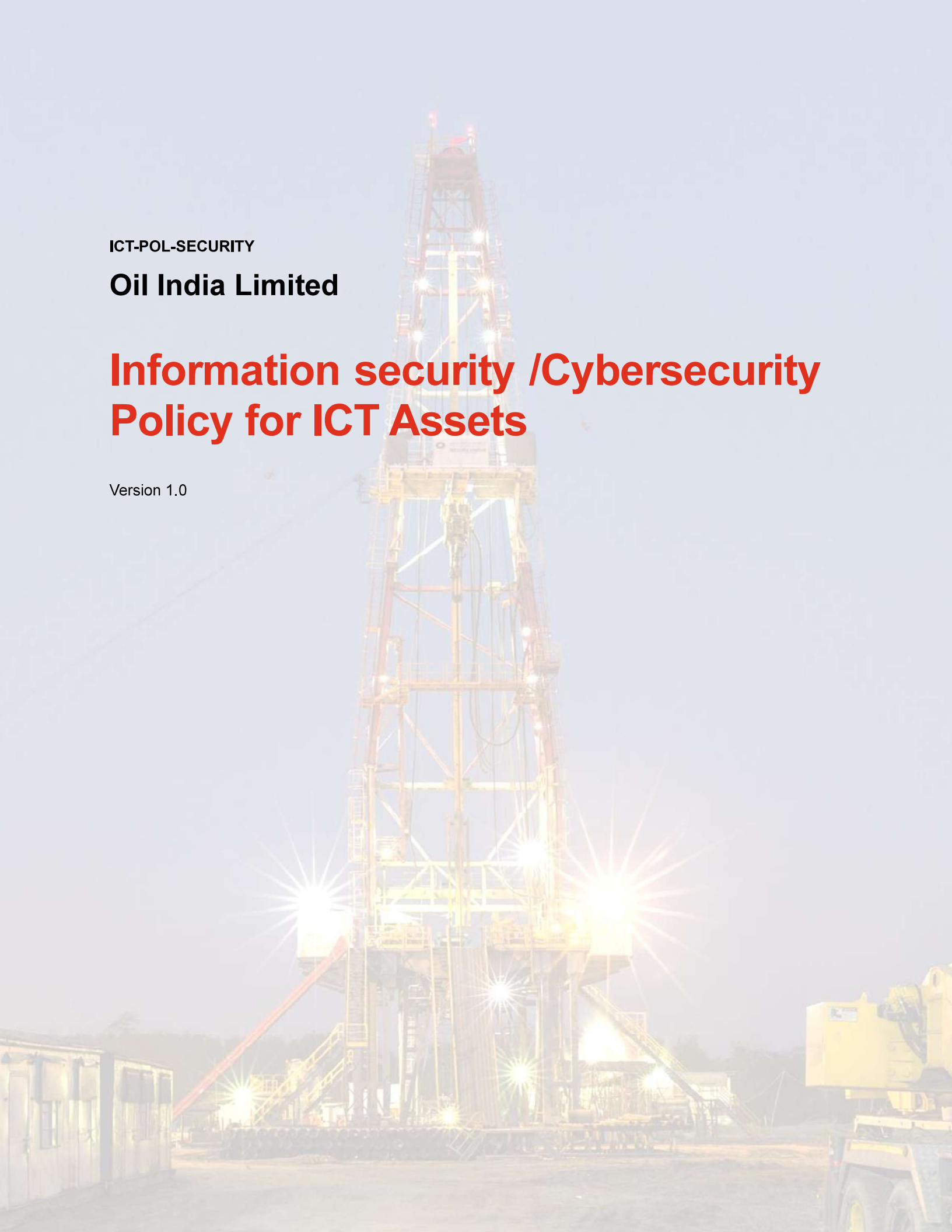


ICT-POL-SECURITY

## Oil India Limited

# Information security /Cybersecurity Policy for ICT Assets

Version 1.0

## DOCUMENT CONTROL

| Document Control | |
|---|---|
| Document Title: Information security /Cybersecurity Policy for ICT Assets | Version: 1.0 |
| Document Owner: CISO | Document ID: ICT-POL-SECURITY |
| Department: CISO | Review Frequency: Annual |

| Revision History | | | | |
|---|---|---|---|---|
| Version No. | Effective Date | Prepared By | Approved By | Description |
| 1.0 | 03.10.2025 | CISO | Executive Council | Base Document |
| | | | | |
| | | | | |

# Table of Contents

# 1 INTRODUCTION

The Information Security/Cybersecurity Policy for ICT Assets at Oil India Limited (OIL) establishes a robust framework to protect organizational data and ICT assets. This policy is designed to ensure the confidentiality, integrity, and availability of information systems, aligning with OIL's strategic objectives and information security requirements.

