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	18th August 2024	First Version Created	CIO	

	Created by	Approved By
	CIO	CEO
	21-03-2025	21-03-2026

DOCUMENT CONTROL

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

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

Targeted Readership: All Stakeholders

TABLE OF CONTENTS

1. INTRODUCTION

INOXCVA has firmly established itself as a global market leader in the demanding sector of vacuum insulated cryogenic equipment. Our strength lies in designing, engineering, manufacturing, supplying, and commissioning turnkey packaged systems.

We are one of the largest manufacturers of both standard and customized cryogenic equipment, designed for the storage, distribution, and transfer of cryogens across the entire cryogenic temperature range, from 2~200oKelvin (-271 to -73oC). These cryogens include Helium, Hydrogen, Nitrogen, Oxygen, Argon, CO2, N2O, LNG, and Ethylene.
By leveraging our design, modelling, analysis, sourcing, procurement, and manufacturing, expertise we are enabling the mainstreaming of clean energy alternatives such as LNG, liquid hydrogen, and fusion energy.

2. ABOUT THE INFORMATION TECHNOLOGY POLICY

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.

3. IT FUNCTION

Key Objectives:

- Enterprise Application Infrastructure and Systems Operations: To establish, maintain, and enhance enterprise information systems and infrastructure services that support business requirements.
- 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.
- 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.
- 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.
- Emerging Technologies: To identify and evaluate emerging technologies to determine their potential benefit to INOXCVA

4. EQUIPMENT MANAGEMENT POLICY

Objective:

- 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.

5. PERSONAL COMPUTER (PC) STANDARDS

Objective*:*

This policy ensures that all PCs used for official work at INOXCVA follow standard hardware and software configurations approved by the IT department. Hardware standards are designed to maintain optimum productivity, system health, and security, while making it easier to support and troubleshoot devices across the organization.

Software standards support effective system administration, proper license tracking, and consistent technical support. Unauthorized software is not permitted on company devices, and all systems are required to meet the minimum specifications defined by IT. Any deviation from these standards requires prior written approval from the IT department.

6. Removal Media Handling Policy

Objective

The Objective of this policy is to set out principles for ensuring that INOXCVA's removable media handling processes reduce the risk of unauthorized disclosure, modification, removal, or destruction of information stored on removable media and that appropriate disciplinary actions are taken against those who violate this policy.

Scope of Policy

This policy applies to:

a) All INOXCVA employees, contractors, consultants, temporary staff, interns, and personnel affiliated with third parties

b) All locations where information assets are used

c) All INOXCVA, affiliate, or third-party IT resources

d) ALL sensitive/confidential digital or no digital information for which the INOXCVA, affiliates, and/or third parties are in possession

e) All devices connected to INOXCVA, affiliate, or third-party networks.

f) All remote workers

7. Antivirus Management Policy

Objective:

This Objective of 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).

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

8. INTERNET USAGE POLICY

Objective:

This policy provides guidelines to ensure that the company's internet and network resources are used responsibly and primarily for legitimate business purposes. The organization has implemented an internet firewall and monitoring tools to protect the network, and internet activity may be monitored in accordance with applicable laws. Personal use of the internet is discouraged during work hours and should not involve downloading unauthorized software, visiting harmful websites, or engaging in activities that could expose the company to risk.

Employees are prohibited from using the internet to access, transmit, or share confidential company information without proper authorization. Any misuse of internet resources is considered a violation of this policy and may result in disciplinary action.

9. INFORMATION SECURITY POLICY

Objective:

Information security means protecting the organization's data, applications, networks, and computer systems from unauthorized access, alteration, and destruction. This policy provides a comprehensive framework for classifying and protecting all forms of company information based on their sensitivity level. It covers access controls, data handling practices, incident reporting, and the responsibilities of all staff members to safeguard information assets.

Employees are required to handle company data carefully and follow all prescribed security practices to prevent breaches and data loss. Non-compliance with information security policies is treated as a serious violation and may lead to disciplinary or legal consequences.

