proper judgment should be used to decide whether to deliver a message in person, on phone or via email/electronic messaging systems.
- 16.4.3 The email sent from the official id carry a standard disclaimer. However, the courts in certain circumstances may allow emails in legal proceedings. Therefore, before composing or sending any message, it should be noted that electronic messages can be used as evidence in a court of law.
- 16.4.4 Unauthorized copying and distributing of copyrighted content of the organization is prohibited.

16.5 Email Security:

16.5.1 Anti-Virus:

- 16.5.1.1 Anti-virus software pre-approved by the Department. Head - IT should be installed in the laptop/desktop provided to a new employee after joining the organization.
- 16.5.1.2 All employees in the organization are expected to make sure they have anti-virus software installed in their laptops/desktops (personal or official) used for office work.
- 16.5.1.3 Organization will bear responsibility for providing, installing, updating and maintaining records for one anti-virus per employee at a time for the official laptop provided by the organization. The employee is responsible for installing good quality anti-virus software in their personal laptop/desktop used for office work.
- 16.5.1.4 Stakeholders are prohibited from disabling the anti-virus software on organization provided laptops/desktops.
- 16.5.1.5 Stakeholders should make sure their anti-virus is regularly updated and not out of date.
- 16.5.1.6 Phishing test shall be randomly performed to understand vulnerable employee and target awareness program

16.5.2 Safe Email Usage: Following precautions must be taken to maintain email security:

- 16.5.2.1 Do not to open emails and/or attachments from unknown or suspicious sources unless anticipated by you.
- 16.5.2.2 In case of doubts about emails/ attachments from known senders, confirm from them about the legitimacy of the email/attachment.
- 16.5.2.3 Use Email spam filters to filter out spam emails.

16.6 Inappropriate Use:

- 16.6.1 Official Email platforms or electronic messaging systems including but not limited to chat platforms and instant messaging systems should not be used to send messages containing pornographic, defamatory, derogatory, sexual, racist, harassing or offensive material.
- 16.6.2 Official Email platforms or electronic messaging systems should not be used for personal work, personal gain or the promotion or publication of one's religious, social or political views.
- 16.6.3 Spam/ bulk/junk messages should not be forwarded or sent to anyone from the official email ID unless for an officially approved purpose.

SOFTWARE ANALYSIS, DESIGN, DEVELOPMENT IMPLEMENTATION AND USAGE POLICY

17.1 Objective:

- 17.1.1 The Software Analysis, Design, Development Implementation and Usage Policy is defined to provide robust approach towards New Application Development, which would cover the whole SDLC spanning Requirement, Analysis, Design, Development, Testing Implementation and Usage.
- 17.1.2 Depending on the business criticality to release software in iterative incremental releases, an Agile framework (eg., Scrum, Kanban etc.) based software development approach will be taken, which would cover concept/design phase for requirement's definition (product backlog) and application design (UX/UI wireframe, Solution Architecture definition etc.), iterative feature or development phase for software development, Continuous Integration (CI), automated/manual testing and Continuous Deployment (CD).

17.2 Software Planning:

- 17.2.1 The Business Process Owner the Business Unit Head or IT Department can initiate a Request for a New Application development.
- 17.2.2 The Project Proposal shall provide the following details;
 - Problem Area addressed by the Project
 - Objective and Scope of the Project
 - Brief Details of the Proposed Application
 - Business Justification of the Investment
 - Impact on Other Applications and Financial Controls.
- 17.2.3 The Steering Committee would assesses the feasibility and viability of the Project based on the Business Justification of the investment and the Impact Analysis, which would be part of the Proposal Submitted.
- 17.2.4 A Project Plan detailing steps, timelines, and responsibilities shall be developed and a formal Software Development Life Cycle (SDLC) shall be followed for the Project.
- 17.2.5 A Project/Product Manager shall be assigned for any new application development exercise.
- 17.2.6 All major projects need to be approved as per the Delegation of Authority DOA.

17.3 Software Requirement Analysis/Concept Sprint:

- 17.3.1 All Approved Projects must have a Software Requirement Specification Document prepared by the Business Analyst for the Project. The Software Requirement Specification Document must be reviewed and Approved by the Steering Committee and the Head of the Business for which the Application is made.
- 17.3.2 Software Requirement Specification documentation shall include detailed Functional Requirements Specification and the System Requirement Specification that details the business workflow and the functions to be incorporated in the new application. It would also have the Interface Specifications and Data Migration requirements.
- 17.3.3 The Software Requirement Analysis document should also include the Hardware and the Software Platform and the requirements for the same.
- 17.3.4 Application security requirements for the new application/software shall be prepared and included as part of the Software Requirement Specification document that covers;
 - Security requirements from the Information/Business Owners.
 - Technology controls.
 - Audit requirements.
- 17.3.5 In an Agile based approach, a cross-stakeholder team, including but not restricted to, business and IT, will collaboratively develop a product backlog, listing all the high level functional, non-functional, data, and integration requirements. The requirements will be captured using Agile product management tools like Jira/Trello/Asana etc.

17.4 Software Design:

- 17.4.1 The design phase would commence after the completion of the Requirement Analysis phase, and would start only after the signoff of the Software Requirement Specification document by the Business Process Owner who has initiated the Project Request.
- 17.4.2 A System Analyst, assigned by the Project Manager, would prepare the Design Document, which would then be reviewed and approved by the Project Manager.
- 17.4.3 A system architecture design would provide a broad framework for the overall system objective, hardware and software platforms, integration with existing systems, interfaces with external entities etc.
- 17.4.4 The logical architecture and physical architecture design shall be a part of the Design document.
- 17.4.5 Security specifications for the new application shall be documented to provide the development group with specific requirements regarding Application security.

- 17.4.6 In an Agile based software development approach, the design phase would involve developing UX/UI wireframes, software architecture design, development roadmap planning and detailing of user stories etc. A UX/UI designer, along with the support from business teams and product manager, will develop the wireframes (a hi-fidelity prototype of the user's journeys on the application). The product backlog and UX/UI wireframes will form the basis for definition of technical architecture and tools selections.

17.5 Software Development:

- 17.5.1 Development, testing (including unit testing, system integration, load and user acceptance testing), and production will be done in separate, controlled environments (Development Environment) accessible only to the application development team.
- 17.5.2 No development will allowed directly in the Production environment.
- 17.5.3 Source codes shall be controlled through the use of a version control system.
- 17.5.4 A standard naming convention shall be followed for all source code elements.
- 17.5.5 All these developments are "Work for Hire" and INOXCVA Limited is the sole owner of any intellectual property, whether registered/registrable or not, created. The Stakeholder involved in the development of such intellectual property relinquishes all rights including moral rights.
- 17.5.6 In Agile based software development approach, a self-organized multi- stakeholder team comprising of product manager/owner, subject matter experts, scrum master, architect, developers and testers will work on the product backlog items for a given sprint. The key activities of this phase include software development, unit testing, and CI/CD activities. If Scrum methodology is being used then sprint activities such as sprint planning, daily stand up, sprint review, backlog grooming and retrospective will be conducted as per the desired frequency.

17.6 Testing:

- 17.6.1 The Project Manager in consultation with the Steering Committee shall determine the Testing strategy to be adopted for the New Application Development.
- 17.6.2 The testing process would cover the following types of tests:
- Unit Testing
 - System/Integration Testing
 - Load Testing
 - User Acceptance Testing

- 17.6.3 The User Acceptance testing shall be mandatory in any situation while the applicability of other tests shall be determined, as discussed above.

17.7 Unit Testing:

- 17.7.1 All development projects shall undergo Unit Testing with predesigned Test Data (which can cover all the test scenarios), prior to installation in production, under separate test environment, locked against any modification by programmers.
- 17.7.2 Unit test results shall be documented and kept for reference.
- 17.7.3 Changes to the application carried out as a result of the testing shall be subject to appropriate re-testing procedures.
- 17.7.4 The Project Manager shall perform an independent review of unit test results.