# 2 PURPOSE

The Information Security Policy establishes Oil India Limited's commitment to safeguarding its data, systems, and technology infrastructure. It sets the foundation for protecting confidentiality, integrity, and availability while aligning security measures with business objectives, risk management, and regulatory compliance. By integrating cybersecurity into enterprise operations, the policy ensures resilience against cyber threats and fosters a culture of accountability and continuous improvement across the organization.

This policy serves as the overarching directive for OIL's information security governance model and is supported by topic-specific policies, standards, procedures, and guidelines that collectively form the foundation of the organization's Information Security Management System (ISMS).

# 3 SCOPE AND APPLICABILITY

This policy applies to all personnel, third parties, and systems that access, process, or manage Oil India Limited's information or ICT assets across all locations and functions.

# 4 OBJECTIVES

Oil India Limited (OIL) has defined the following information security objectives to ensure consistent protection of its ICT assets and to support the organization's strategic, regulatory, and operational goals:

1. Protect the Confidentiality, Integrity, and Availability (CIA) of OIL's information assets, systems, and services from unauthorized access, disruption, or compromise.
2. Ensure compliance with applicable national regulations and standards, including the Information Technology Act, 2000, CERT-In guidelines, the Digital Personal Data Protection (DPDP) Act, 2023, and international standards such as ISO/IEC 27001:2022 and the NIST Cybersecurity Framework.
3. Establish and maintain a risk-based Information Security Management System (ISMS) that enables the organization to proactively identify, assess, and treat information security risks.
4. Support secure digital transformation and technology innovation by embedding security into new ICT and OT initiatives, enterprise platforms, and modernization efforts.
5. Ensure business continuity and operational resilience through implementation of robust disaster recovery, backup, and incident response capabilities.
6. Promote a strong security culture by increasing awareness, accountability, and participation of employees, contractors, and third parties in information security practices.
7. Maintain effective governance and oversight of all security activities through the Run and Govern model, with clear delineation of roles, responsibilities, and approval processes.
8. Continuously improve the maturity, performance, and coverage of security controls and practices through audits, reviews, feedback, and lessons learned.

# 5 GUIDING INFORMATION SECURITY PRINCIPLES

Oil India Limited (OIL) has established comprehensive principles to guide the protection and management of its information and technology assets across ICT and OT environments. These principles are embedded in OIL's Information Security Management System (ISMS) and apply organization-wide to ensure secure and compliant operations.

1. **Confidentiality, Integrity, and Availability (CIA):** OIL safeguards information assets against unauthorized access, corruption, and disruption, ensuring secure and reliable operations throughout their lifecycle.
2. **Risk-Based Approach:** Security decisions and controls are prioritized based on formal risk assessments, asset criticality, threat exposure, and business impact.
3. **Least Privilege and Need-to-Know:** Access is restricted to the minimum necessary for roles and functions, promoting secure operations.
4. **Defence in Depth:** Multiple layers of security controls are implemented to mitigate the risk of single-point failures and security breaches.
5. **Separation of Duties:** Critical activities involve multiple roles to prevent fraud, reduce errors, and ensure independent oversight.
6. **Secure by Design:** Security requirements are integrated from the outset during the architecture, design, and procurement of systems.
7. **Accountability:** Individuals are accountable for the security of systems and information they manage, with clearly defined roles and responsibilities.
8. **Compliance and Legal Alignment:** OIL adheres to Indian laws (e.g., IT Act, DPDP Act), CERT-In directives, and global standards such as ISO/IEC 27001 and NIST CSF.
9. **Continuous Improvement:** Regular assessments, audits, and feedback are used to enhance information security practices in response to emerging threats and operational insights.

Through these principles, OIL promotes a strong security culture, supports secure digital transformation, and ensures the confidentiality, integrity, and availability of its ICT and OT assets while complying with relevant legal and regulatory standards.

# 6 GOVERNANCE

Oil India Limited (OIL) has established an effective governance framework to manage Information Security, ICT, and Operational Technology (OT) in line with strategic business goals, regulatory requirements, and global best practices. This framework supports a Run and Govern model, integrating corporate oversight with operational execution.

