Information Security Policy

DOCUMENT IDENTIFICATION	:	PO-002
LATEST REVISION	:	2.1
REVISION DATE	:	30-09-2025

JSW
Better Everyday

Document Control Information

Document Title	:	Information Security Policy
Document No.	:	PO-002
Document Revision	:	2.1
Effective Date	:	30-09-2025
Document Classification	:	JSW Internal

Document Publication History

Document Prepared By	:	Jeevak Moon
Date of Creation/ Update	:	30-09-2025
Document Reviewed By	:	Manish Sehgal
Document Approved By	:	Harish Mehra
Initial Release Revision	:	1.0
Initial Release Date	:	15-11-2021

Document Revision History

Revision No.	Revision Description	Change Author	Change Reviewer	Change Approver	Revision Date
1.0	Initial Release	Abdul Dalvi	Usman Kathi	Dheeraj Sinha	15-11-2021
1.1	Annual Review- No changes	Karthik Iyer	Usman Kathi	Dheeraj Sinha	15-11-2022
1.2	Section 2- added Vision/ Mission statement Section 5.7. Modified: Exception process Added 8.3.4: clause for Loss of Media	Shweta Bharaswadkar	Usman Kathi	Dheeraj Sinha	20-11-2023
2.0	Aligned with ISO 27001: 2022 standard	Santoshi D	Umashankar Prajapati	Harish Mehra	19-02-2025
2.1	Updated reference for JSW Group companies	Jeevak Moon	Manish Sehgal	Harish Mehra	30-09-2025

Confidentiality Agreement

Note: The controlled master copy of this document is on the shared drive / Intranet Portal of JSW Group. Printed copies are not controlled. If you are working from a printed copy, please verify with the published version in the shared drive / Intranet Portal of JSW Group to ensure it is the latestrevision.

Authorized Signatory

Name: Harish Mehra, Group CIO

Date: 30-09-2025

Table of Contents

1. Introduction

JSW Group hereby refers to JSW Steel Limited, JSW Energy Limited, JSW Infrastructure Limited, JSW Cement Limited, JSW Paints Limited, and other Group companies and subsidiaries, hereinafter also referred to as "the Organization".

JSW Group's information assets and systems are of paramount importance to its business operations, customer service, and in a nutshell, to its existence. Due to the criticality of these systems and the information contained within, JSW Group treats information security as an integral part of its business risk management.

Information Security is the protection of Information and Information Assets, from a wide range of threats in order to safeguard business and profits. It is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Information Security Management System (ISMS) is an overall management system, based on a business risk approach, to establish implement, operate, monitor, review, maintain and improve information security. ISMS is a systematic approach to managing sensitive company information so that it remains secure. It encompasses People, Process and Technology.

It provides the following **benefits** to JSW Group:

- Protects the JSW Group information assets
- Manages and minimizes risk exposure
- Enhances customer satisfaction that improves customer retention
- Builds a culture of security
- Keeps confidential information secure
- Allows secure exchange of information
- Ensures meeting legal obligations
- Provides consistency in the delivery of service or product
- Security education, training, and awareness requirements.
- Business continuity requirements

1.1. Five design principles for Security at JSW Group

- Information Security is everyone's business
- Ensure all regulatory requirements are fulfilled – in compliance and in spirit
- Ensure Segregation of duties (e.g. design/ implementation v/s validate)
- Zero Trust in all aspects of Information Access
- Inculcate a strong security mind-set

2. Vision/ Mission Statement

Mission Statement: "To safeguard our stakeholders' trust by establishing and maintaining a robust Information Security Management System. We are dedicated to preserving the confidentiality, integrity, and availability of our information assets, ensuring compliance with relevant regulations, and continually improving our security posture to adapt to evolving threats."

Vision Statement: To be enabling partner to our core business of manufacturing not limited to JSW Steel, Energy, Cement, Paint as well as operations and maintenance to help them differentiate in marketplace and grow to fulfill expectations of stakeholders ensuring information security, business continuity and resilience. We aspire to create an environment where information security is ingrained in our daily operations, innovation is securely embraced, and our commitment to safeguarding sensitive data sets us apart as a trusted and reliable partner in the digital landscape.

3. Purpose

The purpose of this document is to demonstrate JSW Group's Top Management's commitment and directives for Information Security Management Systems (ISMS) and recommend appropriate security controls that need to be established, implemented, and maintained to ensure information security at JSW Group. Further, this policy shall establish a framework in JSW Group for the development of Standards, Procedures and Guidelines for information security and its implementation and compliance.

The broad objectives of this policy are enlisted below:

1. To strengthen internal controls and prevent threats to the JSW Group's information, thereby ensuring the appropriate protection to the information assets by regular monitoring.
2. To prevent unauthorized disclosure of information stored or processed on JSW Group's information systems (Confidentiality).
3. To prevent accidental or unauthorized deliberate alteration or deletion of information (Integrity).
4. To ensure that information is available to authorized persons whenever required (Availability).
5. To ensure that users are accountable for their actions (Accountability)
6. To ensure that the policies and related procedures are designed in such a way that it alignsto the Information Security Risk Management Framework.
7. To ensure that the information security posture of JSW Group keeps pace with the cultural maturity of the organization over the following stages: from ad-hoc to vulnerability driven; from vulnerability driven to cyber risk-driven; from cyber risk-driven to enterprise risk driven.
8. To ensure that appropriate technology, resources, and infrastructure are deployed within JSW Group.
9. To continually monitor, review, report exceptions and take actions thereon for improving the effectiveness of the Information Security Management Systems.
10. To ensure that appropriate measures are taken in case of any violation of the JSW Group

ISP.

11. To meet legal, regulatory, and statutory requirements that apply to JSW Group.
12. To create a level of awareness on information security as part of day-to-day operations at JSW Group, and to ensure that all end-users understand one's roles and responsibilities for maintaining information security.
13. To document specific information security standards, procedures and guidelines based on this policy and improve the overall capabilities of the Information Security Management System of JSW Group.

4. Scope

This document is applicable to all business and support processes and operations at JSW Group including information assets hosted by or on behalf of JSW Group across all geographies. Further, the policy applies to employees, consultants, associates, and suppliers / third-party personnel (contractors and their sub-contractors) having access to JSW Group information assets.

5. Objective

The objectives of the JSW Group Information Security Policies are:

- To strengthen internal control and prevent threats to the JSW Group information, thereby ensuring the appropriate protection of information assets of JSW Group through regular monitoring.
- To ensure the confidentiality, integrity and availability of information assets of JSW Group through maintenance of asset registers and risk assessment.
- To continually strengthen and improve the overall capabilities of the Information Security Management System of the JSW Group. This shall be assessed based security metrics designed for the organization and risk treatment methodology.
- JSW Group tracks the performance of its Information Security objectives and effectiveness of Information Security management system through defined Key Performance Indicators (KPIs). Also, it reviews, monitors and reports the same to senior management on periodic basis and takes appropriate corrective action.

6. Review Frequency

This document shall be reviewed annually or in response to significant changes in the existing organizational structure or technical infrastructure.

Any processes that are identified to be redundant during the review shall be withdrawn. The updated process shall be published on the Intranet after the review and notified to all JSW Group users through appropriate channels.

The owner of this document is the IT Security Team. The document shall be approved by Group CIO and the IT Security Head shall be responsible for reviewing and updating this procedure.

7. Leadership commitment and Direction for Information Security.

Objective

To provide management commitment, direction and support for information security in accordance with business requirements and applicable laws and regulations.

This ISP framework provides guidance on how JSW Group can assess and improve its ability to prevent, detect, and respond to information attacks. Information security within the organization depends on co-operation and a multi-disciplinary approach. Employees, contractors, and third-party personnel are responsible for maintaining a secure environment. Management of JSW Group shall provide guidance to create a secure environment with the help of an established security policy, define roles and responsibilities, and provide consistent direction and co-ordination towards security efforts. This policy framework aims to identify roles and responsibilities related to the protection of information assets throughout the organization.

The overarching principle of this ISP is decided by the JSW Group management and has the followingkey points.

- JSW Group will follow relevant as well as feasible security measures based on the changing threat landscape, threat prioritization relevant to the company and depending on the requirements of the security posture.
- JSW Group will balance its agility and security posture to enable and scale business.
- The first priority of security architecture will be to have maximum visibility in overall security posture and mitigate the incidents with people, process, and technology.
- JSW Group will continuously thrive to improvise the information security posture basis scale of business and financial considerations.