17.8 System/Integration Testing:

- 17.8.1 All development projects shall undergo System/Integration Testing with predesigned Test Data (which can cover all the test scenarios), prior to installation in production, under separate test environment, locked against any modification by programmers.
- 17.8.2 Changes to the application carried out as a result of the testing shall be subject to appropriate re-testing procedures.
- 17.8.3 The Project Manager shall perform an independent review of System/Integration test results.
- 17.8.4 Integration test results shall be documented and kept for future reference.

17.9 Load Testing:

- 17.9.1 All major development projects shall undergo load testing in a separate, independently controlled test environment, prior to installation in production.
- 17.9.2 The IT Programmer(s) shall prepare the Load Test Plan, which would be reviewed and approved by the System Analyst for the Project.
- 17.9.3 Load testing shall be conducted based on a reviewed and approved Load Test Plan or Test Scripts.
- 17.9.3.1 Appropriate Load Testing Tools shall be used for this purpose.
- 17.9.3.2 Load Test results shall be documented and kept for future reference.

17.10 User Acceptance Testing:

- 17.10.1 All new Development Projects shall undergo User Acceptance testing prior to installation of the software in production.
- 17.10.2 The “user” team based on an approved UAT Test plan documenting the test scenarios and expected outcomes shall conduct UAT Testing with Pre-designed test data sets (which can cover all the test scenarios.) in a test / quality environment locked for any modifications.
- 17.10.3 Changes to the application carried out as a result of the testing shall be subject to appropriate re-testing procedures.
- 17.10.4 User Acceptance test results shall be documented and kept for future reference.
- 17.10.5 The Head of the Business Unit for which the Application is developed shall indicate acceptance of the Application through a formal sign-off.

17.11 Implementation:

- 17.11.1 The Application owner shall sign off after successful completion of the testing phase before moving the same to production server.
- 17.11.2 Configuration management shall be effected as described in the section “Configuration Management” of this document.
- 17.11.3 The exceptions encountered in Deployment shall be logged and monitored.

ACQUISITION & IMPLEMENTATION OF PACKAGED SOFTWARE POLICY

18.1 Objective:

- 18.1.1 This Policy is aimed ensure a consistent approach towards acquisition and implementation of standard packaged software and covers Purchase, Acquisition and Implementation of Standard Packaged Software including COTS (Commercial Off the Shelf) and MOTS (Modified Off the Shelf) such as ERP Package, CRM Package, SCM Package etc. that can be customized and configured to suit the business need of ‘INOXCVA Limited’.
- 18.1.2 The purchase and installation of Standard Packaged Software, for office automation that do not require customization (such as MS Office, Internet Explorer, Operating System Software, and Network Software etc) is covered under Asset Management.

18.2 Software Purchase and Acquisition:

18.2.1 Purchases of standard packaged software shall be based on business need.

18.2.2 On the requisition of the Business Head, the Steering Committee shall review the request and if found suitable after Business Need Analysis, can initiate purchase as per Delegation of Authority.

18.3 Business Need Analysis:

18.3.1 Detailed business need analysis shall be conducted and a high level functional requirements specification shall be prepared by the requisitioning department.

18.3.2 The business need analysis shall also include an estimate of the proposed user-base.

18.3.3 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.

18.4 Product Selection:

18.4.1 Any purchases of packaged software shall be carried out after following the Product Evaluation and Selection process.

18.4.2 The Product Evaluation shall be based on (but not limited to);

18.4.2.1 Response to RFP/RFQ/RFI from Vendors.

18.4.2.2 Mapping of the product with the high level functional requirements.

18.4.2.3 Product reference feedback from other clients and Demo.

18.4.2.4 After sales support.

18.4.2.5 Product / license pricing.

18.4.2.6 Vendor organizational background.

18.4.2.7 Comparative analysis between products.

18.4.2.8 Market intelligence etc.

18.5 Ownership:

18.5.1 The Ownership of the packaged software shall be vested with the IT Department, whereas the respective Business Unit Head shall be the Custodian. However, respective Business Unit Head shall be the owner for information or data corresponding to the Business Function in the Software.

18.6 Implementation:

- 18.6.1 A Project Plan detailing steps, timelines, and responsibilities shall be developed and is to be followed for the implementation of the packaged software.
- 18.6.2 A Project Manager shall be assigned for any packaged software implementation exercise.
- 18.6.3 A detailed Requirement Analysis document mapping the current business process (As-Is Process), the desired Business Process (To-Be Process) and listing down the functional requirement shall be prepared.
- 18.6.4 Any data migration and master data requirement shall also be listed down. The Requirement Analysis Document must be reviewed and approved by the Business Process Owner(s).
- 18.6.5 A Gap Analysis shall be performed between the desired Business Process (To- Be Process) and the compatibility with the packaged software. The same shall be documented in a "Gap Analysis" document.
- 18.6.6 A process risk assessment should be undertaken and the controls required to mitigate risks shall be identified and included as part of the requirements analysis by the Business Process Owner.
- 18.6.7 A Configuration document shall be prepared highlighting the proposed configuration parameters required for implementation of the packaged software, based on approved Requirement analysis document.
- 18.6.8 Software configuration or custom development shall be performed as per the configuration document.
- 18.6.9 The IT Programmers shall perform all configuration or custom development activity in the 'Development' environment.
- 18.6.10 Application Testing as per pre defined and approved Test Plans shall be performed in the pre defined 'Test' environment. All configurations or custom development shall be transferred from the Development to the Test environment.
- 18.6.11 All packaged software implementation shall undergo a User Acceptance Testing as per the predefined and approved User Acceptance Test Plan. The Business Process Owner shall perform the User Acceptance Test.

- 18.6.12 Pre-designed test data sets (which can cover all the test scenarios including security features testing) shall be used for testing purposes.
- 18.6.13 A User Training Manual shall be prepared and appropriate user training shall be conducted to train the users on usage of the Software Package.
- 18.6.14 The configured software can be moved into the production environment only after a formal signoff from the Business Process Owner.
- 18.6.15 Only the Application Administrator shall move the packaged software into the Production environment.
- 18.6.16 The CI List shall be updated after the Packaged Software has been moved into the Production environment as per the Configuration Management Policy.

18.7 General Guidelines:

- 18.7.1 Third-party software (free as well as purchased) required for day-to-day work will be preinstalled onto all company systems before handing them over to employees. A designated person in the IT Department. can be contacted to add to/delete from the list of pre-installed software on organizational computers.
- 18.7.2 No other third-party software – free or licensed can be installed onto a computer system owned or provided to the Stakeholder, without prior approval of the Steering Committee.
- 18.7.3 To request installation of software onto a personal computing device, a Stakeholder needs to send a written request via the IT Ticket System or IT Support Email.
- 18.7.4 Any software developed & copyrighted by the organization belongs to the organization. Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.

18.8 Compliance:

- 18.8.1 No Stakeholder is allowed to install pirated software on official computing systems.
- 18.8.2 Software purchased by the organization or installed on organizational computer systems must be used within the terms of its license agreement.

- 18.8.3 Any duplication, illegal reproduction or unauthorized creation, use and distribution of licensed software within or outside the organization is strictly prohibited. Any such act will be subject to strict disciplinary action.
- 18.8.4 The Procurement Department procedures & guidelines need to be followed to purchase new software (commercial or shareware) for official purposes.
- 18.8.5 Any Stakeholder who notices misuse or improper use of software within the organization must inform his/her Reporting Manager(s).

18.9 Software Registration:

- 18.9.1 Software licensed or purchased by the organization must be registered in the name of the organization with the Job Role or Department in which it will be used and not in the name of an individual.
- 18.9.2 After proper registration, the software may be installed as per the Software Usage Policy of the organization. A copy of all license agreements must be maintained by the IT Department.
- 18.9.3 After installation, all original installation media (CDs, DVDs, etc.) must be safely stored in a designated location by the IT Department.

18.10 Audit:

- 18.10.1 The IT Department will conduct periodic audit in all company-owned systems to make sure all compliances are being met.
- 18.10.2 Prior notice may or may not be provided by the IT Department before conducting Audit.
- 18.10.3 During this audit, the IT Department will also make sure the anti-virus is updated, the system is scanned and cleaned and the computer is free of garbage data, viruses, worms or other harmful programmatic codes.
- 18.10.4 The full cooperation of all Stakeholders is required during such audits.