## 6.1 GOVERNANCE STRUCTURE

The governance structure includes key components:

- **Board of Directors:** Provide strategic oversight, resource support, and approves cybersecurity policies and the Information Security Management System (ISMS).
- **Director (Operations):** Hold executive responsibility for ICT, OT, and cybersecurity, receiving reports from the Chief Digital Officer (CDO), Chief Information Security Officer (CISO), and Executive Director – Engineering Services (ED-ES).
- **Chief Digital Officer (CDO):** Lead ICT modernization, digital transformation, ensure alignment with business objectives and ensure regulatory compliance and ICT governance across OIL in coordination with CISO..

- **Chief Information Security Officer (CISO):** Directs cybersecurity strategy, risk management, regulatory compliance, and oversees the ISMS.
- **Executive Directors (ED-PLS and ED-ES):** Provide Strategic leadership to drive technology transformation, mitigate Cybersecurity risks across OT, and ensure regulatory compliance and OT governance across OIL in coordination with CISO.
- **Domain Heads (IT, Instrumentation, T&I PHQ):** Manage execution of security controls, infrastructure management, and incident response.
- **Information Security Council (ISC):** Ensure the protection of the organization's information assets through effective security measures. The council oversees all aspects of information security, such as policies, risk management, and incident response at a leadership level.
- **Information Security Working Group (ISWG):** Foster a culture of cybersecurity awareness, ownership, and proactive risk management across all departments. Act as a bridge between the central cybersecurity team (e.g., CISO) and business units, ensuring that security practices are effectively communicated, understood, and implemented at the departmental level.
- **Digital Steering Committee (DSC):** Align digital, ICT, and OT strategies with business transformation goals while fostering cross-functional collaboration and informed decision-making across departments.
- **Technical Change and Architecture Board (TCAB):** Evaluate ICT and OT architecture changes for alignment with business needs and cybersecurity standards.

The governance framework, led by the CISO and overseen by the ISC, ensures clear roles and responsibilities for managing information security across the organization, promoting effective policy implementation and monitoring.

## 6.2 ASSET GOVERNANCE – OWNERSHIP AND CONTROL

OIL shall ensure effective information security governance by defining clear ownership and accountability at the asset level. This is achieved through the formal designation of Asset Owners and Asset Custodians for all ICT and OT assets, including applications, infrastructure components, databases, network segments, and data repositories.

**Asset Owners** are accountable for the asset's value, classification, and acceptable use. They authorize access based on business needs, approve risk treatment actions, and ensure compliance with legal, regulatory, and contractual requirements. Although Asset Owners do not directly administer the asset, they are responsible for its protection and alignment with OIL's security policies.

**Asset Custodians** manage the day-to-day protection, maintenance, and operational management of assets on behalf of Asset Owners. Their responsibilities include implementing technical controls, ensuring compliance with approved configurations, supporting security assessments and audits, and maintaining accurate inventory and documentation. Asset Custodians typically belong to ICT operations, OT operations, or field IT/OT teams, operating under governance directives from Asset Owners and the CISO's office.

Asset Owners may be part of business units like Finance or Engineering, while Asset Custodians may span multiple support teams across ICT, OT, and third-party vendors. To enforce accountability, each ICT/OT asset must have a documented Owner and Custodian, with asset records maintained in a centralized inventory and reviewed periodically.

# 7 DISTRIBUTION

The policy is distributed internally within OIL, with external access requiring approval from the CISO's Office. This controlled distribution ensures confidentiality and integrity, with requests evaluated based on engagement nature and information sensitivity.

# 8 WAIVERS AND EXCEPTIONS

Waivers and exceptions to the policy must be requested from the Chief Information Security Officer (CISO), detailing the specific policy, rationale, and compensating measures. Approved waivers are documented with terms and conditions, while unapproved deviations are prohibited.

# 9 NON-COMPLIANCE

Non-compliance with this Policy may result in disciplinary and/or legal action, in accordance with applicable laws and the organization's existing policies. The Chief Information Security Officer (CISO) is responsible for ensuring the effective implementation, communication, and enforcement of this Policy. The CISO shall collaborate with Human Resources and Legal departments, as well as other relevant stakeholders, to address violations and ensure appropriate corrective measures are taken.

# 10 REVIEW FREQUENCY

This policy undergoes annual reviews, with ad hoc reviews triggered by significant changes in legal, business, or technology environments. Communication of the policy occurs annually or whenever modifications are made, ensuring personnel are informed of updates. It is maintained by CISO and approved by the Information Security Council (ISC); however, Information Security Working Group (ISWG) can approve minor changes.

