JINDAL SAW LTD.
TOTAL PIPE SOLUTIONS

Jindal Saw Ltd. Information Security and Risk Management Policy

Policy Date: 1.1.2023

Revision Approval Date: 1.9.2023

Policy Owner: CIO

Policy Coordinators: Mr. Navneet Sharma and Mr. Sunil Tripathi

Policy Managers: Location IT Heads

Statement of Policy

Jindal Saw Ltd is committed to conducting all activities in compliance with applicable laws and regulations.

Jindal Saw Ltd has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use, protect personal sensitive information, protect critical data with the help of people, process & efficient technology.

As per policy the process followed is based on International Organization for Standardization 27005 framework.

Objective

The objective of Risk Management is to identify, control & mitigate risks at the inception of any breach. The policy and associated guidance provide a common methodology and organized approach to Information Security risk management as per requirement of regulatory compliance following Cert-IN guidelines to safeguard organization information, assets & protect business objectives.

Applicability

This policy is applicable for all Jindal Saw Ltd, information, infrastructure, network segments, and devices.

Audience

The audience for this policy is all Jindal Saw Ltd employees, including its subsidiaries and partners, affiliates, contractors, trainees, guests, and volunteers who are provided with authorized access to Jindal Saw Systems as per directions of management. The aforesaid titles will be referred collectively hereafter as “Jindal Saw Ltd”.

Information Security Risk:

IT security risks can be broadly categorized as internal and external risks, each of which poses unique challenges and potential consequences for an organization.

Internal IT Risks:
Internal IT risks originate from within the organization and are often related to the people, processes, and technologies used within the company. Some common examples of internal IT risks include:

Human Error: Mistakes made by employees, contractors, or other personnel can lead to data breaches, system failures, and other security issues. This can include accidental deletion of critical data, misconfigured systems, or falling victim to phishing attacks.

Insider Threats: Employees or other trusted individuals with malicious intent can misuse their access to systems and data. This might involve stealing sensitive information, intentionally causing system disruptions, or using their privileges to exploit vulnerabilities.

Data Loss: Inadequate data backup and recovery processes can result in permanent loss of critical business data due to hardware failures, software glitches, or accidental deletions.

Poorly Designed Processes: Inefficient or outdated IT processes can lead to errors, delays, and increased security vulnerabilities. This might include lack of proper change management procedures, inadequate access controls, or insufficient disaster recovery plans.

Lack of Training: Insufficient training for employees can result in poor cybersecurity practices and unawareness of potential risks. Staff members might unknowingly engage in activities that expose the organization to threats.

External IT Risks:
External IT risks originate from sources outside the organization and are often related to threats posed by cybercriminals, competitors, or other external entities. Some common examples of external IT risks include:

Cyberattacks: External actors can launch various cyberattacks, such as malware infections, ransomware attacks, distributed denial-of-service (DDoS) attacks, and phishing campaigns to compromise systems and steal data.

Data Breaches: Cybercriminals may target an organization's databases or systems to steal sensitive customer information, employee data, financial records, and other valuable data.

Vendor and Supply Chain Risks: Third-party vendors and suppliers might introduce vulnerabilities into an organization's systems. If these third parties experience a breach, it could also impact the organization's security.

Regulatory and Compliance Risks: Organizations must comply with various laws and regulations related to data privacy and security. Failing to comply can lead to legal consequences and reputational damage.

Natural Disasters: Natural disasters like earthquakes, floods, and fires can disrupt IT infrastructure, causing downtime and potential data loss.

Emerging Technologies: The adoption of new technologies, such as Internet of Things (IoT) devices or cloud services, can introduce new vulnerabilities if not properly secured.

To effectively manage IT risks, organizations need to implement a comprehensive risk management strategy that involves.

- Identifying
- Assessing
- Mitigating and monitoring these risks.

This often requires a combination of technical measures, policy enforcement, employee training, and regular audits to ensure the organization's IT environment remains secure and resilient against both internal and external threats.