7.1 Information Security Policies

This policy shall provide management direction and support to various initiatives within the domains of the stated policy and shall be communicated throughout JSW Group users in a form that is relevant, accessible, and understandable to the intended audience.

7.2 Review of Documents related to Information Security

- All documents such as policies, procedures, guidelines, etc. related to information security shall be reviewed at least annually. Each document shall have an owner and shall be responsible to review and make amendments to the respective documents. The Group CIO and the Steering Committee shall be responsible to approve the changes.

- Records for the management review and approval shall be maintained by the document owner and can be asked to furnish during regular reviews or other related activities.

7.3 Risk Assessment

JSW Group shall define a process to identify, assess and evaluate risks to its information and information processing systems, and the potential impact on the business and support processes. Risk Assessment shall be performed on an annual basis covering various information and infrastructure assets and to prioritize the required controls based on the business impact and the likelihood of risk occurring.

The Head of the IT Security Department (ITSD) shall initiate risk assessment exercises by sending formal communication to various departments to perform the risk assessment activities.

Additionally, the risk assessment shall also be performed in case of any specific events as mentioned below, but not limited to:

- Major changes to processes, application, network, and security architecture
- Addition/ changes to information assets
- Emergence of new threats or vulnerabilities due to changes in the environment
- Triggers from business and regulatory changes, compliance, etc.

The scope of the risk assessments performed in case of the specific events as mentioned above, would be specific to cover potential information security risks that may arise due to thetrigger event. The risk assessment and treatment activities performed by the IT Security Department (ITSD) shall refer PO-004-Risk Management Framework.

A Risk Treatment Plan shall be defined by the Head of the IT Security Department (ITSD) in conjunction with the respective department Heads and same shall be communicated to the Group CIO and Steering Committee. Head of the IT Security Department (ITSD) shall overseethe status of risk treatment activities performed across various departments to manage the identified information security risks using appropriate governance mechanisms.

7.4 Policy Communication

1. JSW Group shall communicate the importance of information security through regular mailers, trainings, posters to all its end users.
2. Information Security Policy, Acceptable Usage Policy and other relevant documents suchas Framework, Procedures, Guidelines, etc. of JSW Group shall be communicated to all users on an annual basis and on every change.
3. These documents are intended only for the internal use by JSW Group, the recipient(s) shall ensure that this document is not reproduced or circulated to external entities without prior approval of the document owner. The IT Security Department (ITSD) shall display this policy on JSW Group Intranet Portalfor reference of all JSW Group personnel.
4. The Steering Committee shall identify the need for external public communication and communication shall be put into effect through JSW Group's established communication channels.

7.5 Policy Implementation

1. The Head of the IT Security Department (ITSD) shall be responsible for the implementationof this policy who in turn shall be assisted by designated team members for the maintenance and implementation within JSW Group's operating environment.
2. The IT Security Department (ITSD) in conjunction with the Human Resource Department (HRD) shall create non-compliances and post the same to relevant department heads for appropriate actions.

7.6 Policy Compliance

JSW Group expects all users including its employees, contractors, consultants, and suppliers / third-party personnel having access to JSW Group's information and information processing facilities / systems to comply with this ISP and other relevant documents. All personnel should sign an undertaking to abide by this policy. All violation or any attempted violation of this policy shall result in disciplinary action to be taken by HRD. Disciplinary action shall be consistent with theseverity of the incident, as determined by an investigation. Any violations of the policy must be reported to ITSD.

7.7 Exceptions / Deviations

Approval for exceptions or deviations from this policy and other relevant process, wherever warranted, shall be provided only after an appropriate assessment of the compensatory controls and risks arising out of providing such exceptions. This assessment shall be conducted by the ITSD. Exceptions shall be approved by the Head of ITSD, ITSD Head may delegate the approval authority for any similar or subsequent exceptions / deviations to IT Security Manager.

Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request. All exceptions / deviations, when approved, shall be for a minimum period and shall not exceed a year/month in any case. Any extension request shall be reviewed and assessed again by the approver before the expiry of the approved period.

Exception Grant

All exceptions must be fully documented and approved by ITSD in-line with the Security Exception form and retained by the ITSD as long as the exception exists. Also, ITSD must track and renew the existing exception annually.

The documentation must be completed and maintained by the Information Security team and must address:

- The value and sensitivity of the information asset at risk, including business consequences of its disclosure, destruction, modification, delay or misuse.
- The policy (or policies) to which exception applies
- A description of the risk and exposure that results from non-compliance
- Acceptance of the risks identified
- The business reason for non-compliance
- Any compensating controls that will reduce the risk to an acceptable level
- Any actions, which will lead to compliance, and a schedule to implement those actions.

7.8 Right to Monitor

JSW Group respects the privacy of its employees and users, however, it reserves the right to audit and/ or monitor user activities and information stored, processed, transmitted, or handled by the user using JSW Group's information systems. If any personnel found to be in breach of the security policies and procedures, may result in disciplinary action to be taken by HRD.

8 Information Security Governance

8.1 Information Security Organization

Objective

To manage information security within the organization and to define and assign security roles and responsibilities at all levels ensuring appropriate segregation of duties and basis the principle of need-based access.

8.1.1 Information Security Roles and Responsibilities

1. An information security organization shall be set up to undertake information security activities in accordance with the defined framework, policies, and processes. This organization structure for information security shall be clearly defined, reviewed, and updated as and when there is a structural change at JSW Group.
2. The information security responsibilities of users shall be identified, documented, and communicated to them. While defining roles and responsibilities within the organization structure, appropriate segregation of duties and the principle of need-based access shall be employed, wherever applicable, so that incompatible roles are not assigned to the same individual.

8.1.2 Segregation of Duties

1. Information security processes shall be adopted as per the principle of segregation of duties to the extent possible. The principle of least privilege shall be employed to reduce opportunities for unauthorized or unintentional modification or misuse of JSW Group's informationsystems and assets.
2. Whenever a process involves transaction of confidential information, the system shall include controls involving separation of duties or other compensating control measures to ensure that no one individual has exclusive control over the information assets.
3. In case of deviations to processes related to segregation of duties, a formal risk assessment shall be performed, and the exceptions shall be accepted by the corresponding department and business heads. These deviations shall be recorded for future references.

8.1.3 Contact with relevant Authorities

1. Contact with the government authorities / nodal agencies (law enforcement, telecom regulatory bodies, fire department, hospitals, emergency services, supervisoryauthorities

etc.) shall established.

2. A current list of authorities with appropriate contact details shall always be maintained and available to required personnel. This list shall be updated at least once in a year.
3. The organization shall identify and communicate to relevant personnel on when and by who in authorities should be contacted and how identified information security incidents should be reported in a timely manner.
4. Decision involving law enforcement regarding information security incidents or problems shall be taken by the Group CIO/ Steering Committee in conjunction with the Head of ITSD. Unless compelled by law to disclose attacks against its computer systems or networks, JSW Group may not report these incidents to the public or any government agency.
5. Contacts with authorities shall also be used to facilitate the understanding about the current and upcoming expectations of these authorities (e.g., applicable information security regulations).

8.1.4 Contact with Special Interest Groups

1. Appropriate contacts must be maintained with special interest groups such as security forums and professional associations by the Head of ITSD. This shall help gain access to best practices in information security, timely advisories, and warnings of alerts, specialist security advice and to create liaison points while dealing with information security incidents.
2. A current list of authorities with appropriate contact details shall always be maintained by the IT Security Team. This list shall be updated at least once in a year.
3. Specialist advice on security may be sought from either internal or external advisors, if required.

8.1.5 Information Security in Project Management

1. Project management activities carried out at JSW Group's premises or at supplier locations where JSW Group's information or information processing systems are located should be integrated with information security requirements.
2. The project team shall identify applicable information security objectives as part of the project management activities.
3. Controls required to implement and govern information security shall be identified and documented as part of the project implementation plan.
4. Implications of information security events should be addressed and reviewed regularly by the respective teams.