# 11 SUPPORTING POLICIES

This Information Security Policy is supported by a comprehensive set of topic-specific policies that provide detailed controls, requirements, and procedures for managing and protecting ICT and OT assets across Oil India Limited (OIL). These policies collectively form the operational foundation of OIL's Information Security Management System (ISMS) and are maintained by the Office of the Chief Information Security Officer (CISO) in coordination with relevant stakeholders.

Given OIL's federated and decentralized structure, these supporting policies ensure consistency across departments while allowing for domain-specific implementation under the responsibility of respective Asset Owners, Custodians, and Functional Heads.

- Acceptable Use Policy: This policy defines the acceptable use of ICT resources by employees, ensuring that these resources are used responsibly and ethically.
- Disaster Recovery Policy: This policy provides a plan for recovering ICT systems and data in the event of a disaster, ensuring business continuity.
- Incident Response Policy: This policy outlines the procedures for responding to cybersecurity incidents, including detection, reporting, and mitigation.
- Mobile Device Security Policy: This policy addresses the security measures required for mobile devices used within the organization, protecting against unauthorized access and data breaches.
- Network Security Policy: This policy defines the security measures for protecting the organization's network infrastructure from cyber threats.
- Network Segmentation Policy: This policy involves dividing the network into segments to improve security and manageability, reducing the risk of widespread cyber-attacks.

- Identity and Access Management Policy: This policy governs the processes for managing user identities and access to ICT resources, ensuring that only authorized individuals have access.
- Remote Access Policy: This policy outlines the security requirements for accessing the organization's ICT resources remotely, ensuring secure connections.
- Risk Management Policy: This policy involves identifying, assessing, and mitigating risks to ICT systems, ensuring proactive management of potential threats.
- Security Awareness and Training Policy: This policy provides guidelines for educating employees about cybersecurity risks and best practices, promoting a security-conscious culture.
- Third-Party Security Policy: This policy addresses the security requirements for third-party vendors and partners, ensuring that they comply with the organization's security standards.
- Vulnerability Management Policy: This policy involves identifying, assessing, and mitigating vulnerabilities in ICT systems to prevent exploitation by cyber threats.
- Data Classification Policy: This policy defines the classification of data based on sensitivity and importance, guiding the protection measures required for each category.
- Data Protection Policy: This policy outlines the measures for safeguarding personal and sensitive data against unauthorized access and breaches.
- Endpoint Security Policy: This policy involves securing endpoints such as computers and mobile devices against cyber threats, ensuring they are protected from malware and unauthorized access.
- Data Backup and Recovery Policy: This policy provides guidelines for regularly backing up data and recovering it in case of data loss, ensuring data integrity and availability.
- Change Management Policy: This policy governs the processes for managing changes to ICT systems, ensuring that changes are implemented securely and efficiently.
- Security Monitoring Policy: This policy involves continuous monitoring of ICT systems for potential security threats, enabling timely detection and response.
- Asset Management Policy: This policy provides guidelines for managing ICT assets, ensuring they are tracked, maintained, and protected. Refer this policy for detailed information on Asset Owner (AO), Asset Custodian, CISO and User.
- Third-Party Information Exchange Policy: This policy addresses the security requirements for exchanging information with third parties, ensuring data is shared securely.
- Access Control Policy: This policy defines the measures for controlling access to ICT resources, ensuring that access is granted based on roles and responsibilities.
- Patch Management Policy: This policy involves regularly updating software and systems to fix vulnerabilities and improve security.
- Configuration Management Policy: This policy governs the processes for managing the configuration of ICT systems, ensuring they are secure and consistent.
- Cloud Security Policy: This policy outlines the security measures for using cloud services, ensuring data and applications are protected in the cloud environment.
- Software Development Policy: This policy provides guidelines for secure software development practices, ensuring that applications are developed with security in mind.

# 12 REFERENCE STANDARDS

| Sr. No. | Policy/ Procedure References |
|---|---|
| 1. | ISO/IEC 27001-2022 /27002-2022 |
| 2. | NIST Cybersecurity Framework |
| 3. | CIS Benchmarks |

OT-POL-SECURITY

## Oil India Limited

# Information Security/Cyber Security Policy for OT assets

Version V0.0

## DOCUMENT CONTROL

| Document Control | |
|---|---|
| Document Title: Information Security/Cyber Security Policy for OT assets | |
| Document Owner: CISO | Document Number: OT-POL-SECURITY |
| Department: CISO | Review Frequency: Annual |

| Revision History | | | | |
|---|---|---|---|---|
| Version No. | Effective Date | Prepared By | Approved By | Description |
| 1.0 | 03.10.2025 | CISO | Executive Council | Base Document |
| | | | | |
| | | | | |

# TABLE OF CONTENTS

## 1. INTRODUCTION

This OT Information Security/Cyber Security Policy outlines the principles, roles, responsibilities, and controls required to secure OT assets and networks. It is designed to ensure the confidentiality, integrity, and availability of OT systems and to support compliance with applicable regulations, industry standards, and organizational risk management objectives.