IT risk management strategy:

This refers to the structured approach an organization takes to identify, assess, mitigate, and monitor risks related to its information technology (IT) systems and infrastructure. The goal of an effective IT risk management strategy is to minimize the potential negative impact of IT-related risks on the organization's operations, data, and overall business objectives. Here's a step-by-step outline of an IT risk management strategy:

- **Risk Identification:** Identify potential IT risks that could impact the organization's IT systems, data, processes, and goals. This involves recognizing both internal and external threats.
  Categorize risks into different types, such as security risks, operational risks, compliance risks.

- **Risk Assessment:** Evaluate the likelihood and potential impact of each identified risk. This can involve using qualitative and quantitative methods to assign risk scores or levels.
  Prioritize risks based on their potential impact and likelihood. Focus on risks that have the highest potential to cause harm to the organization.

- **Risk Mitigation:** Develop a plan to mitigate or reduce the identified risks. This can involve a combination of preventative, detective, and corrective measures. Implement security controls, best practices, and technologies to address vulnerabilities and threats.
  Consider a layered approach to security that includes measures such as firewalls, intrusion. detection systems, access controls, encryption, and employee training.

- **Risk Monitoring and Reporting:** Continuously monitor the IT environment for changes that could affect the identified risks. Establish a mechanism for reporting and tracking incidents and breaches. Implement incident response plans to address security breaches promptly.
  Regularly review and update risk assessments as the IT landscape and the organization's objectives evolve.

- **Business Continuity and Disaster Recovery:** Develop and maintain comprehensive business continuity and disaster recovery plans to ensure the organization can recover from IT-related disruptions quickly. Test these plans periodically to ensure they are effective and can be executed smoothly during a crisis.

Policy Management

The Office of Information Security (OIS- Corporate IT Department) has a Chief Risk Officer who is responsible for the compliance of Information Security and Risk Management Process by implementing adequate security systems for all IT related equipment including network and network devices.

Chief Risk Officer

Detail of activities to be undertaken include:

- Risk Monitoring
- Risk Mitigation
- Maintenance of Risk Register
- Present annual risk update.
- Communicate information security risks to all stakeholders.

Risk Register and Reporting

The Risk Register is a comprehensive document that details out the following whenever there is an occurrence of a risk event. This information would be updated and securely kept at a central repository with authorized access. This information would be used for reporting as and when required.

The risk register shall comprise of the following components:

Date	Risk Number	Assessment ID	Risk Description	Existing Controls	Consequence	Risk Ranking	Risk Mitigation Strategy	Risk Owner
The date that risks are identified or modified. Optional dates to include are the target and completion dates	A unique identifying number for the risk.	Unique Identifier from risk assessment reports that identified the risk.	A brief description of the risk, its causes, and its impact.	A brief description of the controls that are currently in place for the risk.	The consequence (severity or impact) for the risk.	A priority list which is determined by the relative ranking of the risks by their qualitative risk score.	The action which is to be taken to reduce the risk.	The person who has the responsibility for the risk, manages the risk mitigation efforts, and the risk response if the risk occurs.

Reporting

The OIS would present annually to the Audit Committee and Board of Directors a report detailing strategic and operational risks identified and the steps taken to mitigate the same.

Data Governance

The primary importance of having this policy is to secure data and to set practices and standards related to quality, format, authorised access and retention of data. The concept of data governance includes the people and processes defined and enforced to handle / update / retrieve data properly and consistently. The policies and procedures is formulated to reduce ambiguity, establish clear accountabilities, and disseminate data-related information to all stakeholders as per directions of management.

Risk Management Performance

Performance will be identified and measured by:

- Information Security incidents that have occurred, investigation details, resolution and final analysis.
- Enhanced controls deployed to ensure non-reoccurrence of the same by either deploying appropriate systems and applications and / or change in SOP's.

Policy Review

This policy will be reviewed periodically once a year.