8.2 Internal Audit

- Annual Internal Audits shall be carried out to provide information on whether ISMS conforms to JSW Group's own requirements for its Information Security, the requirements of the standards and to evaluate effectiveness of the IT general controls. Corrective actions shall be taken in case of any non-conformity to the requirements.
- The effectiveness of the corrective action taken shall be reviewed and changes shall be made to the information security management system, if required.
- All the information documents related to the detection of non-conformity and rectifying shall be retained as evidence.
- The JSW Group shall plan, establish, implement and maintain an audit program that takes into consideration the importance of the processes concerned and results of previous audits.
- The audit criteria and scope shall be defined. Such audits need to be performed as per the Internal Audit Plan approved by the Audit Head. IT Security Head can consider the internal audit findings and recommend the action plan to remediate the same.

8.3 Management Review

Information Security Council shall review the Information Security posture of the JSW Group periodically to assess adequacy and effectiveness of the information security policy. Members of this committee shall review the following:

- Information incidents
- Feedback on information security performance
- Information security gaps and risk assessments outputs
- Security improvement plan
- Status of corrective actions implemented

8.4 Mobile Device and Teleworking

Objective To ensure the security of teleworking and use of mobile devices.

8.4.1 Mobile Device Policy

1. This policy applies to any mobile devices utilized to access JSW Group information and/or information systems. Access to JSW Group network and information through mobile devices shallbe provided based on a business need that is approved by the appropriate authorities.
2. Appropriate controls such as Mobile Device Management (MDM) solution, authentication, encryption, anti-virus software, latest patches, remote wipe-out, backups, etc. shall be identified, documented, and implemented to manage the risks associated with the usage of mobile devices.
3. Regular awareness sessions shall be conducted for users using mobile devices, to increase their awareness on the additional risks resulting from using mobile devices and precautions to be taken while using such devices.

8.4.2 Teleworking

1. Teleworking shall only be permitted to users with specific business requirements along with approval from appropriate authority for a definite period of time. Further, teleworking shall only be permitted and only if appropriate security arrangements and controls are in place at the teleworking site.
2. Data encryption and cryptographic techniques shall be implemented to ensure secure transmission and storage of data on devices utilized for teleworking. All authorized personnel shall be allowed to connect to JSW Group's network remotely using JSW Group VPN with two-factor authentication mechanism.
3. All access and activities including privilege access over teleworking shall be logged and the logs shall be preserved, protected, and reviewed regularly.
4. Security of information assets at teleworking site shall be ensured by the user, further, users shall also be responsible to provide appropriate care to ensure that JSW Group informationand information systems accessed during teleworking are not compromised.
5. All teleworking requests shall be reviewed periodically and advise on revocation of those that no longer have a compelling business justification.

8.4.3 Bring Your Own Device

1. All employees including temporary employees and suppliers who prefer to use their personally owned IT equipment for the official work purposes shall be explicitly authorized by appropriate authority to do so.
2. Such authorized users shall secure JSW Group information to the same extent as on JSW Group's owned IT asset and shall comply with controls laid down through this policy.
3. Appropriate controls such as MDM solution, authentication, encryption, anti-virus software, latest patches, remote wipe-out, etc. shall be identified, documented, and implemented to manage the risks associated with the usage of mobile devices.
4. Secure containers shall be created on personal mobile devices to segregate business information from user's personal information. Policies of MDM solution shall only be applied on such secure containers to ensure user's personal information is unaffected e.g.,remote wipe option shall be configured to only delete business information stored on the user's personal mobile device, however in the event user information is deleted by this remote wipe, JSW Group shall not be held liable.
5. JSW Group shall respect the privacy of user’s personal device and shall only request access to the device by technicians to implement security controls, as identified and approved by JSW Group management.

9 Human Resource Security

9.1 Prior to Employment

Objective	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

9.1.1 Screening / Background Verification

1. Information security controls shall be integrated in the Human Resource (HR) processes to protect JSW Group's interests as part of the process of joining, transfer, or separation.
2. All JSW Group employees including temporary employees and contractors shall be subject to screening/ background verification checks prior to employment.
3. Contractual agreements shall mandate suppliers/ third-party vendors to perform screening/ background verification for its personnel in line with this policy and policy on 'Supplier Relationship'. In exceptional cases, an authorized representative from the supplier/ third-party organization can sign a blanket agreement on behalf of contractors and third-party personnel.
4. The contract with any background verification vendor must clearly specify the vendor's data privacy obligation and responsibilities for the verification.

9.1.2 Terms & Conditions of Employment

1. Employees of JSW Group must sign and agree to the terms and conditions of employment contract before providing them access to the JSW Group information assets. These terms and conditions shall state JSW Group's as well as the employee's responsibilities towards information security and include responsibilities for maintaining the confidentiality and integrity of JSW Group's information and assets.
2. Employees shall grant JSW Group exclusive rights to patents, copyrights, inventions, or other intellectual property they originate or develop during their course of employment.
3. Contractors and supplier / third-party vendors including its personnel shall be required to sign a non-disclosure agreement before gaining access to JSW Group's information systems.
4. Employee's and supplier / third-party personnel's responsibilities for protecting the confidentiality of JSW Group information shall extend beyond the termination of employment / contract.

9.2 During Employment

Objective	To ensure that employees and contractors are aware of and fulfil theirinformation security responsibilities.

1. All staff and third-party personnel shall agree to perform their security responsibilities and comply with the requirements specified in the security policies.
2. All staff and third-party personnel shall be responsible for protection of any sensitive information and assets assigned to them.
3. All staff and third-party personnel shall use information processing systems and data

residing on systems for authorized business purposes only.

4. All staff and third-party personnel shall report any suspected information security incident or weaknesses to his/her reporting manager and Cyber Security team.
5. The Cyber Security team shall ensure relevant cyber security awareness education and training (upon hire as part of induction and subsequently periodic) for all staff of JSW Group and where relevant, third-party personnel.
6. The Cyber Security team shall monitor, review and measure the effectiveness of cyber security awareness through internal compliance and awareness tests.
7. The Business IT Head shall report all information security breaches committed by any employee to the HR head for taking necessary disciplinary actions against them.

9.2.1 Management Responsibilities

1. A code of conduct as part of acceptable usage policy must be used to cover employees, contractor and supplier / third-party user's responsibilities regarding confidentiality, data protection and appropriate usage of JSW Group's equipment and facilities.
2. All employees, consultants and third-party personnel who have access to JSW Group's information assets shall sign the acceptable usage policy and NDA stating the protection of JSW Group's information and assets.
3. Management shall require employees, contractors, and third-party personnel to apply security controls in accordance with JSW Group's established policies and procedures.
4. Management shall ensure that employees, consultants, and third-party personnel provide a commitment to confidentiality and adherence to JSW Group information security policies and procedures.

9.2.2 Information Security Awareness, Education and Training

1. Information security training and awareness programs shall be provided by the ITSD Head or designate to employees, contractors, and supplier / third-party personnel to create consciousness about the information security policies and processes as well as information security initiatives deployed.
2. Awareness training shall commence with a formal induction process designed to introduce the JSW Group's security policies and expectations before access to information or services is granted.
3. Employees, contractors, and supplier / third-party personnel shall undergo a mandatory information security awareness training at-least annually.

9.2.3 Disciplinary Process

The violation of JSW Group security policies and procedures by employees shall be dealt with through a formal disciplinary process maintained by HRD. The disciplinary process shall ensure correct and fair treatment of employees, contractors and supplier / third-party personnel who are suspected of having committed breaches of security. The disciplinary

process may include a written warning to the user, strict actions in terms of penalties and even termination in case of policy violation and as deemed by the disciplinary committee. HRD shall communicate to all personnel, this formal disciplinary process.

9.3 Termination and Change of Employment

Objective To protect the organization's interests as part of the process of changing or terminating employment.

9.3.1 Termination or Change of Employment Responsibilities

1. Termination of employees, contractors and supplier / third-party personnel shall be performed in an orderly manner based on legal contracts between the parties. Exit clauses must be followed; JSW Group's information available with such resources shall be verified and handed over to JSW Group authorities post which exit shall be authorized.

2. The assets of JSW Group available with terminated individuals shall be taken back and all their access rights (both physical and logical) shall be revoked immediately. In case access needs to be retained, the same shall be approved by the HR team and resp BU Head.

3. JSW Group shall take into consideration the changes of responsibility or transfer of employees, contractors and supplier / third-party personnel and access the appropriateness of their access when such occasions arise.