## 2. PURPOSE

The purpose of this policy is to protect Oil India Limited's (hereafter referred to as "OIL" or the "organization") Operational Technology assets from cyber threats, whether internal or external, deliberate, or accidental.

This policy would help in implementing a robust system by establishing governance and practices to ensure confidentiality, integrity, availability and safety of the systems. The objective of Cyber Security Policy shall be to provide direction and support OIL for maintaining cyber security in accordance with business requirements and relevant laws and regulations.

## 3. SCOPE

This policy applies to all employees, contractors, consultants, and third-party users accessing the OT assets/infrastructure of OIL.

This policy covers the usage of all the OIL's OT resources, including, but not limited to:

a. Embedded systems such as PLCs, DCS, safety systems, RTUs, and HMIs.

b. Host-based systems including servers, workstations, and laptops as well as advanced application nodes like anti-virus systems, patch servers, and domain controllers used for OT systems.

c. Network-related systems including telecom equipment, network switches, routers, firewalls, gateways, databases, and printers within the OT environment.

d. All software, whether provided by OEMs, developed in-house, or licensed for business use, including computer operating systems, firmware, and any other software residing on all OT systems.

## 4. REFERENCES

| ISO 27001:2022 CONTROL NUMBER | NIST CSF V2.0 RELEVANT CONTROL NUMBER | CONTROL TITLE |
|---|---|---|
| A.5.1 | GV.PO-01, GV.PO-02 | Policies for Operational Technology security |
| A.5 | GV.SC-04, GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-08, GV.SC-09, GV.SC-10, ID.AM-01, ID.AM-02, ID.AM-04, ID.AM-05, ID.AM-07, ID.AM-08, ID.RA-02, ID.RA-10, ID.IM-04, PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AA-06, PR.IR-03, DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-06, DE.AE-07, DE.AE-08, RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.MA-05, RS.AN-03, RS.AN-06, RS.AN-07, RS.AN-08, RS.CO-02, RS.CO-03, RS.MI-01, RS.MI-02, RC.RP-01, RC.RP-02, RC.RP-03, RC.RP-04, RC.RP-05, RC.RP-06, RC.CO-03, RC.CO-04 | Organizational Controls |
| A.6 | GV.RR-04, PR.AT-01, PR.AT-02 | People Controls |
| A.7 | PR.AA-06, DE.CM-02, PR.IR-02 | Physical Controls |

| | | |
|---|---|---|
| A.8 | ID.AM-03, ID.RA-01, ID.RA-04, ID.RA-05, ID.RA-07, ID.RA-08, PR.DS-01, PR.DS-02, PR.DS-10, PR.DS-11, PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-04, PR.PS-05, PR.PS-06, PR.IR-01, PR.IR-04, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09 | Technological Controls |

## 5. APPLICABILITY

This policy is applicable to all personnel within OIL including contractors, and third parties, that have access to OT information and OT systems/assets that may collect, store, process, generate and/or transmit information, whether these assets are: I) directly operated and managed by the OIL; ii) provided or managed by another contractor or other source; or iii) hosted by the OIL and managed or operated by another contractor, or another source.

## 6. DISTRIBUTION

The distribution of OIL's OT Information Security/Cyber Security Policy is primarily for internal personnel. External access, such as for contractors or third parties, requires prior approval from the OT Instrumentation Team. This ensures information confidentiality and integrity. Requests are evaluated based on engagement nature, information sensitivity, and regulatory obligations, maintaining security standards to protect OIL's strategic interests.

## 7. WAIVERS

Waivers to OIL's OT Information Security/Cyber Security Policy must be requested from the Chief Information Security Officer, detailing the specific policy, rationale, and compensating measures. The CISO evaluates requests based on their impact on security and compliance. Approved waivers are documented with terms and conditions. Unapproved deviations are prohibited, ensuring adherence to OIL's security standards and strategic objectives.

