INDO COUNT INDUSTRIES LIMITED

CYBER SECURITY POLICY

Version No.: 1.0
Version Date: 25-12-2023
Approved by: Board of Directors

A. OBJECTIVE

This Cyber Security Policy (Policy) outlines the commitment of Indo Count Industries Ltd. ('ICIL' or 'the Company') for managing information security risks effectively and efficiently, coordinated globally and in compliance with applicable regulations wherever it conducts business.

This Policy is the foundation for all information security activities. It focuses not only on the technology for the storage, processing, and transmission of information, but also on administrative and operational practices for the protection of all information, data, files, and processing resources owned by the Company. It is the intent of this Policy to facilitate the exchange of information and computing resources while balancing the need for protecting information with the cost of implementation.

B. SCOPE OF APPLICABILITY

This Policy applies to all employees, vendors, contractors, and consultants, who create, distribute, access, or manage information by means of ICIL's information technology systems including personal or corporate computers, networks, and communication services by which they are connected. It equally applies to individuals and enterprises, who by virtue of their relationship to ICIL are entrusted with confidential or sensitive information.

C. POLICY RESPONSIBILITY

The IT Head of ICIL has overall responsibility for information security matters. These responsibilities include:

1. Routinely monitoring security measures and analyzing data/logs to detect security incidents.
2. Ensuring appropriate User access and authentication controls are in place.
3. Ensuring that the documented security policies, standards, and procedures are reviewed, updated, and maintained periodically by appropriate individuals.

4. Evaluating security exposures, misuse, or non-compliance situations and ensuring the implementation of security controls to address those incidences.
5. Ensuring that employees execute their security responsibilities by related policies, standards,and procedures.
6. Ensuring that periodic training is imparted to all authorized Users of ICIL's systems, in coordination with the HR department.
7. Research new technologies to enhance security capabilities and implement improvements to ensure that ICIL information and systems are protected from new and emerging threats.
8. Reporting periodically to the RMC about cyber security measures and related issues at ICIL.

D. POLICY REQUIREMENTS

1. Security Management

The security of corporate information, applications, systems, and networks is fundamental to the continued success of ICIL. The Company has put in effective security management measures that establish controls and measures to minimize the risk of loss of information and system resources, corruption of data, disruption of access to the data, and unauthorized disclosure of information. At ICIL, security management is achieved through effective policies, standards, and procedures that will ensure the confidentiality, integrity, and availability of relevant information, applications, systems, and networks for authorized Users.

2. Confidentiality

Confidentiality relates to the protection of information from unauthorized access regardless of where it resides or how it is stored. At ICIL, adequate measures are in place to ensure that Information that is sensitive or proprietary is protected at a higher level than other information.

3. Integrity

Integrity is the protection of information, applications, systems, and networks from intentional, unauthorized, or accidental changes. At ICIL, all Users with approvals to access sensitive information, applications, systems, and networks are identified and authenticated through appropriate mechanisms.

4. Availability

Availability is the assurance that ICIL information and resources are accessible by authorized Users as needed. There are two issues relative to availability - denial of services caused by a lack of security controls (e.g. destruction of data or equipment, computer viruses, etc.), and loss of services from information resources due to natural disasters (e.g. storms, floods, fires). ICIL has implemented a robust Business Continuity Planning process to address these issues, should they occur.

5. Authentication

Authentication requires that the origin of a message be correctly identified with assurance that it is not a false or forged identity. Passwords are used to authenticate a User based upon the fact that only the User should know the password. ICIL's password policy mandates that strong passwords will be used and must contain a number of rules such as combinations of letters and numbers with combinations of upper and lower cases. One-time passwords are also implemented for high-risk applications as well as encryption to provide the authentication security service to identify the origin of messages. In addition to the use of passwords, Multi-factor Authentication is implemented where is it possible and appropriate.

6. Managing Information Assets

All information, data, applications, networks, and equipment are the property of ICIL and are provided to its employees so that they can conduct their job responsibilities effectively. Organizational information, applications, systems, and networks are actively managed by ICIL's IT department to ensure security, confidentiality, integrity, availability, and authenticity.

7. Accountability

The Company's administrative and computing environments will maintain consistent standards for establishing the accountability and authenticity of system Users. These environments will develop unique standards for protecting information, applications, systems, and network resources contained within these environments that will be commensurate with maintaining the integrity of those critical resources.

To maintain accountability for system access, ICIL has implemented the following:

- All individuals with access to the systems will use a User ID that has been authorized by company management and specifically assigned to that individual. Sharing of User IDs is prohibited except in specific, approved situations.
- All individuals with network, system, and application User IDs will retain a confidential password that will be used to authenticate the identity of the individual. Intentional disclosure or sharing of passwords is prohibited. In case the password is shared or disclosed to any person then appropriate action will be taken against both the users and will be termed as violation under this policy.