4. HRD shall notify relevant stakeholders including IT Infrastructure Department and Administration and Physical Security Department about the transfer or termination of any employee and any other supplier / third-party personnel or contractors of the JSW Group within a definite time period and the user ID of the employee, supplier / third-party personnel or contractor shall be within a defined time period. Wherever HRD has no role to play, the immediate manager / respective Department Head shall submit a request to relevant stakeholders.

5. Employees, contractors, and supplier / third-party personnel shall return JSW Group's provided assets in their possession upon termination of their employment, contract, or agreement and ensure that in such cases all copies of JSW Group owned information in their possession is revoked or deleted.

6. Users shall not be encouraged to store personal data on JSW Group provided IT systems. However, in cases where such events are witnessed, the IT Team may return the same to the employee post due diligence and a written communication to the IT Security Team.

7. The activities performed by a third party may be subject to additional monitoring at the time of termination or change of employment, on communication from respective Business representative in co-ordination with JSW Group IT.

8. In the case of a contractor provided through an external party, the termination process is undertaken by the external party in accordance with the contract between the organization and the external party.

10 Asset Management

10.1. Responsibility for Assets

Objective To identify organizational assets and define appropriate protection responsibilities.

10.1.1. Inventory of Assets

1. An inventory of all JSW Group IT assets shall be listed in an 'IT Asset Inventory'. This asset inventory shall be prepared and maintained according to the process defined in the 'Asset Management Procedure'. Further, an information asset register shall be defined in accordance with ‘Information Security Risk Management Framework’.
2. Each asset shall be clearly identified individually and (if appropriate) collectively in combination with other assets to form an identifiable asset.
3. Ownership of this inventory shall be formally established. It should contain all pertinent information relating to the operation and maintenance of these assets.

10.1.2. Ownership of Assets

1. All identified assets shall be 'owned' by designated individuals within JSW Group.
2. The asset owner shall classify the information assets in the asset register as based on its criticality in accordance with the 'Information Security Risk Management Framework'.
3. The asset owner shall ensure appropriate controls are implemented to protect the assets. These controls shall be implemented in compliance to the documented informationsecurity policies, standards, minimum baseline security standards, procedures, etc.
4. The completeness and accuracy of the defined asset inventory and asset register shall be verified by means of a physical asset verification on periodic basis.

10.1.3. Asset Register

1. Business heads or Business SPOCs shall develop and maintain an asset register containing all assets within their business function.
2. The asset register shall contain at a minimum, the asset type, asset location, owner, custodians and name of the function/processes that use those assets.

10.1.4. Acceptable Use of Assets

All users shall acknowledge and follow the practices laid out in the ‘Acceptable Usage Policy’. Any breach in this regard may result in disciplinary action.

10.1.5. Return of Assets

1. JSW Group shall ensure that employees, contractors, and suppliers must forfeit access to information assets owned by JSW Group on termination of employment or contractual agreement.

2. Physical assets assigned to employees, contractors and supplier / third-party personnel must be returned to the respective department before termination of employment or contractual agreement.

3. The HRD shall initiate the off-boarding exercise, post which accesses to the assets shall be revoked and IT Infrastructure, Administration and Physical Security Department and other relevant departments shall ensure return of assets allocated to the user. The final settlement process shall ensure/ manage return of assets to JSW Group.

10.2. Information Classification

Objective To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

10.2.1. Classification of Information

1. All documents / information created by JSW Group or received by JSW Group shall be classified for confidentiality and protected and handled in line with the information classification schemeas defined in the 'Asset Management Procedure'.

2. Information of JSW Group shall be classified based on its relative business value, legal requirements, and impact due to loss of confidentiality, integrity, and availability of the information. The level of security shall be identified based on the classification applied.

3. Information shall be classified using JSW Group's Information Classification Guidelines.

Classification Category	Definition	Examples
Confidential	This classification applies to the most critical business information, which is intended strictly for use within JSW Group. Its unauthorized disclosure could adversely impact JSW Group's business, stockholders, business partners and/or its customers, leading to legal and financial repercussions and adverse public opinion. The information that sometimes considered being private is included in this classification.	Business Plans, Business Strategies, Financial Plans and Records such as Un-published financial statements, Trademark/ Patent Formulas/ Molds, Custom Process Techniques used, Customer details, JSW Group Price details, In-house developed application code, Network Diagram, Employee information, etc.
Internal	This classification applies to general information, which is accessible to a wide circle of JSW Group employees but is not intended for outsiders. While its unauthorized disclosure is against the	Training Materials, JSW Group Policies and Procedures, SOPs, Internal Staff Circulars, Access Review Reports / Mails,

Classification Category	Definition	Examples
	policy, it is not expected to adversely impact the JSW Group's business, employees, customers, stockholders and/or business partners.	Change Requests, Patch Deployment Reports, IT Help-desk Requests etc.
Public	This classification applies to information, which has been explicitly approved by the JSW Group's management for release to the public. This classification applies to information, which has been explicitly approved by JSW Group's management for release to the public	Published Financial Statements, Information available in public domain, Website, etc.

10.2.2. Asset Retention and Disposal

1. Information owners shall define types of records and their retention requirements.
2. Records which are no longer active shall be archived for a period of time as set forth in the JSW Group Data Retention Schedule.
3. Information shall be disposed when no longer needed subject to its retention schedule and approval by asset owner.
4. Hardware assets and electronic records shall be disposed in a secure manner in accordance with the Asset Disposal guidelines.
5. All assets destroyed in compliance with this policy shall require ‘e-waste certificate’ to be retained as per defined policy.
6. Prior to disposal of system devices like Hard Drives, RAMs, etc., the same shall be sanitized by use of techniques like degaussing, low-level formatting, or physical destruction to ensure that data cannot be reconstructed.

10.2.3. Labelling of Information

1. Labels are physical or digital markings that clearly state the classification level of the information.
2. Wherever possible information shall be labelled with the classification level determined bythe asset owner before being released for use. Asset owner shall ensure that the

labelling of information is carried out as approved and the user or the recipient of this information shall consistently maintain the assigned classification and label.

3. Unlabeled information/ information assets shall be viewed as per the nature of the information.
4. Labels for sensitive information should appear on the outside of any removable storage media. If a storage media contains information with multiple classifications, the most sensitive category should appear on the outside label.
5. All equipment and physical assets must be tagged with the unique identifier (Asset ID).

10.2.4. Handling of Assets

The level of protection during access, storage, transmission, disposal, etc. for assets shall bein proportion to information classification and as per the process defined in the 'Asset Management Procedure'.

10.3.Media Handling

Objective To prevent unauthorized disclosure, modification, removal, or destruction ofinformation stored on media.

10.3.1. Management of Removable Media

1. By principle, access to removable media shall not be allowed to be used within JSW Group's environment. However, in cases where the usage cannot be avoided, an exception shall be approved in accordance with the process defined in 'Asset Management Procedure'.
2. Only JSW Group issued removable devices shall be used and for sensitive information media with encryption facility shall be used.
3. Removable media such as tapes, disks, removable hard drives, shall be stored in a safe and secure environment with access to authorized persons only. Theft or stolen removable media should be reported immediately to IT Infrastructure and IT Security Department.

10.3.2. Disposal of Media

1. Media / assets containing critical and sensitive information shall be disposed of in a secure manner post end of life status or in-case media is unusable. Prior to disposal of removable media, all data shall be securely deleted, or the media shall be destroyed.
2. Disposal shall be done only by authorized users and a formal report of the secure disposal of media containing internal and confidential information shall be maintained as per the process defined in 'Asset Management Procedure'.
3. During cases of donation of old media/ assets, JSW Group shall ensure that the HDDs are formatted multiple times to ensure that data cannot be restored; Low level formatting

shall be performed on the media drives.

10.3.3. Physical Media Transfer

1. Media / asset containing JSW Group information must be appropriately protected (encryption and authentication protection enabled) against loss, theft or inadvertent disclosure when beingtransported outside of JSW Groups premises.
2. Media / asset transfer shall be documented & approved by relevant authorities as definedin 'Asset Management Procedure'.
3. Where supplier / third-party is involved as a part of the physical transfer of media / asset containing JSW Group information, terms and conditions of service shall be agreed.