## 8. NON-COMPLIANCE

Non-compliance with OIL's OT Information Security/Cyber Security Policy can lead to disciplinary or legal actions. Department and functional heads, along with the HR/Legal Team, are accountable for ensuring adherence among all staff. They are responsible for implementing appropriate remedial measures, maintaining compliance, and safeguarding the organization's security standards and strategic objectives.

## 9. ROLES & RESPONSIBILITIES

| Role | Responsibility |
|---|---|
| CISO | • Shall review and approve exceptions to this policy.<br>• Shall ensure implementation of the cybersecurity policy.<br>• Shall oversee risk assessments and vulnerability analyses for OT environments. |
| Governance, Risk and Compliance Team | • Shall define cybersecurity policy.<br>• Shall identify cybersecurity goals and objectives consistent with organization business need/objectives.<br>• Shall define the scope and boundaries of the cybersecurity program.<br>• Shall define cybersecurity implementation strategies<br>• Shall define formal process for creating, documenting, reviewing, updating, and implementing security policies.<br>• Shall get approval of cybersecurity policies, procedures, guidelines and processes |

| Role | Responsibility |
|---|---|
| | • Shall enforce implementation of approved cybersecurity policies, procedures, guideline<br>• Shall periodically evaluate and review effectiveness of cybersecurity policies, procedures, standards<br>• Shall ensure compliance with legal and regulatory requirements for cybersecurity.<br>• Shall perform cybersecurity audit at least annually or whenever significant changes have been made in OT systems/ Infrastructure.<br>• Shall prepare cybersecurity audit report along with recommendations for improving OT security.<br>• Shall obtain senior management approval of cybersecurity audit report.<br>• Shall send a copy of management approved audit report periodically to relevant regulators. |
| All employees and third-party personnel | • Shall abide by the policy under all circumstances<br>• Shall report any violations of the cybersecurity policy |

## 10. MANAGEMENT COMMITMENT FOR OT SECURITY POLICY

- OIL's senior management acknowledges the critical importance of OT security for organizational success.
- Both leadership and staff are committed to adhering to OT security policies and protocols.
- Define roles and responsibilities related to OT security at all organizational levels to ensure effective implementation.
- Align cybersecurity practices with globally recognized standards like IEC 62443 and ISO/IEC 27001:2022, and comply with applicable regulatory mandates.
- Implement security controls to protect critical operations, engineering configurations, and ensure the safety and availability of OT systems.
- Continuously monitor the performance of the OT security management system and allocate resources for its maintenance and improvement.
- Promote a risk-based approach to OT security through regular industrial cybersecurity risk assessments.
- Ensure operational resilience and continuity of critical OT functions during failures, cyber incidents, or disasters.
- Implement layered detection, prevention, and recovery controls tailored for OT environments, and investigate security events for corrective actions.
- Ensure third parties, suppliers, integrators, and contractors follow OIL's OT security policies throughout the industrial supply chain.
- Foster a strong OT cybersecurity culture among employees, contractors, and partners through targeted awareness and training programs.
- Conduct Business Impact Analyses to understand dependencies and the impact of potential disruptions on OT functions.
- Conduct annual security risk assessments to identify vulnerabilities, threats, and risks, ensuring timely corrective actions.
- Determine cybersecurity controls for OT systems based on the outcomes of Risk Assessments and Business Impact Analyses.

## 11. ALSO REFER

**1. OT Asset Management Policy:** This policy mandates managing all hardware and software required for plant operations by classifying assets according to their impact on safety and security.

**2. OT Access Management Policy:** This policy ensures that access to OT systems is role-based and authorized, requiring secure controls and regular reviews of user permissions.

**3. OT Physical and Environmental Security Policy:** This policy restricts physical access to OT equipment to authorized personnel and mandates maintaining environmental controls and safety measures.

**4. OT Mobile Device Security Policy:** This policy requires mobile devices authorized for OT access to be role-restricted and to ensure secure connections.

**5. OT Network Security Policy:** This policy demands designing OT networks according to industry standards, maintaining secure boundaries, segmenting networks, and monitoring for anomalies.

**6. OT Endpoint Security Policy:** This policy mandates implementing endpoint protection, deploying antivirus solutions, and conducting regular security reviews of endpoint devices.

**7. OT Patch Management Policy:** This policy requires regular updates to OT systems with OEM-approved patches and evaluating compensatory controls for unpatched vulnerabilities.

**8. OT Data Classification Policy:** This policy classifies data into security levels, mandates labeling, and manages access using cryptography for confidential data.