10. COMPUTING ENVIRONMENT MANAGEMENT

Objective:

This policy ensures that all IT infrastructure — servers, workstations, databases, and applications to managed correctly and securely to support reliable business operations. Documented operating procedures are to be maintained for all key systems, covering start up, shutdown, routine maintenance, and error handling. Changes to the computing environment are carried out through the approved change management process to prevent unauthorized alterations.

Access to the computing environment is restricted to authorized IT personnel, and all activity is monitored and logged. The goal is to ensure information processing facilities operate without disruption and in full compliance with security standards.

11. NETWORK SECURITY POLICY

Objective:

Network security is a critical part of INOXCVA's overall information security strategy, protecting the systems and data that connect all parts of the business. This policy ensures that all networking, communication, and computing technologies are used in a secure and controlled manner. Unauthorized access to the network, misuse of networking resources, and transmission of sensitive data over unprotected channels are strictly prohibited.

12. VIRTUAL PRIVATE NETWORK POLICY

Objectives:

This policy defines secure and controlled remote access for authorized employees, contractors, and vendors requiring connectivity to INOXCVA systems from external locations. VPN access is limited to approve users.

All remote connections are to be established using approved VPN clients and in alignment with the organizations access control and authentication standards. Unauthorized use of VPN services or attempts to bypass established controls are strictly prohibited and may result in disciplinary action. The policy also covers site-to-site VPN connections between manufacturing plants, R&D centres, and partner facilities.

13. Information Classification and Protection Policy

Objectives:

This policy requires all company information to be classified based on its sensitivity — as Public, Internal Use, or Restricted/Confidential — so that the right level of protection can be applied to each type. Information owners are responsible for correctly classifying the data they manage and ensuring it is handled and stored according to its classification level.

Restricted and confidential information is accessible only to individuals with a valid business requirement, and all disclosures are subject to formal authorization. This policy applies to all employees, contractors, and third parties handling company information in any format, whether digital or physical. Proper classification supports the reduction of risks related to data breaches, unauthorized disclosure, and regulatory non-compliance.

14. WEBSITE SECURITY

Objective:

The objective of this policy is to establish uniform standards and controls for website security across the organization, ensuring protection of domain names, hosting environments, application platforms, and content management processes. These controls are designed to safeguard organizational assets, maintain brand integrity, prevent unauthorized access, and mitigate risks associated with website operations globally.

15. VIRUS MANAGEMENT POLICY

Objective:

This policy ensures that all company devices compulsorily install and configure the corporate antivirus with latest technology XDR features connected with SIEM and SOAR threat hunting platforms to have secure and safe computing environment and protection against threats like, viruses, worms, Trojans, and other forms of malicious software. Users are not permitted to disable, bypass, or tamper with antivirus tools under any circumstances.

16. Backup & Restore Policy

Objective:

This policy ensures that all critical data and information systems at INOXCVA are regularly centralised backed up of business data of all users machines, servers, storages and all computing devices and ensure full backup data availability as n when require.

The policy based on business continuity, minimizes the risk of data loss, and ensures compliance with ISO 27001:2022 control A.12.3.

17. Artificial Intelligence Acceptable Use Policy

Objectives:

The Objective of this policy is to set out principles and ensure the ethical and responsible deployment of AI at INOXCVA and ensure that all employees adhere to the AI acceptable use policies and procedures. This policy ensures that businesses critical information and data must not be used to open LLM based environments. System DLP (Data Leakage Prevention) mechanism will ensure that data must be within our own control for Generative AI Queries and applications.

18. Logging and Monitoring Policy

Objectives:

The Objective of this policy ensure that all the activities related to users access related to networks, servers and data access / update to be logged record as per (Role based access controls) RBAC mode and log data of activities stored for further forensics / audit purpose as per IT act 2000 and company act requirements.

This policy applicable to all employees, contractors and associates whomsoever is having access rights for accessing company's business data directly / indirectly.

19. USER RESPONSIBILITIES / ACCOUNTABILITY

Objectives:

The objective of this policy is to ensure that all security incidents are reported promptly, that employees receive proper security awareness training, and that all stakeholders use company systems and assets responsibly in compliance with the Code of Conduct, IT Policy, and applicable laws. This helps protect information systems, strengthen security practices, and maintain accountability across the organization.