10.3.4. Loss of Media/ Asset

1. Loss of media or asset containing JSW Group information shall be informed to the IT Security Department, and the user shall report an information security incident immediately via the following channels:
   - Incident reporting tool;
   - Email (100@JSW Group.in); and
   - Telephone (in-case of non-availability of portal) 1800 419 8676.
2. If applicable or suggested by above team then, lodge a complaint with the local authorities.

11.Access Management

11.1. Business Requirements of Access Controls

Objective To limit access to information and information processing facilities.

11.1.1. Access Control Policy

1. Except for the publicly held / available JSW Group information, access to all other information / information assets, systems, applications, equipment, network and security devices and premises shall be granted based on the legitimate business needs and after the requisiteapproval is obtained.
2. Access to JSW Group's information assets shall be according to the principles of 'least privilege'and on a 'need to know' basis that is specific to the individual's roles and responsibilities.
3. Principle of segregation of duties shall be established during provision access, for e.g., segregation of duties shall be ensured among personnel responsible for requesting, approving, and administering access to information assets.
4. Procedures shall establish to support the secure creation, amendment, review, and revocation of user's logical and physical access to information assets and information processing facilities.

5. Information systems, applications, equipment and network and security devices shall usea centralized authentication mechanism to authenticate users based on a single user ID and password. In absence of the centralized authentication mechanism, a local authentication system shall be used as a primary mechanism to authenticate users.
6. User IDs shall be linked to specific individuals and shall not be associated with computer terminals, departments, or job / role titles unless duly authorized.
7. Users (employees, contractors, and supplier / third-party personnel) shall be responsible for the activities carried out using their user IDs and passwords or any other authentication mechanism. If a user suspects any malicious activity, then change the password and reportsuspicious activity to IT Security Department immediately.

11.1.2. Access to Networks and Network Services

1. Access to networks and network services shall be restricted based on the business requirements and shall be handled in accordance with this policy and defined procedures.
2. Groups of information systems, services, and users shall be segregated appropriately onthe network, e.g., users shall be provided access only to those areas of the network and systems for which they are authorized.
3. Wherever required, additional controls such as multi-factor authentication, secure VPN tunnels or encrypted sessions shall be used to access remote network services. JSW Group networks shall not be connected with any un-trusted voice or data networks, unless the voice / data exchange channels are encrypted and other security measures (such as authentication, authorization, audit logging and monitoring etc.) are in place along with approval from the ITSD and Infrastructure Department.
4. When using JSW Group’s IT systems, or when conducting official business, users shall not deliberately conceal or misrepresent one’s network identity.
5. Users remotely accessing internal networks shall ensure that they are authenticated through appropriate mechanisms prior to accessing JSW Group network / systems (both in-houseand SaaS based systems).
6. Corporate networks and guest wireless networks shall be segregated. Access to guest networks shall be authenticated and such networks shall only provide internet access. Guest network access shall be provided to visitors or third-party personnel based on a formal request that is approved by respective department heads. Guest access shall be time bound.
7. Access to intranet portals shall be granted to supplier / third-party personnel shall be based on a valid business justification basis and be approved by the respective Department Heads and Head of ITSD.
8. Usage and activities performed on JSW Group's network and network services (including guest networks) shall be logged and monitored.

11.2. User Access Management

Objective To ensure authorized user access and to prevent unauthorized access to systems and services.

11.2.1. User Registration and De-registration

1. Access Management Procedure shall be defined and documented to encompass all stages in the life cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems, applications,equipment, etc.
2. The user IDs shall clearly indicate the responsible individual's name, and under no circumstances such user IDs permitted tobe generic, descriptive of an organizational title or role, descriptive of a project, or anonymous. Naming conventions shall cover all end users, contractors, consultants and vendors. In case of exceptions, the same shall follow an approval mechanism.
3. Generic user IDs where necessarily required as an exception shall be assigned to a nominated user post approval from the respective Business Head or Business SPOC. The nominated user along with the Business head shall maintain accountability, by whom, when and for what the generic ID is used.
4. The use of Group and shared IDs shall be restricted and if it is absolutely required to use shared IDs, monitoring of such accounts shall be established to ensure traceability/audit trails of usage to individual users.
5. Unique system user IDs shall be created for all application, operating system and service accounts IDs shall not be used for login by a user but shall be reserved for application operability and system interoperability.
6. Upon creation of user ID, the new user shall be provided only standard and limited privileges required to perform duties.
   A formal record shall be maintained, and be available for review, of all user registrations and de-registrations on JSW Group resources.

11.2.2. User Access Provisioning

1. A formal user access provisioning process shall be implemented to assign access rights for accessing information / information systems and information processing facilities.
2. Access to JSW Group's information / information systems and information processing facilities must be in accordance with the principles of 'least privilege' and 'need to have' basis
3. Access shall be provisioned based on the authorization as defined in 'User Access Management Procedure'.
4. The administrator of Information systems shall not grant a user, access to any system without the authorization of the user's supervisor or manager.
5. Role based access shall be provided based on the systems profiles defined by the system and business owners.

11.2.3. Management of Privileged Access Rights

1. Privileged access rights shall only be provisioned to users on a need-to-use and on an event-by-event basis. Such access shall be enabled based on the least privilege requiredto perform user's job responsibilities and based on approvals from appropriate authorities. These approvals should be documented and produced when requested.
2. Administrator / privilege accesses shall be granted through a central solution such as a Privilege Identity Management (PIM) / Privilege Access Management (PAM). Wherever accesses through PIM / PAM is not feasible such as in-case of 'legacy applications', a direct console access shall be granted. Such accesses shall be authorized by applicationowner and respective department heads.
3. Approval from Head of IT Infrastructure shall be obtained before granting administrator rights to users. This access shall be used for legitimate business purposes and shall be removed when no longer necessary.
4. All privilege access shall be time bound, and all activities performed using such access shall be adequately logged and monitored.
5. Local administrative rights shall be disabled on all workstations (laptops and desktops) provided to end users. Local administrative access shall only be enabled based on valid business justification and risk acceptance approved by Department Head, IT Infrastructure Head, and IT Security Head. All such privileges shall be time bound.
6. Privileged users must be authenticated using either two-step or two-factor authentication, wherever applicable. A quality password is required along with additional authentication such as biometric, tokens, OTP, authenticator, etc.
7. Changes to privileged accounts shall be logged.

11.2.4. Management of Secret Authentication Information of Users

1. All information systems shall be configured with parameters for password management, as specified in the 'Password Management Procedure'.
2. The password management system shall be based on the Authentication, Authorization and Accountability principle and capable of enforcing the defined password configuration parameters.
3. System root passwords shall be at the time of inceptions being stored in a sealed envelopein a fire safe environment. The custody of the same shall be kept with the Head of IT Infrastructure and shall be changed on an annual basis.
4. The identity of a user shall be verified prior to providing a new or temporary authentication information.
5. Authentication information, including temporary authentication information shall be transmitted to users in a secure manner (e.g. over an authenticated and protected channel) and the use of unprotected channels for this purpose shall be avoided.

6. Authentication information such as passwords or personal identification numbers (PINs) generated automatically shall be non-guessable and unique.
7. Randomly generated temporary passwords shall be provided to a new user initially and a password reset shall be enforced upon first login.
8. Vendor default passwords shall be changed prior to use.
9. Passwords shall be secured during transmission and storage.
10. Authentication information such as passwords shall be kept confidential and shall be shared only with authorized persons basis proper justification and approvals.
11. The password policy shall address the following at the minimum:
    - Password length should be a minimum of eight (8) characters for end users and for privileged accounts.
    - Passwords should be complex, consisting of any 3 out of 4 characters – lowercase, uppercase, numerals and special character
    - Users shall be forced to change the passwords after first logon.
    - Domain users shall be forced to change their passwords at least every 90 days. Passwords should automatically expire if not changed within 90 days. Expired passwords for end user accounts should result in a forced password change upon next sign in. Users should not use last 5 passwords (password history).
    - Privileged account passwords must be changed at least once every 90 days. Privileged Account Passwords should automatically expire if not changed within 90 days.
    - Default system privileged accounts such as root and administrator accounts are configured with ‘password never expire’ and the password shall be vaulted.