INCIDENT MANAGEMENT POLICY

19.1 Objective:

- 19.1.1 The term 'incident' in this document means any irregular or adverse event, which occurs in any part of the information system. Well defined Incident reporting responsibilities and procedures will ensure quick and effective response and minimize damage from security incidents, malfunctions and help to monitor and learn from security incidents.

19.2 Incident Management Coverage:

- 19.2.1 Incident management procedures shall cover all types of potential security incidents, including;
- Theft/damage to computer data, hardware equipment and communication network
 - Information system failures and loss of service
 - Illegal access to a system
 - Deliberate denial of service
 - Virus and Worm incidents
 - Errors resulting from inaccurate processing of data
 - Breaches of confidentiality
 - Any mis-happening which is not expected in routine service availability

19.3 Incident Response Team:

- 19.3.1 Any Incident noticed by the Stakeholder shall be escalated to the IT Helpdesk. Help desk shall act as the triage team or first point of contact for incident reporting by end users.
- 19.3.2 A designated team for Incident handling may be invoked using domain (Network, Windows, Unix etc) experts from Network and system administration Team, under the leadership of Network and Infrastructure Head.
- 19.3.3 Depending on the type of security incident, the members of a Security Incident Team can include from any of the following;
- Change Control Board
 - Steering Committee
 - CIO
 - System/IT Administrator
 - Business Process Owner
 - Legal
 - HR Representative
 - Public Relations / Press Office

19.4 Incident handling procedures:

19.4.1 The Incident handling procedure shall cover;

- Incident Categorization and Prioritization
- Analysis and identification of the cause of the incident.
- Initial containment of the Incident Eradication and Recovery.
- Collection of audit trails and similar evidence.
- Communication with those affected by or involved with recovery from the incident.
- Follow up and Documentation.

19.4.2 Incident Follow-up;

- A summary record of each incident shall be maintained by Network Administration Team.
- A summary report of all security incidents shall be submitted to Steering Committee on regular Interval.

19.5 Threat Detection:

19.5.1 To increase chances of detecting and mitigating a threat quickly and efficiently the following techniques shall be used in tandem:

- Security event threat detection technology to aggregate Data from events across the network, including authentication, network access, and logs from critical systems shall be aggregated.
- Network threat detection technology to understand traffic patterns on the network and monitor traffic within and between trusted networks, as well as to the internet.
- Endpoint threat detection technology to provide detailed information about possibly malicious events on user machines, as well as any behavioral or forensic information to aid in investigating threats.

COMPLIANCE

20.1 Objective:

20.1.1 The operation and management of information systems may be subject to contractual and regulatory requirements. The objective of this Policy is to ensure compliance, avoid breaches of any regulatory or contractual requirements resulting in civil or criminal prosecution.

20.2 Use of authorized Software:

- 20.2.1 Only licensed and approved software shall be used and software licenses should be controlled and maintained by the IT Department to ensure compliance. The original copies of licenses should be maintained by the IT Department.
- 20.2.2 Software license conditions, including those of limited use, should be observed at all times and no Stakeholder shall make or use unauthorized copies of software or applications.
- 20.2.3 Use of any other software, without authorization from the Steering Committee is strictly prohibited.
- 20.2.4 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 Steering Committee, except for the purposes of backup.
- 20.2.5 Freeware, Shareware, public domain software shall only be used with approval of Administrator.
- 20.2.6 The IT Department shall conduct periodic reviews of software usages, Laptops and Servers to ensure that no unauthorized software is being used. All software found in violation will be removed immediately. Users found contravening 'software compliance policy may be subjected to disciplinary action.

ADHERENCE TO CONFIDENTIALITY AND PRIVACY LAWS, CYBER LAWS GUIDELINES

- 21.1** Adherence to applicable laws including without limitation Data Privacy laws, Cyber laws etc; and related guidelines that are in force. It shall be responsibility of the Change Control Board to identify applicable country specific regulatory requirement relating to data privacy, electronic transactions etc; and ensure adherence to the same.
- 21.2** It is the responsibility of all Stakeholders to comply with all applicable laws/guidelines issued in this regard. Any violation/non-compliance with applicable laws is a major misconduct and disciplinary proceedings may be initiated against the erring Stakeholder.

ACCEPTABLE USAGE POLICY

22.1 Objective:

- 22.1.1 This section outlines policy for use of the computing systems and facilities. The purpose of these guidelines is to ensure that all Stakeholders viz users (users, support personnel and management) use the computing facilities in an effective, efficient, ethical and lawful manner.

22.2 Internet and Email Usage Policy:

- 22.2.1 Following is a inclusive list of activities which are considered improper and hence prohibited:
 - 22.2.1.1 Creating, accessing, downloading, or transmitting messages or images that are lewd, obscene or pornographic, disparaging, offensive or harassing due to their reference to race, sex, age, marital status, religion, nationality, physical or mental disability etc. and may be considered inappropriate in the workplace.
 - 22.2.1.2 Spreading “chain mail” and other such frivolous communications. sing e-mail, the Internet or any other communication tool / media to harass, intimidate or annoy other persons including co-workers.
 - 22.2.1.3 Accessing any software for on-line computer games or using official mail ID for registering with websites (e.g. news sites).
 - 22.2.1.4 Using the computer equipment and software to conduct personal business/transactions.
 - 22.2.1.5 Accessing and/or trying to access IT systems for which the user does not have any access.
 - 22.2.1.6 Downloading, copying or transmitting software and/or documents protected by copyright. Any employee with a question concerning a copyright issue should contact the System Administrator.
 - 22.2.1.7 Downloading any other software or materials (such as on-line publications) unless such download has been appropriately approved and / or have subscribed for organization wide use.
 - 22.2.1.8 Introducing computer viruses, worms, or Trojan horses.
 - 22.2.1.9 Using the system to solicit for commercial ventures, religious or political causes, outside organizations or other unofficial solicitations.
 - 22.2.1.10 Using the IT systems to send or receive confidential information copyrighted materials, trade secrets, proprietary financial information or similar materials without prior authorization.
 - 22.2.1.11 Using a code, access a file, or retrieve any stored information unless authorized to do so.
 - 22.2.1.12 Accessing message(s) to which an employee is not the intended recipient or sending message(s) under someone else’s name.

22.3 Desktop Usage Guideline

- 22.3.1 PCs / Laptops are provided to the users for business purposes and for enhancing their productivity and effectiveness in discharging their duties.
- 22.3.2 PCs should be protected by passwords and should be logged off when left unattended.
- 22.3.3 Unauthorized software should not be installed on the system from any source such as the Internet, or personal CDs, floppies etc.
- 22.3.4 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 computing system or even spread to other systems on the network.
- 22.3.5 Computing systems should be shut down at the end of the day's work for security reasons and also to save power.
- 22.3.6 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.
- 22.3.7 Users shall never disable Antivirus software, backup, or asset software.
- 22.3.8 If users suspect any infection to the system by virus or malicious contents, they must immediately shutdown the computer, disconnect it from the network, and report the same to the IT Helpdesk.

22.4 Portable computing/Laptop Security:

- 22.4.1 Portable computers and software are issued for business purposes only.
- 22.4.2 Stakeholder shall be responsible for the equipment, software and regular backing up of data at the Office Server.
- 22.4.3 Upon request User shall immediately return any allocated Assets in good working order (unless it is being returned because of a malfunction) along with all documentation, software and configurations

22.5 Password Security:

22.5.1 It shall be the responsibility of the individual Stakeholders who have been allotted the Asset, to secure the Asset with a strong and effective password to avoid any unauthorised access to Information system.

22.5.2 Users shall:

- 22.5.2.1 Never use easy to guess passwords and create strong password as per the password policy
- 22.5.2.2 Never share or write password or store or use option of save password in clear text
- 22.5.2.3 Always change the initial password immediately after first login and thereafter at regular intervals.
- 22.5.2.4 Be responsible for any transaction made through their official ID's.
- 22.5.2.5 Any violation of the above is a major misconduct and disciplinary and/or legal proceedings may be initiated against the concerned Stakeholder.