20. SOFTWARE ANALYSIS, DESIGN, DEVELOPMENT IMPLEMENTATION

Objective:

The objective of this policy is to establish a structured and secure approach for software analysis, design, development, implementation, and usage within Inoxcva. It ensures that all new application development follows the complete Software Development Life Cycle (SDLC) includes waterfall methodology and Agile methodology which includes requirements, analysis, design, development, testing, implementation for secure code development.

21. COMPLIANCE

Objective:

The objective of this policy is to ensure that the operation and management of information systems at Inoxcva comply with all contractual, regulatory, and legal requirements. It aims to prevent breaches that could result in civil or criminal liability by mandating the use of authorized software, enforcing license conditions, and prohibiting unauthorized or unapproved applications.

22. Clear Desk Policy

Objectives:

The objectives of this policy is to define procedures to safeguard one or multiple copies of data (which can be used for recovery in the event of an attack) and to minimize the impact of business interruption. It also sets out principles for ensuring that INOXCVA's data backups reduce the risk of data loss.

23. ACQUISITION & IMPLEMENTATION OF PACKAGED SOFTWARE POLICY

Objective:

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) software to be cyber secure with duly VAPT and Code audited and verified for secure usage.

24. INCIDENT MANAGEMENT POLICY

Objective:

The objective of this policy is to ensure that all incidents affecting Inoxcva's information systems are reported and handled quickly to reduce damage, restore services, and strengthen security. It covers all types of incidents, defines clear response responsibilities, sets procedures for handling and documenting events, and uses threat detection tools to identify and mitigate risks effectively.

25. ADHERENCE TO CONFIDENTIALITY AND PRIVACY LAWS, CYBER LAWS GUIDELINES

Objectives:

The objective of this policy is to ensure that Inoxcva complies with all applicable data privacy laws, cyber laws, and related guidelines. All users of the business data whether employee / third party sign a NDA (non-disclosure agreement) which is backend banded with SLA and Contract with users.

26. ACCEPTABLE USAGE POLICY

Objective:

This policy defines the standards for using INOXCVA's computing systems, facilities, and resources in an effective, ethical, lawful, and efficient manner. All stakeholders—including users, support staff, and management—are expected to use IT resources only for legitimate business purposes and in alignment with company policies.

Activities that are prohibited include unauthorized access to systems, sharing login credentials, installing unapproved software, and using company resources for personal gain or illegal activity.

27. CAPACITY PLANNING AND PERFORMANCE MANAGEMENT POLICY

Objective:

This policy ensures that INOXCVA always maintains sufficient IT capacity in terms of hardware, networking equipment, software, storage, and skilled personnel to meet current and anticipated business demands cost-effectively. Regular capacity reviews are conducted to assess whether existing resources can support growth, peak loads, and new business requirements.

Performance metrics are tracked and reviewed periodically, and capacity enhancements are planned in advance to minimize the risk of bottlenecks or service disruptions. The goal is to ensure that IT infrastructure never becomes a constraint on business performance or growth.

28. BUSINESS CONTINUITY PLANNING POLICY

Objective:

Business Continuity Plan is to cater to the operational aspect of Crisis Planning for potential natural disasters like earthquakes, severe storms, flooding, etc. or disruptive acts deliberately caused by manmade attack vectors i.e. (virus attack, bombings, riots and theft) or technical software glitches results to server crash, application crash etc., could lead to significant disruption of business, if recovery measures are not planned in advance.

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.

29. THIRD PARTY AND OUTSOURCING SERVICES POLICY

Objective:

This policy establishes a framework for identifying, evaluating, and managing all third-party IT services and outsourced functions, including cloud services, software development, AMC contracts, and IT audit engagements. All third-party vendors are to be assessed for security, financial stability, and compliance prior to engagement, and formal agreements are to clearly define their IT and security obligations.