**9. OT Configuration Management Policy:** This policy establishes baseline security standards for OT assets and requires regular monitoring and review to revert unauthorized changes.

**10. OT Change Management Policy:** This policy implements a controlled process for OT system changes, including testing, approvals, and emergency response procedures.

**11. OT Cloud Security Policy:** This policy requires conducting risk assessments for IIoT systems, defining shared responsibilities, and ensuring cloud security alignment with standards.

**12. OT Logging and Monitoring Policy:** This policy mandates recording and protecting system and network logs, ensuring continuous monitoring and comprehensive reporting.

**13. OT Backup and Recovery Policy:** This policy requires regular backups of essential OT data, secure storage of backups, and defining retention periods per policy.

**14. OT Risk Management Policy:** This policy mandates regular assessments and remediation of OT risks, requiring documentation and impact ratings for proactive management.

**15. OT Disaster Recovery Policy:** This policy requires developing recovery strategies for OT systems, conducting training, and aligning disaster recovery with business continuity.

**16. OT Incident Management Policy:** This policy maintains incident response plans, mandates reporting and documenting incidents, and uses monitoring tools to identify security events.

**17. OT Third Party Security Policy:** This policy assesses third-party risks, includes security clauses in contracts, and mandates regular audits of third-party compliance.

**18. OT Training and Awareness Policy:** This policy requires conducting periodic security training for employees and third parties to ensure compliance with OT security policies.

## 12. EXCEPTION

Where there is a justifiable business need that requires action to be performed that conflicts with this document, such exceptions shall be reported with identified risk and the CISO shall approve/deny the exceptions. Any violations to this policy may be subjected to disciplinary action.

## 13. REVIEW FREQUENCY

OIL shall review its OT Information Security/Cyber Security Policy on an annual basis. However, to improve the organizational security posture, the policy may undergo an ad hoc review in situations which may include but is not limited to:

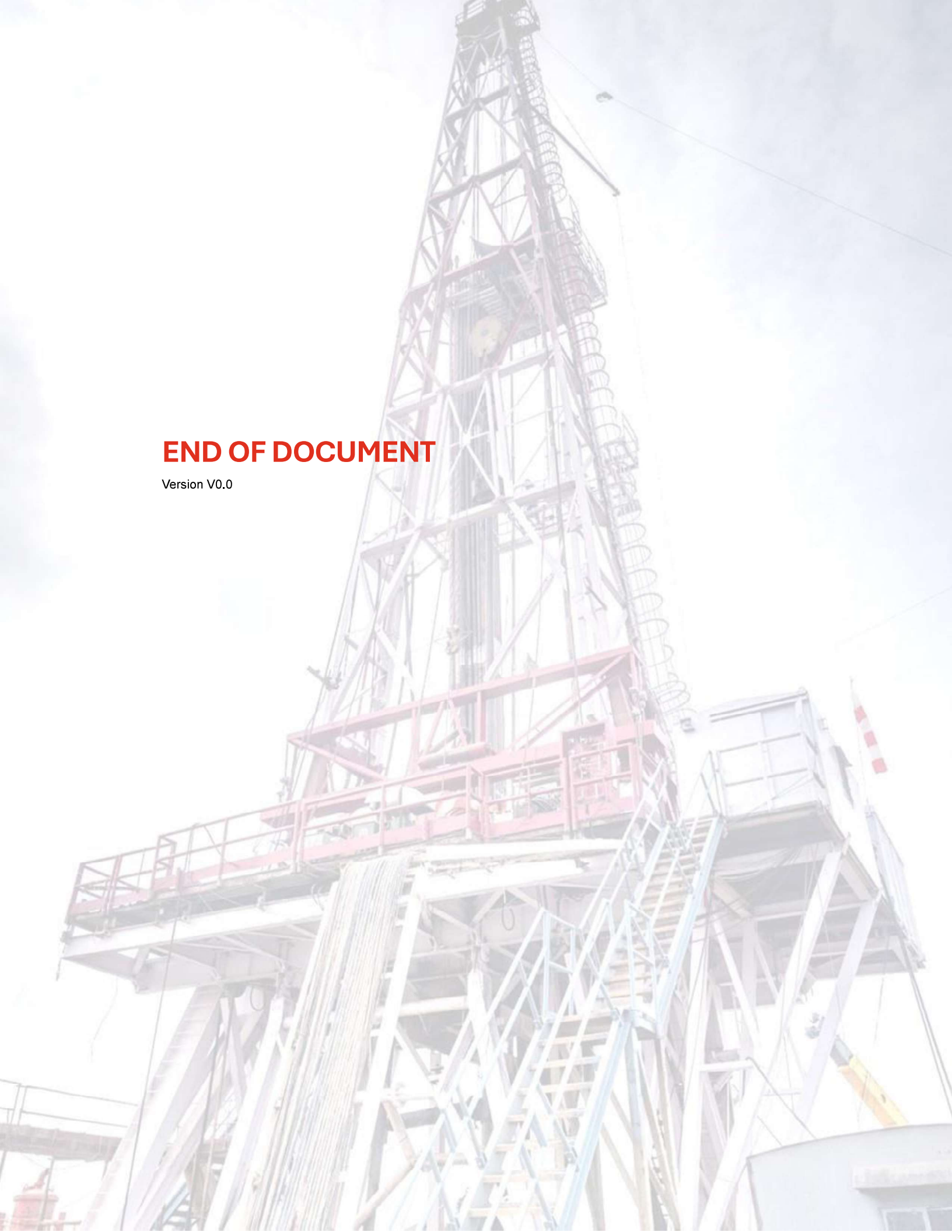
- When there is a major technology change/update,
- Any severe incidents occur that may affect vulnerability management.