22.6 General Usage guideline:

- 22.6.1 The computer systems, messaging systems e-mails and all information and intellectual property vested therein is the absolute property of INOXCVA Limited. Any intellectual property rights on any work products, arising from out of the association of the Stakeholders is "Work for Hire".
- 22.6.2 The company's IT systems are to be used by the employees strictly for official business purposes.
- 22.6.3 The company reserves the right to monitor/record all information and revoke the privilege of use of the computing systems temporarily or permanently in the interest of the organization.
- 22.6.4 If it is found that the Assets have been intentionally, or otherwise misused or attempted to have been misused, tampered with or manipulated, the Organization shall initiate appropriate disciplinary/legal actions on concerned Stakeholders.
- 22.6.5 The IT Assets provided to individuals shall be for Business/Official Use, and would have to be returned to the IT Department during separation from the organization, or transfer or whenever a new asset is provided to the Users.
- 22.6.6 All files should be secure at all times. When users leave work area it is recommended to;
 - Clear all classified information from desktop
 - Use a screen Lock on PC or Laptop
 - Lock up laptop either in a drawer or take it with himself when leaving office.

- 22.6.7 Any non-compliance of these requirements is a security violation and a major misconduct and shall be immediately reported to IT helpdesk and the relevant HOD. Disciplinary/legal proceedings may be initiated against the erring Stakeholder.

CAPACITY PLANNING AND PERFORMANCE MANAGEMENT POLICY

23.1 Objective:

23.1.1 The objective is to ensure cost justifiable capacity for all Assets like;

- Hardware
- Networking Equipment (LANs, WANs, bridges, routers)
- Peripherals (bulk storage devices, printers)
- Software (OS, network Software, purchase/in-house)
- Skilled People

23.2 Guidelines:

- 23.2.1 Change Management Board shall be responsible for overall capacity and performance management.
- 23.2.2 While implementing new network services a performance and capacity planning with list the business functions, nature of transactions, frequency of execution, their type and importance shall be evaluated.
- 23.2.3 Requirements for performance in terms of response time, transactions, number of users, required resources and capacity or any other significant work unit shall be clearly defined and formally approved by Change Management Board.
- 23.2.4 System resource utilization and service performance shall be monitored regularly by Steering Committee.
- 23.2.5 Identified critical systems and parameters like Throughput (Volume & Utilization), CPU Utilization, Memory Utilization, File storage utilization, Bandwidth utilization, Threshold etc; shall be monitored and reviewed periodically.
- 23.2.6 System shall be configured to automatically generate alerts whenever system resource utilization goes beyond the defined threshold.
- 23.2.7 All alerts shall be communicated to a separate IT Helpdesk and System Administrator shall be responsible for regular monitoring of system resource utilization.
- 23.2.8 Steering Committee shall prepare a quarterly summary report of system utilization for review of the Change Control Board.
- 23.2.9 A quarterly capacity plan shall be drafted based on documented current levels of resource utilization and service performance and factors in business strategy and

plans by the Steering Committee with Forecast future requirements for IT resources and developed quantifiable recommendations.

23.2.10 In case of significant high utilization of system resources, resulting in service performance degradation Steering Committee shall be immediately communicated and necessary remediation steps shall be taken.

23.2.11 Steering Committee should also communicate capacity plan to HR.

BUSINESS CONTINUITY PLANNING POLICY

24.1 Objective:

24.1.1 A separate Business Continuity Plan is required to cater to the operational aspect of Crisis Planning. Potential natural disasters like earthquakes, severe storms, flooding, etc. or disruptive acts deliberately caused by man (virus attack, bombings, riots and theft) or technical glitches like, server crash etc., could lead to significant disruption of business, if recovery measures are not planned in advance.

24.1.2 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 of time and ensure continuity of business functions during such Crisis.

24.2 Project Initiation:

24.2.1 CFO shall prepare the Scope and Objectives of the Business Continuity and Crisis Management initiative.

24.2.2 The Change Control Board will review the same. Once approved IT Steering Committee shall identify Crisis Management Lead (CML) for different locations.

24.2.3 The individual Crisis Management Lead (CML) for the location shall identify BCP team for each location, including the corporate office.

24.3 Risk Assessment:

24.3.1 Risks related to all Assets shall be Identified and evaluated by the BCP team at each location. The probability of risk occurrence and the impact of risk must be determined.

- 24.3.2 A detailed threat analysis shall be conducted for the business processes, including prioritization of risks or threats, identification of possible vulnerabilities and existing mitigation for each location.
- 24.3.3 The Risk Analysis for each location must be reviewed by the Steering Committee.

24.4 Business Impact Analysis:

- 24.4.1 The BCP team at each location, in consultation with the Business Process Owners, shall conduct a Business Impact Analysis for the individual location.
- 24.4.2 The Business Impact Analysis shall consider the impact of the function or unit on business and business restoration possibility.
- 24.4.3 The Business Impact Analysis for each location must be reviewed by the Steering Committee.
- 24.4.4 The Steering Committee shall put up a detailed report for the approval of the Change Control Board.

24.5 Strategy Selection:

- 24.5.1 The BCP team at each location shall compile the resource requirements for hardware, software, utilities, data, supplies etc for Business Continuity.
- 24.5.2 The BCP team at each location shall identify IT Recovery Strategy to meet Max Tolerable Downtime/Recovery Time Objective.
- 24.5.3 The BCP team at each location shall identify an alternate location for the Primary location(s) hosting the Mission Critical Applications.
- 24.5.4 The BCP team at each location must identify the Remote storage strategy at the Alternate location. The possible strategies (but not limited to) can be:
- Electronic Vaulting
 - Remote Journaling
 - Database Shadowing
 - Mirroring
- 24.5.5 The IT recovery strategy, alternate location and the Remote storage strategy must be reviewed and approved by the Change Control Board.

24.6 Plan Development:

- 24.6.1 The CML at each location shall identify a two level recovery organization (i.e. crisis management team and a facility recovery team) for each of the locations. The roles and responsibilities of the team must be clearly defined.
- 24.6.2 A separate BCP and the maintenance procedures shall be prepared at each location by the BCP team at the location.
- 24.6.3 The Business Continuity Plan must encompass all aspects of the organization like:
- Personnel
 - Facility
 - Infrastructure
 - Information and Support Systems
- 24.6.4 BCP shall be updated whenever (but not restricted to) any of the following event occur:
- Change in criticality of any business functions
 - Change in the personnel responsible for crisis management
 - Change in the risk profile of any of the enablers to the business functions
- 24.6.5 The BCP for each location shall be Reviewed and Approved by the IT Steering Committee on a periodic basis.

24.7 Testing and Maintenance:

- 24.7.1 The BCP at each location shall organize periodic Mock Disaster Recovery drill to test as per the test calendar. The Mock drills can be Planned as well as Unplanned.
- 24.7.2 The test calendar shall be reviewed and approved by the IT Steering Committee.
- 24.7.3 Any discrepancy or gaps shall be noted and the BCP updated accordingly shall be put up for review of Change control Board by the Steering Committee.
- 24.7.4 BCP at each location shall plan and conduct the BCP Training for all members of the Crisis Management, Facility recovery and Business Continuity team on a periodic basis.

THIRD PARTY AND OUTSOURCING SERVICES POLICY

25.1 Objective:

- 25.1.1 This policy is aimed at providing a framework and guidelines for identification and management of Third Party and Outsourcing Services. This shall include out sourcing of IT services, Cloud Services, annual maintenance contract (AMC), IT Audit engagements, out sourced software development and implementation etc.

25.2 Vendor Evaluation and Selection:

- 25.2.1 Any Third Party and Outsourcing Services Contract shall be awarded after completion of the Vendor Evaluation and Selection process.
- 25.2.2 The Vendor Evaluation shall be based on (but not limited to) response to RFP/RFQ/RFI, Technical capabilities, Vendor References, Site Visits, Comparative Analysis between Vendors, Market Intelligence etc as applicable.
- 25.2.3 Security requirements shall be considered while finalizing any vendors and vendor shall be audited for their security practices.
- 25.2.4 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.

25.3 Contract:

- 25.3.1 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 of time) or Project/Deliverable based.
- 25.3.2 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 shall rest with the Third Party Manager.
- 25.3.3 The formal contract 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.
- 25.3.4 Risks associated with outsourcing shall be assessed and appropriate security controls need to be formulated into the contract. This needs to be signed by the Third Party and Outsourcing service provider.
- 25.3.5 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.
- 25.3.6 The formal contract must be reviewed and approved by the Legal Department. For outsourcing of major IT services, approval of the Change Control Board shall be obtained.