11.2.5. Review of User Access Rights

1. Information asset owners along IT Infrastructure Department shall be responsible for performing periodic user access reviews for all information systems.
2. User access rights shall also be reviewed in the event of any major change to information systems which involve a change to the existing user roles and privileges.
3. Appropriate corrections shall be taken to address discrepancies identified during such reviews.
4. Procedures shall be established to support execution of user access reviews on JSW Group information systems.

11.2.6. Removal or Adjustment of Access Rights

1. The rights of the user to access information systems shall be revoked/ disabled when:
    - Users no longer requires access; or
    - User ID was found to be inactive for 3 months or more
2. IT shall be ensured that user ID is disabled / deactivated / deleted within a definite

timeframe of from the date of termination of user employment / supplier contract.

3. Prior to revocation of access rights, the user ID shall be evaluated to identify their businessneed and backed-up. Approval from respective Department Heads shall be obtained for exceptions where an account has to be retained for an extended period of time after termination.
4. User ID's, especially for revoked/ disabled users, shall not be deleted from Information Systems to support effective audit trail.
5. Process shall be established to support timely revocation of access for absconding users and uninformed absences.
6. All vendor supplied default user IDs shall be disabled or removed where possible.
7. JSW Group systems to be scanned to identify orphan IDs, dormant IDs, unauthorized IDs, etc. Annually as part of quarterly ID validation process.
8. Request for change in the access right shall be documented and approved by the user's Manager or the respective Business SPOC.
9. Audit trails for all requests for additions, modifications or deletions of individual accounts and access rights shall be maintained.

11.3. User Responsibilities

Objective To make users accountable for safeguarding their authentication information.

11.3.1. Use of Secret Authentication Information

1. Users shall follow the policy defined in section 9.4.3 Password Management System andthe defined 'Password Management Procedure'.
2. Further, all users shall take due care to protect JSW Group information systems and servicesfrom unauthorized access, tampering and/or accidental damage.
3. Users shall read, acknowledge, and adhere to all the 'Acceptable Usage Policy' while accessing JSW Group information systems.

11.4. System and Application Access Control

Objective To prevent unauthorized access to systems and applications.

11.4.1. Information Access Restriction

1. Access to information systems, applications, equipment, database, network, and security devices, etc. shall be provided as per the Access Control Policy.
2. Business sensitive information shall not be stored on the personal cloud storage such as google drive, one drive, etc. Only the JSW Group's cloud storage environment shall

be used for storage of business sensitive information. Access control mechanisms shall be deployed accordingly to ensure that public drives are not accessible. Post authentication, the route shall be diverted to JSW Group's cloud storage.

3. Applications used for processing and storing the critical information shall not be hosted onthe shared server. All such applications shall be identified and documented by the application owner.
4. User access (except administrators) to data repositories shall be approved and recorded.
5. Application accounts created for inter-application access shall not be used by individual users.
6. Application access for critical applications shall be reviewed on an annual basis.

11.4.2. Secure Log-on Procedures

1. Information Systems shall be controlled through a secure log-on procedure.
2. Where technically feasible, an advisory warning message (login banner) shall be displayed by the systems to the user prior to initiating an information system. The warning message shall inform the person attempting to access the system that the use of the information system or service is governed by this policy, breach or contravention shall lead to internaldisciplinary action or legal proceedings. The warning message shall not provide any information that may aid or help a user with malicious intentions.
3. Information systems shall be configured to protect against any brute force log on attempts(e.g., extended waiting time after each failed logon attempt and/or block access after a specified number of failed attempts). Authentication failure messages shall be generic andnon-descriptive in nature.
4. Where technically feasible, information systems (including applications) shall have sessiontime-out control to clear the session screen and terminate both the application and the network sessions.
5. Information systems shall be configured to log all successful / unsuccessful login attemptsalong with its corresponding date and time.
6. Users shall be required to re-authenticate themselves after a specific period of inactivity.

11.4.3. Password Management System

1. A robust password management system shall be implemented to ensure quality passwords following industry-leading practices. A 'Password Management Procedure' shall be documented to define the password policy parameters to be configured in information systems.
2. The system shall enforce complex password and force changes after a defined period.

3. The allocation and management of secret authentication information like passwords andtokens shall be controlled and communicated securely.
4. Password shall be mandatory for all user accounts on all information systems connected to JSW Group network or any standalone information system.
5. The users shall follow JSW Group's practices in the use of secret authentication information and maintain the confidentiality of their secret authentication information at all times.

11.4.4. Use of Privileged Utility Programs

1. Access to various system utility programs that can override system and application controls shall be restricted to ensure that users do not obtain information or privileges other than what is required to perform one's job function and responsibilities.
2. Users should not be able to terminate, temporarily disable, uninstall, prevent start-up, or circumvent critical system controls such as anti-virus, encryption software, etc. Any such requirement must go through ITSD for review and approval.

11.4.5. Access Control to Program Source Code

1. Source code libraries or version control systems shall be maintained for applications developed at JSW Group or by supplier/ third-party vendor on behalf of JSW Group.
2. Program librarians shall be nominated by application owner to maintain the source code libraries.
3. Adequate access control mechanisms shall be adequately source code libraries to reduce the potential for corruption of the programs.
4. Access to program libraries shall not be granted unless approved by the respective application owner.
5. Access to the source code libraries shall be logged and monitored to prevent / detect unauthorized changes.
6. Program libraries shall be managed in accordance with the defined process in 'Application Security Lifecycle Management Procedure'.

12. Cryptography

12.1. Cryptographic Controls

Objective To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

12.1.1. Policy on the Use of Cryptographic Controls

1. 'Encryption and Key Management Procedure' shall be documented to define the process related to cryptography controls, standards, requirements, approved solutions, etc. to be

adopted for use / implementation / management of JSW Group information.

2. Cryptography / encryption solutions shall be implemented giving special consideration to the sensitivity of the information, which shall be determined in accordance with the information classification scheme. This is to ensure that business sensitive information is protected during storage and transmission.
3. While implementing this policy and relevant procedures, special consideration needs to also be given to the cryptography laws and regulations that might apply to the use of cryptographic techniques and to the issues of trans-border flow of encrypted information.
4. All encryption products and processes deployed on information assets shall be approved by Head of Information Security before deployment.
5. Encryption algorithms shall be implemented based on risk assessment.

12.1.2. Key Management

1. All cryptographic keys shall be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure.
2. Equipment used to generate, store and archive keys need to be physically protected and access to such keys shall be protected against unauthorized disclosure and stored in a secure manner.
3. Certificates, where utilized, shall be issued by the approved Certificate Authority. If Certificate Authority's private key has been compromised all subscriber certificates shall be revoked.
4. The contents of service level agreements or contracts with external suppliers of cryptographic services (e.g., with a certification authority), shall cover issues of liability, reliability of services and response times for the provision of services.
5. Process related to key management activities shall be documented.

13.Physical and Environmental Security

13.1. Secure Areas

Objective To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

13.1.1. Physical Security Perimeter

1. The external perimeter of the JSW Group's premises shall have a compound wall of solid construction. Adequate lighting should be provided all around the building perimeter.
2. All entries from to the external perimeter shall be guarded on a 24x7 basis by trained security guards.
3. All visitors shall be thoroughly checked by security person for any kind of weapons,

explosives, storage devices, removable media, and electronic devices.

4. All personnel should wear visible identification badge when they are within JSW Group's premises. Employees may challenge any stranger / visitor not wearing visible identification.
5. JSW Group premises must be logically / physically divided into different zones based on the on the criticality of the information assets hosted in the premises. Each zone must have an appropriate level of access restrictions and access authorization requirements.
6. CCTV cameras shall be installed at key locations of premises and due diligence should be ensured during monitoring. The CCTV recordings shall be retained for a specified period.

13.1.2. Physical Entry Controls

1. Process for management of the entry / exit controls for the JSW Group premises including secureareas shall be established and implemented.
2. JSW Group employees must be provided access to the premises as per the job responsibilities in the organization. All visitors to JSW Group premises must be authorized and be escorted by the JSW Group employee whenever in the premises.
3. Entry to all secure area should be controlled by electromechanical access locks such as swipe cards, biometric access, etc. Access to the secure area should be allowed only to those authorized. Access rights to the secure area shall be reviewed on periodic basis.
4. All access to the secure area by visitors shall be logged in a visitor register and be reviewed on periodic basis.
5. Process for physical access management to JSW Group premises including secure areas for allpersonnel including JSW Group employees, contractors, suppliers / third-party personnel shall be established and implemented.
6. Monitoring events and records for physical access (e.g., access cards, biometric access, etc.) shall be retained based on business and legal requirements.
7. In case of any major deviations/ suspected events noted, the same shall be notified to appropriate authorities.