8. Information Access

At ICIL, all access to information is duly authorized, with access granted or revoked based on business requirements only. Access and update capabilities/restrictions will apply to all ICIL data. Security measures will apply to all systems developed and/or maintained by ICIL, its affiliates, outside vendors, or contractors.

The appropriate Head of the Business Unit and the Head of Department are responsible for authorizing access to systems and information, verifying information integrity, and controlling extracted information. All access to systems and information is provided based on business need.

9. Information Resources

At ICIL, information resources including computer software and support systems are protected appropriately to maintain the sensitivity and critical nature of information that is processed, stored, or communicated. Environmental and security controls are in place and assessed periodically for their effectiveness and appropriate level of risk. All communication facilities and equipment (including those provided by third-party service providers) are protected from unauthorized modification and tampering to ensure that messages in transit are not modified or received by unintended parties or that communication services are not interrupted.

10. Security Monitoring and Enforcement

The IT Head has the responsibility to implement appropriate measures to detect attempts to compromise the security or integrity of information and information technology systems. ICIL implements monitoring capabilities after due consideration of which situations are to be monitored based on the extent of risk, the most effective means for monitoring security activities, the resources available for monitoring, and system constraints that limit the ability to monitor security events.

When activities that conflict with security policies and standards are detected, the IT Head will take the appropriate steps to enforce desired security practices. The steps involved range from training of Users, revoking access, altering security parameters, and possibly disciplinary actions as per ICIL HR policies.

E. SECURITY MEASURES

1. Physical and Environmental Security

ICIL maintains controls to limit access to physical assets and mitigates risks associated with environmental issues (fires, floods, power loss) to help ensure data protection and system availability.

The following Physical security measures are in place.

a. **Physical Access Controls**: Access to buildings, data centers, and server rooms is restricted and controlled. Access control measures include the use of biometric systems and surveillance cameras.

b. **Server Room Security**: Server rooms are secured with robust access controls and monitoring systems. Access to server rooms is restricted to authorized personnel.

c. **Visitor Management:** Procedures are established for the registration and monitoring of visitors. Visitor access is restricted, and visitor badges are issued.

d. **Environmental Controls**: Data centers and server rooms have controlled environmental conditions, including temperature control. Fire prevention measures are in place, including smoke detectors.

e. **Secure Disposal of Equipment**: Data sanitization measures are implemented before equipment disposal.

2. Email Security

ICIL ensures security of its Email system by implementing the below controls:

a. Complex password policy and two factor authentication (OTP via SMS)

b. Email gateway (Anti-Threat Protection) in place for scanning all inbound and outbound emails.

c. Email auto scoring to identify and quarantine spam or suspicious emails.

d. ICIL domain and email authentication in place (DMARC, DKIM, SPF) for mitigating the impact of phishing and malware attacks, preventing spoofing, protecting against brand abuse, scams and avoiding business email compromise.

e. Automated and real-time email archival system – all emails are indexed, compressed and stored in an encrypted format.

3. Endpoint/ Server Security

ICIL ensures protection against vulnerabilities like spam, malware, viruses, etc. through its robust Endpoint/Server security system which features:

a. EDR (NextGen AV) software installed on each of the endpoint and server.

b. Data Leak Prevention software installed on each endpoint and server (Web, Email).

c. Drive encryption on each endpoint.

d. Web control protection software on each endpoint.

e. Disabled external storage is other than where authorized.

f. Timely deployment of security patches on each endpoint and server

g. Endpoint hardening via Active Directory Group Policies.

h. Business critical data backup daily to avoid data loss and corruption.

4. Network Security

ICIL ensures the protection of its networks against evolving threats or from any act or process that may breach its security through the below controls:

a. Network IP subnets are segregated and separated on each ICIL location on wired and wireless network.

b. Every ICIL location is guarded with Firewalls to build high-performance, ultra-scalable, and security-driven networks.

c. All ICIL locations are connected via IPSec VPN tunnels for secure data transmission.

d. Network policies are enforced with web and content filtering for only allowing business related web access.

e. Various Firewall policies control all inbound and outbound traffic which is monitored and blocked for malware and ransomware attacks.

f. Wireless network is secured via connection limited to radius authentication and MAC based Wi-Fi access.

g. Guest access on wireless network is configured and restricted for accessing basic Internet for limited periods.

h. Critical security patches and firmware are timely patched into all network devices.