- 25.3.7 INOXCVA Limited shall have the right to audit contractual responsibilities of the Third Party and Outsourcing Services provider at any given point of time during the period of the contract.
- 25.3.8 The Third Party and Outsourcing Services provider must take explicit permission of the Third party Manager to involve any subcontractors for the fulfilment of the contractual responsibility.
- 25.3.9 INOXCVA Limited shall own all the right to any intellectual property arising from collaborative work with the Third Party and Outsourcing Services provider like development of software etc., as “Work Made for Hire”.

25.4 Service Level Agreement:

- 25.4.1 Service Level Agreement (SLA) or Warranty details shall be agreed upon in writing with the Third Party and Outsourcing Services provider.
- 25.4.2 The Service Level Agreement must consider the following parameters
- Service description
 - Roles and Responsibilities
 - Service Level (Metric)
 - Service Level (Value per Metric)
 - Pricing table (if applicable)
 - Rewards and Penalties (if applicable)
 - Review Frequency
- 25.4.3 The SLA shall be defined based on the expected or desired Performance level, Number of Resolutions, On-time delivery, Rework Percentage etc.

25.5 Security and Operations:

- 25.5.1 Third Party and Outsourcing Services provider must sign the Non-Disclosure Agreement (NDA) if they are exposed to any confidential data or information before they initiate work.
- 25.5.2 The access by the Third Party and Outsourcing Services provider shall be on need-to-know basis and shall be logged, tracked and audited on periodic basis.
- 25.5.3 Necessary Documentation must be maintained for documents and information shared and activities conducted.

- 25.5.4 The document and information must be returned and any soft copy document maintained on mobile computing device shall be destroyed on contract expiry or termination.
- 25.5.5 No part of the document, or information provided may be copied without the prior explicit permission of the Steering Committee.
- 25.5.6 During the period of the Contract, it is the responsibility of the Third Party and Outsourcing Services provider to protect any document or information provided to them against loss, theft or misuse. Any such incident must be immediately reported to the Third Party Manager.

25.6 Review and Monitoring;

- 25.6.1 If the services provided by the Third Party and Outsourcing Services have been segregated into phases (namely, in cases of Application Maintenance, Application Development, Consulting etc), then all phases must be reviewed and approved before moving onto the next phase activities.
- 25.6.2 The Third Party Manager on a monthly basis would review the Performance and SLA Compliance.
- 25.6.3 Periodic review meetings must be conducted with the Third Party and Outsourcing Services provider to assess the performance and SLA Compliance.
- 25.6.4 The Minutes of the Meeting must be documented for review of the Change Control Board before publishing to relevant stakeholders.

25.7 Contract Expiry:

- 25.7.1 Contract Closure details must be documented on expiry of the Contract. A closure meeting must be conducted with all relevant stakeholders.
- 25.7.2 The Steering Committee shall review the Contract Closure details.
- 25.7.3 The respective department head department shall be communicated on expiry of the Contract.

25.8 Renewal and Modification of Contract:

- 25.8.1 Any contract with a Third Party and Outsourcing Services provider can be modified upon mutual agreement A New Contract and SLA or an Addendum can be added to the old Contract.
- 25.8.2 New Purchase Order must be generated on any Contract Renewal.
- 25.8.3 Any modification of the contract must be reviewed and approved by the Change Control Board

IT AUDIT POLICY

26.1 Objective:

26.1.1 The scope of this policy is to establish a mechanism for facilitating Information Systems Audit at on a periodic basis, with an objective to ensure the following.

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

26.2 Guidelines:

26.2.1 An external or independent internal authority shall conduct IT Audit as may be determined on an annual basis or as and when the Change Control Board perceives any such need.

26.2.2 The CIO and the IT Steering Committee shall decide on the mode of audit (external or independent internal authority).

26.2.3 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'.

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

26.2.5 The various types of Information Systems Security Audit shall include the following:

- IS Strategy & Policy
- IT Security Policy
- Application Systems
- Vulnerability Analysis and Penetrative Testing of 'INOXCVA LIMITED GROUP' Networks
- Technology & Infrastructure Audit
- Business Continuity Planning including Demonstrated Recovery & General Computer Controls Environment

26.2.6 The Steering Committee or designate shall be responsible for coordinating with the Auditor(s) for the purpose of the Audit.

26.2.7 Any required access to systems, documents, information for the Auditor(s) shall be provided as per the 'Security and Operations' Policy.

26.2.8 IT Audit should be done as per best practice guidelines like ISACA, ITIL, etc.

- 26.2.9 System audit tools can be used for the purpose of Audit. Any System Audit Tool that is used shall be adequately protected to prevent any misuse.
- 26.2.10 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.
- 26.2.11 The IT Audit results and findings should be documented and submitted to the IT Steering Committee, who in turn shall present the audit findings to the Change Control Board.
- 26.2.12 The Steering Committee shall be responsible for ensuring implementation of corrective actions for gaps identified by the Audit.
- 26.2.13 A roadmap defining the timeframe for closing all gaps must be prepared and presented by the Steering Committee to the Change Control Board within a month of the submission of the Audit Report.
- 26.2.14 The Change Control Board shall review the compliance status of agreed remedial action in order to close the gaps identified in the Audit.
- 26.2.15 All Audit Reports shall be stored for retention requirement.

CHANGE AND PROBLEM MANAGEMENT

27.1 Objective:

- 27.1.1 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 and continuity of operations is not compromised.
- 27.1.2 Problem management is aimed at providing timely and satisfactorily addressing and resolving issues related to usage of IT resources by end users.

27.2 General Guidelines:

- 27.2.1 This policy defines the process for enacting changes on the IT infrastructure including application software, system software, networking resources and computer hardware.
- 27.2.2 This section addresses policies relating to the following:
- Application change management
 - Infrastructure Change Management
 - Problem Management

27.2.3 Changes are categorized into three major types as follows;

27.2.3.1 Major changes

- Any change request is considered as a major change if the change has 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.

27.2.3.2 Minor changes

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

27.2.3.3 Emergency Change

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

27.3 *Application Change Management:*

27.3.1 This policy is aimed at covering Request 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.

27.3.2 Change Request

27.3.2.1 Change Requests maybe initiated by any “key” application user or the application owner within the IT Department. “Key” application user is defined as process lead, module lead, Departmental Head and Business Unit Head.

27.3.2.2 All Change Request must come either in Change Request Form or on Mail having proper justification for defined but not limited to following parameters

- Change Request in specific Applications, Modules, Business Process, Business Sub-process
- Change Requet Description
- Change Request Need
- Business Impact / Benefits
- Financial Impact
- Change Catagory
- Priority

27.3.2.3 All Change Requests should be signed by Request Originator and approved by respective Line Managers and Business Process Owners.

27.3.2.4 Change Requests shall be processed based on prior approval from the change Control Board.

- 27.3.2.5 All change Requests shall be analyzed from the perspective of business impact in terms of time and efforts as well as security considerations.
- 27.3.2.6 Emergency change requests can be authorized by the Steering Committee.
- 27.3.2.7 Impact Analysis
- 27.3.2.8 Potential impact of any change on other applications or systems, or on other modules in the same application shall be assessed from risk perspective before accepting a change request.

27.3.3 Source Code Management

- 27.3.3.1 There shall be single repository for production source code management for modifying programs
- 27.3.3.2 The details of this is mentioned as part of the 'Configuration Management' Policy
- 27.3.3.3 Only an authorized system administrator shall have update access to the production source code

27.3.4 Testing

- 27.3.4.1 All changes made to the applications / systems should be thoroughly tested before deployed in to production environment. This shall be applicable only for all major changes.
- 27.3.4.2 The IT Change Manager shall determine the Testing strategy to be adopted for Change Requests. The testing process would cover the following types of tests;
 - Unit Testing
 - System/Integration Testing
 - User Acceptance Testing
- 27.3.4.3 The User Acceptance testing shall be mandatory in any situation while the applicability of other tests shall be determined, as discussed above.