The OT Information Security/Cyber Security Policy shall be communicated to personnel annually and/or whenever there are any modifications to this policy.

## 14. ANNEXURE I - GLOSSARY

| GLOSSARY | | |
|---|---|---|
| **Sr. No.** | **Term/ Acronym** | **Definition/ Description** |
| 1. | Asset | Any physical or logical object owned or managed by an organization, deemed valuable either in perception or actuality. |
| 2. | Background Checks | Processes to verify an individual's suitability to access critical OT systems based on recruitment practices. |
| 3. | Business Continuity Plan | A documented strategy outlining procedures to recover and restore business operations following a major disruption. |
| 4. | Change Management | The structured approach to managing alterations in systems to maintain operational consistency and reliability. |
| 5. | Connected OT Systems | Systems within a layered network where OT devices are linked through network devices like switches and routers, often separate from IT systems. |
| 6. | Cybersecurity Controls | Measures implemented to protect systems from cyber threats, ensuring safety and availability. |
| 8. | Environment Security Controls | Measures to secure the physical surroundings and environment of OT assets. |
| 9. | Endpoint Security | Protection measures such as antivirus solutions deployed on devices to detect and prevent malicious activities. |
| 10. | Exception | A sanctioned deviation from policy due to a justified business need, subject to approval by the CISO. |
| 12. | Function | Refers to the part of the organization that is being evaluated |
| 13. | Incident | An event disrupting normal operations, potentially degrading service quality or causing an interruption. |
| 14. | Network Assets | Core components enabling communication and data flow, including routers, switches, firewalls, servers, software, and configuration data. |
| 15. | Operational Technology (OT) | Systems comprising hardware and software dedicated to monitoring and controlling industrial operations and processes. |
| 16. | OT Security | Technologies and practices designed to safeguard people, assets, and information within an OT environment. |
| 17. | Patch Management | Management process for acquiring, testing, and deploying patches to update computer systems effectively. |
| 18. | Physical and Environmental Security Controls | Measures to secure the physical surroundings and environment of OT assets to ensure their safety and security. |
| 19. | Remote Access | The ability to connect to and interact with assets or systems within a secure perimeter from external locations. |
| 20. | Risk Management | The systematic process of identifying, evaluating, and addressing risks impacting organizational objectives and assets. |

| GLOSSARY | | |
|---|---|---|
| **Sr. No.** | **Term/ Acronym** | **Definition/ Description** |
| 21 | Roles and Responsibilities | Defined duties related to OT security established at organizational levels for effective implementation. |
| 22. | Senior Management Acknowledgment | Recognition by high-level executives of the importance of OT security in organizational success. |
| 23. | Standalone OT System | An OT system operating independently, not integrated with external networks, enhancing security through isolation. |
| 24. | System Resilience and Continuity | Measures ensuring critical OT functions persist through failures, cyber incidents, or disasters. |
| 25. | Third-Party Compliance | Assurance that external entities adhere to OIL's security policies and implement required controls. |
| 26. | Training and Awareness | Programs aimed at educating employees and partners on cybersecurity policies and best practices. |
| 27. | Vulnerability Assessment | A systematic evaluation of security weaknesses in a system to identify and remediate potential threats. |



# END OF DOCUMENT

Version V0.0