13.1.3. Securing Offices, Rooms and Facilities

1. Access to offices, rooms and facilities should be provided to the personnel as required by the job responsibilities. Access to the secure area such as server room / data center must be provided only to the authorized personnel.
2. All facilities shall remain secured (24x7x365). Doors and windows of all rooms should be locked when unattended. Processing areas within restricted zones shall not be visible or identifiable from outside.
3. Where applicable, buildings / premises should be unobtrusive and give minimum indication of its purpose, with no obvious signs, outside or inside the building i.e., identifying the

presence of information processing activities. For e.g., not signage outside the building identifying the same as Data Centre building.

4. Appropriate level of security controls shall be implemented to prevent unauthorized access to facilities and facilities hosting critical equipment. Shared services facilities shall have dedicated / segregated information processing area.
5. All Directories and internal telephone books identifying locations of sensitive information processing facilities should not be readily accessible by the public.
6. The facilities shall comply with the local environment, health and safety laws and regulations.

13.1.4. Protecting Against external and Environmental Threats

1. JSW Group's premises must be fitted with appropriate firefighting devices at critical locations in order to arrest the fire and to avoid damage to the various equipment and resources of JSW Group. If required, specialist advice / services may be obtained on how to avoid such damages.
2. Safety measures like fire, earthquake and other emergency evacuation drills must be performed on periodic basis.
3. Appropriate safety measures shall be taken to avoid loss and damage due to water flooding or inappropriate drainage system within the premises of JSW Group.
4. Physical protection against damage from natural or man-made disaster shall be designed and applied.
5. Process for protection against damage from explosion, riots, civil unrest, and other forms of man-made disaster shall be designed and applied.
6. Controls may include the following examples:
   - Smoke and heat detectors & fire suppression systems
   - Multiple power feeds and Diesel Generators, Uninterruptible Power Supply (UPS) units
   - Entry and exit doors alarmed (forced entry, propped open) and/or monitored by security guards
   - Multiple communication feeds
   - Physical access control procedures
   - Redundant air conditioning
   - Temperature, water, and humidity monitoring systems
7. Necessary fire drills and trainings shall be conducted for all employees on a periodic basis in case of any emergency. Emergency evacuation drills shall also be conducted to ensure emergency evacuation.

13.1.5. Working in Secure Areas

1. All personnel should only be aware of the existence of, or activities within, a secure area only on a need-to-know basis.
2. All working in secure areas must be supervised.
3. Photographic, video, audio, any type of media or other electronic equipment shall not be taken into secure areas without authorization.

13.1.6. Delivery and Loading Areas

1. Access points such as reception area and other points such as loading and unloading areas, where unauthorized persons may enter the premises, must be controlled and isolated from information processing facilities.
2. Delivery staff shall not be allowed to gain access to the JSW Group premises. All delivery staff shall be restricted only up to loading / unloading area.
3. All movement of material carried in and out of the JSW Group premises must be duly authorizedand tracked. Incoming material shall be inspected for potential hazards before it is movedfrom loading / unloading area to the point of use.

13.2. Equipment

Objective To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

13.2.1. Equipment Siting and Protection

1. All equipment should be placed such that they are sited to minimize unnecessary access into work areas.
2. All the electronic office equipment including faxes, printers and EPABX, must be physically secured. Further, equipment shall be placed such that there is no risk from smoke, water, electromagnetic radiations, vibrations, and chemical effects.
3. In areas identified as secure areas specifically server room, data center, network and hub room, UPS room, etc. monitoring of environment controls such as temperature, humidity, heat sensors etc. shall be implemented. Standard temperature and humidity parameters based on the environment conditions must be defined and monitored as part of the daily operational activities.
4. Eating drinking and smoking in proximity to information processing facilities should be strictly prohibited. A specific marked zone for eating shall be established.
5. Security of IT systems may include:
   - Systems must be adequately protected from fire, water and pollution damage and power supply fluctuations.
   - Network hubs must be secured from fire, heat, dust, and water
   - Interception or damage to network cables must be controlled

13.2.2. Supporting Utilities

1. All information processing facilities shall be powered through uninterrupted power supply.
2. Key information systems must be protected from power surges / spikes and sufficient emergency power must exist to enable a managed shutdown of JSW Group systems in the eventof an emergency. Provision must be made to maintain appropriate Heating, Ventilating, and Air Conditioning (HVAC) controls in the server room / data center.
3. Media must be protected from physical damages like fire, moisture, and magnetic interference. Critical and confidential media should be kept in the fireproof safe to protect from fire.
4. JSW Group shall obtain periodic maintenance contracts for requisite supporting utilities.

13.2.3. Cabling Security

1. Adequate protection shall be applied to protect power and telecommunications cabling carrying data or supporting information services from interception or damage.
2. Power and telecommunication cables shall be underground, where possible, or adequately protected from any damage or vandalism by placing the cables in appropriate enclosures. All inspection and termination points of communication and data cables should be locked.
3. Network cables and their corresponding terminals shall be identified and marked.
4. All power cables should be segregated from communications cables to prevent interference.
5. A copy of documents, including the detailed physical network diagrams, showing cable routings and terminations shall be defined and maintained in a secure manner.

13.2.4. Equipment Maintenance

1. All equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications, with any repairs and servicing performed only by qualified and authorized maintenance personnel.
2. Record of all suspected or actual faults with preventive and corrective maintenance shall be kept.
3. In case of any faults, it has to be made certain that the latest list of point-of-contact is used for incident handling. And for this the list of point-of-contact is kept updated and distributed to all the required people.
4. Environmental controls must be installed to protect central / key equipment, where applicable. Such controls shall trigger alarms if environmental problem occurs.
5. Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
6. JSW Group shall obtain periodic maintenance contracts for all equipment.

13.2.5. Removal of Assets

1. Process for removing of assets along with appropriate authorization shall be established

and implemented.

2. Time limits for equipment removal should be set and returns verified for compliance.
3. Where necessary and appropriate, assets should be recorded as being removed offsite and recorded when returned.
4. The identity, role, and affiliation of anyone who handles or uses assets should be documented and this documentation returned with the equipment, information, or software
5. Spot checks may be undertaken to detect the unauthorized removal of assets and where unauthorized equipment is bought onto the site - e.g., video recording equipment. Spot checks shall be carried out in accordance with relevant norms and required legislation and regulations.

13.2.6. Security of Equipment and Assets Off-Premises

1. Regardless of ownership, the use of any equipment outside JSW Group's premises for information processing should be authorized by Physical Security and Administration and in case of IT assets by the IT Infrastructure Department in addition to approval by asset owner.
2. Equipment and media taken off premises should not be left unattended in public places. In the event of theft or tampering or equipment, the personnel tasked with securing the equipment should report the incident to IT security immediately.
3. Manufacturer’s instructions for protecting equipment should always be observed, e.g., protection against exposure to strong electromagnetic fields.
4. Controls for off-premises locations, such as home-working, teleworking and temporary sites shall be determined, and suitable controls applied as appropriate.
5. Cabinets, clear desk policy, access controls for computers and secure communication with the office.
6. When off-premises equipment is transferred among different individuals or external parties, a log should be maintained that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment.
7. Adequate insurance cover shall be in place to protect equipment.

13.2.7. Secure Disposal or Reuse of Equipment

IT hardware and equipment shall be disposed of only after approval. Further, appropriate data and media destruction should be performed prior to disposal. Disposal of retired hardware and media shall comply with prevalent environmental regulations and the media disposal process.

13.2.8. Unattended User Equipment

1. Equipment shall not be left unattended without adequate protection mechanisms (Physical and Logical controls)
2. Users shall be made aware of the security requirements and process for protecting

unattended equipment, as well as one's responsibilities for implementing such protection. Users shall be advised to:

- Terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g., a password protected screen saver
- Log-off from applications or network services when no longer needed
- Secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g., password access, when not in use.