27.3.5 Unit Testing

- 27.3.5.1 Prior to installation in production, all application changes shall undergo Unit Test with pre-designed test data sets (which can cover all the test scenarios) in a separate test environment locked against any modification.
- 27.3.5.2 Unit test results shall be documented and kept for reference.
- 27.3.5.3 Changes to the application carried out as a result of the testing shall be subject to appropriate re-testing procedures.
- 27.3.5.4 The IT Change Manager shall perform an independent review of unit test results.

27.3.6 System/Integration Testing

- 27.3.6.1 Prior to installation in production, all application changes shall undergo system/integration test with pre-designed test data sets (which can cover

all the test scenarios) in a separate test / quality environment that shall be currently refreshed from production and shall be locked against any modification.

- 27.3.6.2 Changes to the application carried out as a result of the testing shall be subject to appropriate re-testing procedures.
- 27.3.6.3 The IT Change Manager shall perform an independent review of System/Integration test results.
- 27.3.6.4 Integration test results shall be documented and kept for future reference.

27.3.7 User Acceptance Testing

- 27.3.7.1 Prior to installation of the software in production and based on an approved UAT Test plan documenting the test scenarios and expected outcomes, UAT Testing with pre-designed test data sets (which can cover all the test scenarios) shall be conducted by the “user” team, in a test / quality environment locked for any modifications.
- 27.3.7.2 Changes to the application carried out as a result of the testing shall be subject to appropriate re-testing procedures.
- 27.3.7.3 User Acceptance test results shall be documented and kept for future reference.
- 27.3.7.4 The Head of the Business Unit must sign-off acceptance.

27.3.8 Deployment

- 27.3.8.1 Only a System or Database Administrator shall have write access in the Production environment and can update the production source code.
- 27.3.8.2 A formal User Acceptance sign-off shall indicate the requirement to move the source code into Production.
- 27.3.8.3 For major changes Deployment Plan and the Release Note shall be used for moving the source code to Production.
- 27.3.8.4 The exceptions encountered in Deployment shall be logged and monitored.

27.3.9 Retention Requirements

- 27.3.9.1 All Change Request Forms, Test Plans, User Acceptance and Deployment Plan would be retained for future reference.
- 27.3.9.2 The current version and two prior production versions of each application shall be retained. All prior versions shall be archived to backup media. The details of the backup Process is mentioned in the Policy for ‘Backup and Recovery Management’.

27.3.10 Review and Monitoring

- 27.3.10.1 Change requests must be adequately documented.
- 27.3.10.2 All Change Requests (including Emergency Change Requests) must be reported to the Change Control Board through the Steering committee on a periodic basis for monitoring and review.

27.3.10.3 This review frequency is detailed in the change management procedure document.

27.3.11 Emergency Changes

27.3.11.1 Emergency changes can be made only by persons authorized by the Steering committee on prior notification to the Change Control Board.

27.3.11.2 All emergency changes shall be documented in an incident or trouble log within 24 hours of the change being effected and should include the time and date of changes, commands executed, program or data affected etc.

27.3.11.3 The completed documents shall be submitted to the Change Control Board for approval.

27.3.12 Configuration Management

27.3.12.1 After the completion of the change management process, all related documents, software codes and versions shall be updated in the configuration management database as per the configuration management Policy.

27.4 Infrastructure Change Management Policy:

27.4.1 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).

27.4.2 The activities pertaining to Infrastructure Change Management include applying hot fix or patch, new network software installation, change of system values, operating system changes, server configuration changes, hardware changes, and changes in database settings.

27.4.3 Application of Patches to Application Software like ERP, Lotus Notes, 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

27.4.4 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.

27.5 Change Initiation:

- 27.5.1 Any Infrastructure Change Requests can only be initiated by the Change Control Board.
- 27.5.2 All Infrastructure Change Requests shall be segregated as Normal Requests or Emergency Requests.
- 27.5.3 All Normal (non-emergency) infrastructure changes must follow the Change Control Procedure outlined as part of the SOPs.
- 27.5.4 All emergency infrastructure changes must follow the Emergency Change Control Procedure outlined as part of the SOPs.

27.6 Change Impact:

- 27.6.1 Potential impact of any change shall be assessed from risk perspective before accepting a change request.
- 27.6.2 Any Changes that shall be carried out must not hamper the security of existing systems or cause any security failure.

27.7 Change Approval:

- 27.7.1 Any Major Change like security (i.e. file permissions, identification and authentication, and discretionary access control) must have a prior approval of the Change Control Board.
- 27.7.2 Emergency change requests can be carried out if deemed fit by the Steering Committee on prior notification to the Change Control Board.

27.8 Change Execution:

- 27.8.1 All Changes in the Production environment shall be announced to the intended audience before and after the implementation.
- 27.8.2 A Change Execution/Implementation Plan should be prepared for all Change Requests.
- 27.8.3 For upgrades, patches and other items provided by 3rd party suppliers, the installation instructions must be followed to implement the change.
- 27.8.4 The roll back plan for unsuccessful changes/implementations should be prepared before implementation.

- 27.8.5 Only System, Network or Database Administrator can implement the change on the Approval of Change Control Board or the Steering Committee as the case may be.
- 27.8.6 Change requests that may have 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.
- 27.8.7 Patches shall be scheduled as batch processes following the normal Infrastructure Change Management process. No automatic updation shall be scheduled on any servers in the Data Centre.
- 27.8.8 Security incident management procedure shall be adhered as per the Security Policy, for possible security issues observed in the change.
- 27.8.9 Suitable version control and a change register shall be maintained for all changes as per the 'Configuration Management' Policy.

27.9 Testing of Change:

- 27.9.1 Test Plan shall be prepared before implementing any Infrastructure Change.
- 27.9.2 All Infrastructure Changes (like application of Patches, Configuration Changes) should be tested in the test environment before Application in the Production environment.
- 27.9.3 Exceptions to this requirement shall be recorded and maintained in those cases wherein the testing is not feasible.

27.10 Review and Monitoring:

- 27.10.1 Change requests must be adequately documented.
- 27.10.2 All Change Requests (including Emergency Change Requests) must be reported to the Change Control Board on a periodic basis for monitoring and review.
- 27.10.3 This review frequency is detailed in the change management procedure document.

27.11 Emergency Changes:

- 27.11.1 Emergency changes can be performed only after authorization of the Steering Committee on prior notification of the Change Control Board.
- 27.11.2 All emergency changes shall be documented in an incident or trouble log within 48 hours of the change being effected with time and date of changes, commands executed, program or data affected etc.

27.11.3 The completed documents shall be submitted to the Change Control Board.

27.12 Configuration Management:

27.12.1 After the completion of the change management process, all related documents, Hardware/, Patch/system software changes and versions shall be updated in the configuration management database as per the configuration management Policy.

ISSUES MANAGEMENT POLICY

28.1 Objective:

- 28.1.1 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.
- 28.1.2 Any problem or issue 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 are covered in scope of this Policy and the corresponding Procedure.
- 28.1.3 Any Problem / Issue resulting in Application / Infrastructure Change request shall be managed as per the Change Management Policy for Application and Infrastructure respectively.

28.2 Problem Management:

- 28.2.1 A helpdesk function shall be maintained for Issue or Problem Resolution.
- 28.2.2 The helpdesk function shall be available during office or business hours.
- 28.2.3 Any Stakeholder can initiate a request for Issue or Problem Resolution through online ticketing system or an email to IT Helpdesk.
- 28.2.4 A Unique ID shall be generated for all Requests for Tracking and Monitoring.
- 28.2.5 The requestor needs to submit all details related to the Problem while raising the Request.

- 28.2.6 Any Problem Requests, unresolved within the permissible turnaround time, shall be escalated as per the escalation procedure.
- 28.2.7 All Request details shall be formally recorded and documented for retention requirements.
- 28.2.8 Periodic exception based reporting shall be carried out to steering Committee for monitoring and review.
- 28.2.9 If any request for issue or problem resolution has been raised which involves change management, then a Separate Change Request has to be raised for the same.