5. Security Operations Center

ICIL has implemented a Security Operations Center (SOC) to collect, detect, investigate and respond to threats across ICIL Data Centres, Office networks and Public Clouds. The SOC performs the following tasks:

a. Monitoring and analysis of alerts generated from the SOC which include firewalls, routers, switches, servers, databases, and applications to identify potential information security incidents like security attacks and anomalous activities.

b. Investigating and notifying security incidents and nature of services impacted via email.

c. Responding to and resolving incidents by taking recommended actions

d. Providing global threat advisory and CTI (Cyber Threat Intelligence) Flash Advisory notifications for taking precautionary actions (updating Hash codes, blocking unauthorized domains and IPs)

6. Security Awareness Programs

ICIL ensures that all Users of information understand how to protect company assets, including information and information resources, and comply with security policies, standards, and procedures. Adequate and appropriate training is provided at periodic intervals to ensure that all Users understand general information security requirements and that they are sufficiently knowledgeable about information technology security policies, standards, and procedures to recognize the need for protecting information and the requirements for which they are specifically responsible.

The IT Head is responsible for developing, implementing and updating Information Security Awareness Programs that support User awareness. Reporting Managers and HODs should also be aware of User performance in this area, encourage good security practices, and address inappropriate behavior as per Company rules and policies.

7. Incident Management:

ICIL has implemented an effective Incident Management procedure for reporting incidents, violations, and suspected security weaknesses.

a. A formal process for Information security incident management shall be documented and implemented.
b. A dedicated Incident Response Team (IRT) is formed to address the Information Security Incidents in an appropriate and timely manner. IRT consist of representatives from Information Security, IT.
c. Information security incidents shall be identified from all relevant sources including users (employees, third parties, contractors), Security Operations Center, customers, threat advisories, etc.
d. Detected anomalies shall be recorded and analysed to check if they can be considered as Information security incidents.
e. All reported information security incidents shall be logged in a centralized system and classified based on their severity and impact to business.

8. Computer Security - Incident Response & Review

ICIL has in place effective plans and procedures for responding to suspected information security incidents that affect the confidentiality, integrity, or availability of data processed or owned by ICIL or for which ICIL serves as a custodian.

These plans and procedures address the following stages of incident response:

a. Preparation
b. Detection and Reporting
c. Analysis
d. Containment
e. Recovery
f. Post-Incident Activities

The facts surrounding an intrusion, infection, or system compromise will be documented, reported to the IT Head, and include the circumstances that led to the discovery of the incident, actions which were immediately taken, the names of persons involved in investigating the incident, and detailed observations about what transpired, what damage was caused, and what systems or files were compromised. Post-incident reviews are conducted to analyze the response to a cybersecurity incident and identify areas for improvement. Lessons learned from incidents are used to update and enhance the incident response plan.

9. Disaster Recovery/Business Continuity Planning

Should the confidentiality, integrity or availability of systems or information be affected by an incident, ICIL has an effective and robust Disaster Recovery and Business Continuity Plan (BCP) in place to minimize loss, reduce impact, and ensure continuity of the organization's functions and revenue stream. The BCP will address pre-planning risk control, crisis management, and business recovery.

10. Vulnerability Management:

Vulnerability Assessments: Vulnerability Assessment and Penetration Testing (VAPT)
are conducted yearly to identify and prioritize security vulnerabilities in systems, networks, and applications. A schedule for conducting assessments and implementing necessary patches and updates is in place.

Patch Management: Procedures for the timely application of security patches and updates to address identified vulnerabilities are defined. Patches are tested in a controlled environment before deployment to production systems.

Asset Inventory: An up-to-date inventory of all IT assets, including hardware and software, is maintained to facilitate effective vulnerability management. Assets are categorized based on criticality and sensitivity.

11. Clean Desk and Clear Screen

a. Users shall ensure that their desk is kept clear of unnecessary paper documents during and after office hours. While leaving, users must ensure that all paper documents and files are locked away in cabinets.

b. Users shall ensure that all prints are immediately collected from the printer tray and fax machines.
c. Users shall make sure that their computer screen is locked while they are away from their computer.
d. Sensitive information on paper that is to be shredded must not be left unattended to be handled later. They must be shredded immediately, or securely stored until the time that they can be shredded.

F. ACCEPTABLE USAGE POLICY

ICIL has in place an Acceptable Usage Policy for all its employees to ensure responsible and secure usage of the Company's information systems.

G. COMPLIANCE

ICIL complies with all applicable central, state, district, local, industry and contractual regulations in all the geographies that it operates in.

Non-compliance or violation of this policy should be brought to the immediate attention of the IT Head. The IT Head will work with the Company management to ensure that the problem is resolved and to take steps to eliminate future violations. An escalation process will define the course of action for all violations consistentwith the severity of the violation.

ICIL reserves the right to discipline, terminate or suspend, at its discretion, individuals who violate this policy. The disciplinary action taken will be consistent with the severity of the violation.

H. POLICY REVIEW

Risk Management Committee (RMC) of the Company shall oversee the governance of this Policy. The IT Head will be responsible for implementation of this Policy with due approvals from the Chief Financial Officer of ICIL.