Vendor performance is monitored on a regular basis, and access to INOXCVA systems or data is controlled and limited to business requirements, with timely revocation when no longer required. Risk assessments are conducted before approving any new outsourcing arrangement, and high-risk vendors are escalated for additional review. Third parties that fail to meet INOXCVA's standards may have their contracts terminated.

30. IT AUDIT POLICY

Objective:

This policy establishes a mechanism for conducting regular, independent auditors of INOXCVA's for audit information systems to verify that IT assets are properly protected, data integrity is maintained, and all policies and procedures are being followed. IT audits may be carried out by an external auditor or an independent internal authority, and findings formally reported to senior management.

Audit scope includes all critical systems, networks, applications, data storage, access controls, and compliance with this IT Policy. Management is responsible for reviewing audit findings and implementing corrective actions within defined timeframes. Regular auditing supports the organization's commitment to accountability, continuous improvement, and regulatory compliance.

31. CHANGE AND PROBLEM MANAGEMENT

Objective:

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.

Problem management is aimed at providing timely and satisfactorily addressing and resolving issues related to usage of IT resources by end users.

32. ISSUES MANAGEMENT POLICY

Objective:

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 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.

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

33. CONFIGURATION MANAGEMENT POLICY

Objective:

This policy ensures uniformity and control over changes to all software versions, system configurations, ERP modules, network infrastructure, and related documentation across INOXCVA's IT environment. All configurable items — including hardware components, software instances, network devices, and application modules identified, documented, and registered in the configuration management database (CMDB).

Changes to configuration items are carried out through the approved change management process, and all changes are tested prior to deployment in production environments. Version

control is maintained for all software and configuration files to enable restoration of previous versions when required.

The objective is to maintain a stable, well-documented, and auditable IT environment.

34. EXCEPTION

Objective:

There may be occasions on 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.

35. Vulnerability Management Policy

Objectives:

This policy ensures that INOXCVA's IT environment is regularly assessed for security vulnerabilities so that risks can be identified, prioritized, and resolved before they are exploited. The vulnerability management team monitors industry sources for security alerts, assigns risk ratings to identified vulnerabilities, and works with system owners to remediate them within defined timeframes based on severity and threat priority.

All identified vulnerabilities are recorded and tracked in a centralized register, with high-severity issues escalated and addressed on priority. Regular vulnerability scans and assessments and conducted across systems, networks, and applications within the defined scope.

36. Patch Management Policy

Objectives:

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 which is applicable to all connected computing devices, servers, storage devices, applications, DB, OS and as applicable.

37. Password Management Policy

Objectives:

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 applicable to all business partners internal as well as externals.

38. ERP Environment Segregation and Change Control Policy

Objectives:

This policy ensures that INOXCVA's ERP system maintains strict separation environment between Development, Testing (UAT), and Production environments to protect the integrity of live business data. Only changes that are fully tested and formally approved are moved to the Production environment, following the established change management process with appropriate documentation and sign-offs.

Role-based access controls (RBAC) are applied across all environments to ensure that users only have the level of access they need — developers do not have access to Production data without explicit approval. Any unauthorized access, movement of data between environments, or bypass of change controls is a serious violation and will result in disciplinary action. Regular audits of environment configurations and access rights are conducted to ensure ongoing compliance.

39. Secure Area Policy

Objective:

This policy protects the organization's physical IT infrastructure which includes server centres network equipment rakes, data backup storage devices and any areas where sensitive information is processed or stored; to protect from unauthorized access, damage, or interference. Access to all secure areas is restricted to authorized personnel only, with entry controls such as access cards, biometric authentication, and electronic locks in place.

40. Security Testing and Vulnerability Management Policy

Objectives:

This policy defines a framework for conducting regular security testing across INOXCVA's IT environment which includes networking devices, servers, workstations, email systems. Purpose to identify and address technical vulnerabilities in a timely manner.

Formal vulnerability assessments scheduled every quarter and results are documented and reviewed by the security team.

Identified vulnerabilities are prioritized based on risk level and are remediated within defined timelines to reduce the likelihood of security breaches. Security testing results are retained as evidence for audits and compliance reviews, and responsibilities for testing activities are clearly defined.

---- End of Document ----