CONFIGURATION MANAGEMENT POLICY

29.1 Objective:

- 29.1.1 This document aims at ensuring uniformity in managing and controlling the changes in versions of application systems, ERP system and customized add- on modules, network and operating system software, interfaces and utilities including related documentation.

29.2 Configurable Item Identification:

- 29.2.1 All individual items of computer hardware and network components, each instance of system software, 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.
- 29.2.2 All Configurable Items (CIs) must be identified, named based on a pre- defined naming convention and a Configuration List shall be maintained.

29.3 Document Configuration:

- 29.3.1 In the event of creation or updation of a document that pertains to any of the identified configurable items, the CI List must be updated along with Document History/Revision Trail with the changes made.
- 29.3.2 A formal review and approval shall be required before releasing any document.
- 29.3.3 A standard numbering scheme shall be used for all documents.

29.3.4 All documents must be archived as per a defined frequency.

29.4 Software Configuration Management:

29.4.1 Custom-developed software

29.4.2.1 All software application source codes shall be kept under version control.

29.4.2.2 The Configuration Manager shall checkout the application source code for changes.

29.4.2.3 On completion of the change (after successful testing and sign-off), the correct version of the application source code shall be Checked In by the Configuration Manager.

29.4.2.4 The new version of the application code shall be appropriately rolled-out at all locations within the agreed time frame.

29.5 Packaged Application Software:

29.5.1 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.

29.5.2 In case maintenance of application 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.

29.6 Infrastructure and System software:

29.6.1 All Servers, Network components and other peripheral devices specifications shall be defined as a Configurable item (CI) and updated in the configuration management database.

29.6.2 The details for each CI shall include but not limited to;

- Hardware specifications
- System details (e.g. version, patch level etc.)
- Configuration details (e.g. Router, firewall configuration file)

29.6.3 Detailed documentation shall be maintained for installation of all patches, updates and upgrades received against a version of operating system and other system software.

29.6.4 Any changes/upgrade to specifications shall be updated in the Configuration Management Database within 48 Hour of the change made.

29.7 Access and Review:

- 29.7.1 The Configuration Manager shall manage the access to the baseline configuration.
- 29.7.2 Access to change and manage baseline configurations should be restricted to the Configuration Manager/Corporate IT Head.
- 29.7.3 The Steering Committee shall periodically generate and review reports relating to the changes in Configurable Items such as (but not limited to) Version Changes Status report and Check-in and Checkout statistics Report.

29.8 Disposal:

- 29.8.1 Obsolete documents shall be identified as "Superseded" in the CI List and shall be removed from the point of use but shall be kept for reference and retention requirement.
- 29.8.2 The CI List must be updated on expiry of any Software License.
- 29.8.3 No stakeholder can use an expired Software license.
- 29.8.4 The CI List must be updated on disposal of the CI Items.

30. User Access Management Process

30.1 User Account Creation

- New users require formal approval from their line manager and IT Security Officer.
- HR notifies IT of new hires, and accounts are created based on job role and department.
- Unique user IDs are assigned to all employees.
- Multi-Factor Authentication (MFA) is enabled where applicable.

30.2 Access Review and Modification

- User access rights must be reviewed periodically (at least every six months).
- Any changes in job roles require an access review and approval from line managers.
- Unused or dormant accounts are disabled after 90 days of inactivity.

30.3 User Account Termination

- HR notifies IT of employee resignations, terminations, or contract expirations.
- IT disables or deletes accounts within 24 hours of termination.
- Access to physical and digital assets is revoked immediately.

30.4 Privileged Access Management (PAM)

- Administrative access is granted only to authorized personnel based on approval.
- Privileged accounts must be used only when necessary and monitored closely.
- Access logs must be reviewed regularly to detect unauthorized activities.

30.5 Access Control for Third Parties

- Vendors and third-party service providers must sign an NDA and adhere to access control policies.
- Temporary access is granted for a defined period and reviewed regularly.

- Remote access for third parties is secured via VPN and MFA.

30.6 Monitoring and Logging

- All user access and activities must be logged and monitored for anomalies.
- Unauthorized access attempts must be investigated and reported immediately.
- Audit logs should be retained for at least 12 months for security and compliance purposes.

30.7 . Incident Management

Any suspected unauthorized access must be reported to the IT Security Officer.

Incident response procedures must be followed to mitigate risks.

Affected accounts must be reviewed and corrective actions taken.

EXCEPTION

30.1 Objective:

- 30.1.1 There may be occasions wherein there may be exigent business requirement justifying deviations from the Policy. In order to provide flexibility in these instances, there is an "Exception to Policy". The "exceptions" will take effect only upon obtaining the prior approval of the concerned authority.

30.2 General Guidelines:

- 30.2.1 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 Change Control Board. Once approved, exceptions to policy will be valid for a pre-decided period after which it must be re-evaluated and re-approved.
- 30.2.2 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 shall be convinced and approve the arrangements to put in place the mitigating or compensating controls.

31.0 Patch Management Policy

31.1 Purpose

This Patch Management Policy establishes the requirements for maintaining up-to-date operating systems, applications, and security software on all information systems within the organization. This policy is designed to minimize the exposure to vulnerabilities associated with outdated software and to comply with ISO 27001 requirements, specifically control A.12.6.1 (Management of technical vulnerabilities).

31.1.2 Scope

This policy applies to all information systems owned, operated, or managed by the organization, including:

- Servers (physical and virtual)

- Workstations and laptops
- Network devices (routers, switches, firewalls)
- Mobile devices (if managed by the organization)
- Applications (commercial and in-house developed)
- IoT devices
- Cloud services and infrastructure

31.2. Policy Statement

The organization shall implement systematic procedures to identify, evaluate, test, and apply security patches to all applicable information systems in a timely manner to protect against known vulnerabilities while minimizing operational disruption.

31.3. Roles and Responsibilities

31.3.1 IT Department

- Maintain an inventory of all systems requiring patch management
- Monitor vendor announcements for relevant security updates and patches
- Classify and prioritize patches based on risk assessment
- Test patches in a non-production environment before deployment
- Apply patches according to defined schedules
- Document all patch management activities
- Report on patch compliance status

31.3.2 System Owners

- Approve patch implementation schedules for their systems
- Coordinate with IT Department for system availability during patching windows
- Validate system functionality after patch implementation

31.3.3 Information Security Team

- Review and approve patch management procedures
- Monitor compliance with this policy
- Assess residual risks for systems that cannot be patched
- Approve exception requests

31.3.4 Users

- Allow their devices to receive patches when prompted
- Report any system issues that may be related to patches

31.4. Patch Management Process

31.4.1 Vulnerability Monitoring and Patch Identification

- Establish procedures to regularly monitor vendor security bulletins, advisories, and update notifications
- Subscribe to relevant security mailing lists and vulnerability notification services
- Utilize automated vulnerability scanning tools to identify systems requiring patches
- Maintain a centralized repository of applicable patches

31.4.2 Risk Assessment and Prioritization

Patches shall be prioritized based on:

- Criticality of the vulnerability (CVSS score or equivalent)
- Exploitation potential and availability of exploits
- Applicability to the organization's environment
- Potential impact on business operations
- Regulatory compliance requirements

31.4.2.1 Patch Priority Levels

1. **Critical:** Must be applied within 48 hours of release (or sooner if actively exploited)
2. **High:** Must be applied within 7 days of release
3. **Medium:** Must be applied within 30 days of release
4. **Low:** Must be applied within 90 days of release

31.4.3 Testing and Validation

- All patches must be tested in a non-production environment before deployment to production systems
- Testing should verify:
 - Patch installation success
 - System stability
 - Application functionality
 - Performance impact
- Document test results and obtain approval before production deployment

31.4.4 Implementation

- Schedule patch implementation during defined maintenance windows whenever possible
- Notify affected users and stakeholders prior to implementation
- Implement patches using automated tools where feasible
- Perform staggered rollouts for critical infrastructure
- Maintain backup or rollback capability in case of issues

31.4.5 Verification

- Verify successful patch implementation through:
 - Patch management system reports
 - Vulnerability scans
 - System logs
 - Manual verification where necessary
- Document verification results

31.4.6 Emergency Patch Management

For critical vulnerabilities with high exploitation risk:

- Expedited assessment and testing process
- Potential for implementation outside regular maintenance windows
- Special approval process for emergency deployment
- Post-implementation review

31.5. Exceptions

31.5.1 Exception Process

- Exceptions to this policy must be formally requested via the Exception Request Form
- Requests must include:
 - System identification
 - Reason for exception
 - Risk assessment
 - Compensating controls
 - Timeframe for exception
- All exceptions must be approved by the Information Security Manager and documented

31.5.2 Compensating Controls

Systems that cannot be patched due to operational constraints must implement compensating controls, which may include:

- Network segmentation
- Enhanced monitoring
- Access restrictions
- Virtual patching at network level
- Additional security controls

31.6. Documentation and Reporting

31.6.1 Required Documentation

- Patch inventory
- Test results
- Implementation records
- Exception records
- Patch compliance status

31.6.2 Reporting

- Monthly patch compliance reports to IT Management
- Quarterly patch status reports to the Information Security Committee
- Ad-hoc reporting for critical vulnerabilities

31.7. Compliance Measurement

Compliance with this policy will be measured through:

- Regular vulnerability scans
- System audits
- Patch management system reports
- Security incident reviews

Non-compliance may result in increased security risks and potential disciplinary action.

31.8. Policy Review

This policy shall be reviewed annually or when significant changes occur to ensure its continued suitability, adequacy, and effectiveness.

31.9. Related Documents

- Information Security Policy
- IT Policy
- Change Management Policy
- Risk Management Policy
- IT Asset Management Policy
- Security Incident Management Policy

31.10. References

- ISO/IEC 27001:2013, specifically control A.12.6.1 (Management of technical vulnerabilities)
- ISO/IEC 27002:2022, specifically control 8.8 (Management of technical vulnerabilities)
- Industry best practices for patch management

31.11. Definitions

- **Patch:** A piece of software designed to update a computer program or its supporting data to fix or improve it
- **Vulnerability:** A weakness which can be exploited by a threat actor to perform unauthorized actions

- **CVSS:** Common Vulnerability Scoring System, a framework for rating the severity of security vulnerabilities
- **Compensating Control:** A security control implemented when the primary control cannot be implemented
- **Virtual Patching:** The process of implementing a security policy to detect and prevent exploitation of a vulnerability

32 . Password Management Policy

32 . 1. Purpose and Scope

This Password Management Policy is a sub-policy of the Central IT Policy and establishes requirements for the creation, maintenance, and management of passwords for all information systems within the organization. This policy aims to ensure compliance with ISO 27001 requirements and to protect organizational information assets from unauthorized access.

This policy applies to all employees, contractors, consultants, temporary staff, and other workers including all personnel affiliated with third parties who access organization information systems.

32 . 2. Policy Statement

The organization shall implement robust password management controls to protect information systems and data from unauthorized access while ensuring alignment with ISO 27001 requirements.

32 . 3. Password Requirements

32 . 3.1 Password Creation

- Passwords must be a minimum of 12 characters in length
- Passwords must contain at least one character from three of the following categories:
 - Uppercase letters (A-Z)
 - Lowercase letters (a-z)
 - Digits (0-9)
 - Special characters (e.g., !@#\$%^&*()_+)
- Passwords must not contain easily guessable information (e.g., username, employee ID, name)
- Passwords must not contain common dictionary words or known compromised passwords

32 . 3.2 Password Expiration and History

- Passwords must be changed at least every 90 days
- New passwords must not match any of the previous 12 passwords
- Temporary passwords must be changed upon first login
- Password history shall be maintained for a minimum of 12 previous passwords

32.3.3 Account Lockout

- User accounts shall be locked after 5 consecutive failed login attempts
- Locked accounts shall remain locked for a minimum of 30 minutes or until reset by the IT department
- A notification shall be sent to the IT security team when account lockouts occur

32.4. Password Management

32.4.1 Password Storage

- All passwords must be stored in encrypted form using industry-standard cryptographic algorithms
- Password hashing must use salted hashing techniques
- Clear text storage of passwords is strictly prohibited in any system or application

32.4.2 Password Transmission

- Passwords must only be transmitted over secure, encrypted channels
- Multi-factor authentication (MFA) shall be implemented for all remote access to organizational systems and for access to sensitive information
- Password reset mechanisms must verify user identity through secure methods

32.4.3 System and Service Accounts

- System and service account passwords must be at least 16 characters in length
- These passwords must be changed at least annually or when an administrator with knowledge of the password leaves the organization
- Service account passwords must be stored in a secure password vault with restricted access

32.5. User Responsibilities

32.5.1 Password Protection

- Users must not share passwords with anyone, including IT staff
- Users must not write down passwords or store them in unencrypted electronic files
- Users must not use organizational passwords for personal accounts or services
- Users must report any suspected compromise of passwords immediately to the IT security team

32.5.2 Password Manager Usage

- The organization shall provide an approved password management solution
- Users are encouraged to use the organization-approved password manager for storing passwords
- The password manager's master password must comply with all requirements in this policy

32.6. Exceptions

Any exceptions to this policy must be:

- Documented with a clear business justification
- Approved by the Chief Information Security Officer (CISO)
- Reviewed at least annually
- Accompanied by appropriate compensating controls

32.7. Compliance Monitoring

32.7.1 Regular Assessments

- Regular password audits shall be conducted to verify compliance with this policy
- Automated tools shall be used to identify weak passwords
- Password strength shall be tested regularly as part of the vulnerability assessment program

32.7.2 Enforcement

- Failure to comply with this policy may result in disciplinary action
- Repeated violations may result in revocation of access privileges

32.8. Review and Update

This policy shall be reviewed at least annually or when significant changes occur to ensure continued suitability, adequacy, and effectiveness.

32.9. Related Documents

- Central IT Policy
- Information Security Policy
- Access Control Policy
- Acceptable Use Policy

33.0 ABBREVIATIONS

33.1 Abbreviations used in this document:

LAN	LOCAL AREA NETWORK
OS	OPERATING SYSTEM
MS	MICROSOFT
SOP	STANDARD OPERATING PROCEDURE
IP	INTERNET PROTOCOL
C&F	CLEARING AND FORWARDING
SPOC	SINGLE POINT OF CONTACT
VPN	VIRTUAL PRIVATE NETWORK
HR	HUMAN RESOURCES
DNS	DOMAIN NAME SERVER
OEM	ORIGINAL EQUIPMENT MANUFACTURER
SNMP	SIMPLE NETWORK MANAGEMENT PROTOCOL
ACL	ACCESS CONTROL LIST
ICMP	INTERNET CONTROL MESSAGE PROTOCOL
IDS	INTRUSION DETECTION SYSTEM
DMZ	DEMILITARIZED ZONE
UPS	UNINTERRUPTED POWER SUPPLY
SDLC	SOFTWARE DEVELOPMENT LIFE CYCLE
CI	CONFIGURABLE ITEM
RFP	REQUEST FOR PROPOSAL
RFQ	REQUEST FOR QUOTE
RFI	REQUEST FOR INFORMATION
SLA	SERVICE LEVEL AGREEMENT
NDA	NON DISCLOSURE AGREEMENT
WAN	WIDE AREA NETWORK
CML	CRISIS MANAGEMENT LEAD

MCA MISSION CRITICAL APPLICATION

BCP BUSINESS CONTINUITY PLAN

ISACA INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION

ITIL INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY

Confidential - Internal Circulation Only -

IT POLICY ACKNOWLEDGEMENT FORM

I acknowledge that I have received a copy of the INOX INDIA LIMITED's IT ("Policy"). I have read and understood all my obligations, duties and responsibilities under each principle and provision of the Policy I hereby agree to comply with the requirements outlined in the IT Policy.

If any situation involving a conflict, potential conflict, or perceived conflict of interest or violation of the INOX INDIA Limited IT Policy occurs, I will report it immediately, as documented within this Policy.

I affirm that non-compliance or violation of aforesaid IT Policy (whether wholly or partially) by me shall constitute material breach of terms of my employment and in such eventuality(s), the Company shall be authorized to take disciplinary action against me, including termination of my employment and/or any other legal action as deemed fit & proper by the Company.

I certify that this is a true and correct statement.

Signature: _____
Name: _____
Employee Code: _____
Date: _____