13.2.9. Clear Desk and Clear Screen Policy

1. A clear desk policy for papers and removable storage media and a clear screen policy forinformation processing facilities shall be adopted to reduce the risks of unauthorized access, loss of and damage to information during and outside normal working hours.
2. The clear desk and clear screen policy shall consider the information classifications legal and contractual requirements and the corresponding risks. The following guidelines should be considered:
   - Sensitive or critical business information, e.g., on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated
   - Computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar user authentication mechanism when unattended and should be protected by key locks, passwords, or other controls when not in use
   - Privacy screens may be considered as an option while accessing sensitive information on user's desktop/laptop screens
   - Unauthorized use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) shall be prevented. Solutions may be deployed to identify printing of sensitive data by unauthorized personnel
   - Media containing sensitive or classified information should be removed from printers immediately.

14. Operations Security

14.1.Operational Procedures and Responsibilities

Objective To ensure correct and secure operations of information processing facilities.

14.1.1. Documented Operating Procedures

1. Wherever applicable, operating procedures shall be developed and maintained for IT processes of JSW Group to enable the system, network, and application team personnel to perform daily operations. The operating procedures for all the critical systems and applications shall have a unified process, implemented, and maintained by respective asset owners.

2. The procedure may encompass:
   - Any automated or scheduled processes that are running on the system or application
   - Day-to-day operational tasks that need to be performed by the operator
   - Actions performed when an error or an exception condition occurs, including the listed contact details of on-call and backup on-call personnel that may be required to assist or that may be dependent on that service
   - Actions required for the start-up, restart or shutdown of a specific system or application
   - Actions performed for the information system / application backup, recovery, or restoration
   - Any maintenance / support agreements with the details of the contact names and commencement and termination dates of agreements
3. Operating procedures may be developed as and when a new information system, application, equipment or a network device or service, etc. is introduced. System documentation in hard copy or soft copy format must be protected from unauthorized access, and must be kept in lock and key, in custody of system owner.
4. All system and application owners shall ensure that procedures are reviewed on period basis and all changes to operating procedures are authorized.

14.1.2. Change Management

1. All changes to IT assets (including applications, servers, systems software, network, and security devices, etc.) shall be recorded and classified.
2. Changes to IT assets shall be assessed for risk, impact, and benefits.
3. Changes shall be tested in a non-production environment for servers & applications before deployment.
4. Change requests shall be approved and implemented in a controlled manner.
5. Process related to change management activities shall be defined, established, and implemented that shall at least include types of changes, recording of changes, business and security approvals, impact assessment due to the change, testing the change and roll back procedures.
6. A Change Advisory Board (CAB) shall be formed for approving and tracking critical changes. Any deviations from the implementation plan shall be recorded and approved by the Change Manager and informed to CAB.
7. Changes shall be reviewed to ensure that they do not compromise security controls (e.g., by checking software to ensure it does not contain malicious code, such as a Trojan horse or a virus)
8. Status of Changes (e.g., successful, failed, cancelled, etc.) post activity shall be recorded and communicated to the change manager or change management team.
9. Back-out positions shall be established so that the system or application can recover from failed changes or unexpected results

10. Record of changes shall be retained as per requirement.
11. Changes to the system or application shall be performed by skilled and competent individuals who can make changes correctly and securely.
12. The change manager or change management team shall ensure that status of all changes is informed and updated by resp activity SPOCs within the required timeframe.

14.1.3. Capacity Management

1. JSW Group shall manage the capacity of IT infrastructure and human resources to meet the current and future agreed workload demands of business and to run daily operations without any disruption or performance degradation.
2. Capacity provisions shall be based on the criticality, projected capacity, and available resources to ensure availability of systems and information.
3. JSW Group shall identify the required actionable for capacity management to ensure effective performance of information systems and business processes. The action plan shall identify and consider the capacity requirements based on business criticality of the concerned systems, business requirements, Service Level Agreements, Memorandums of Understanding, and risk assessments.

14.1.4. Separation of Development, Testing and Operational Environment

1. Development, test, and production facilities and duties should be logically or physically separated to reduce the risks of unauthorized changes to the production system.
2. In cases where segregation of environments is not possible due to limitations such as legacy systems, unavailability of environment, development and test environments may not be segregated but production shall be segregated.
3. Changes to operational systems and applications should be tested in a Testing Environment prior to being applied to operational systems. All operating system changes to be approved and documented.
4. Compilers, editors and other development tools or system utilities should not be accessible from operational systems when not required.

14.2. Protection from Malware

Objective To ensure that information and information processing facilities are protected against malware.

14.2.1. Controls Against Malware

1. All information assets of JSW Group shall be protected against malicious code. Anti-virus & Anti- Malware solutions and processes shall ensure timely detection, efficient containment, anderadication of malicious code.
2. Controls shall be implemented to prevent unauthorized execution of Malware, Trojan, and Ransomware etc.

3. Timely update of Anti-virus & Anti-Malware solutions shall be implemented.

14.3. Backup, Retention and Disposal Policy

Objective To protect against loss of data.

14.3.1. Information Backup

1. Information assets (information and software) shall be backed up regularly, securely, and periodically tested for restoration to ensure continuity of service and availability of systems and information to JSW Group and its operations.
2. Backups of systems and information must be encrypted at-least for critical / sensitive information, and the frequency and extent of these backups shall be mutually agreed between IT Infrastructure Department and the information / system owner.
3. Suitable rotation schedules and secure off-site storage of information should also be established.
4. The ability to restore critical information and software should be tested periodically to ensure that information can be successfully retrieved from the backup storage / media.
5. Backup shall be retained as per JSW Group's business and regulatory requirements, as applicable.
6. Backups should be encrypted to protect sensitive information, when:
    - transmitted via a network to external storage facilities, particularly when engaging with a third party to support backup capabilities
    - stored on physical media, to prevent unauthorized access in the event backups are lost or stolen in transit to an alternative location, such as an off-site storage facility.

14.3.2. Information Retention

Data retention period shall be defined, and records shall be retained for the defined period. This shall be reviewed annually and updated with changes if any. Retention periods for data shall be decided based on the following,

1. JSW Group’s business requirements,
2. Legal or regulatory compliances,
3. Contractual obligations.

Records shall be maintained in a safe and secure environment. Records shall be protected from unauthorized access.

14.3.3. Information Disposal

1. All waste copies of sensitive information that are generated while copying, printing, or faxing shall be shredded using paper shredders/incinerators or shall be placed in locked bins clearly marked as containing confidential data.

2. If the data cannot be erased, then Media shall be physically destroyed prior to disposal in such a manner that data should be beyond retrieval.
3. Non-disclosure agreement shall be signed between the Organization and external contractor for outsourcing disposal. Certificates of secure disposal shall be obtained from external contractor.

14.4. Logging and Monitoring

Objective To record events and generate evidence.

14.4.1. Event Logging

1. Information systems, applications, equipment, network, and security devices, etc. shall have audit logging enabled.
2. The extent of audit logging shall depend on the business criticality of the information system and the data handled by the system.
3. Audit log for the system handling restricted, confidential, and sensitive information shall log at minimum the following:
   - User ID
   - Source IP address of the user's computer
   - Date and time of logon and logoff
   - Logon method, location, terminal identity (if possible), Network address
   - Records of successful and unsuccessful system access attempts.
   - Type of action performed
4. All logs shall be retained for all information system for a definite period of time as per the local laws / regulatory requirements or business / contractual requirements, whichever is higher.
5. Audit logs shall be archived and protected from unauthorized access, modification, and deletion.
6. Audit logs of critical systems shall be reviewed periodically. The review of audit logs shall include at minimum, the following:
   - Unsuccessful login attempts
   - Repeated password changes for a specific user ID
   - Account lock-out and resets
   - Privilege access review for critical servers using PAM
   - Actions that disable security features such as OS patches and antivirus
   - Actions that modify logging features or result in deletion of logs
7. Issues identified during the review, shall be acted upon, and tracked to closure.
8. Logs of all critical servers, network devices and system components that support security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, etc.) shall be stored, reviewed and monitored to detect malicious activities.

9. Critical Business applications and technical infrastructure shall generate appropriate event types (e.g. Object creation, login attempts etc.)
10. Critical servers and network devices shall be configured to log / alert creation and deletion of system-level objects.
11. Critical servers and network devices shall be configured to log / alert initialization, stopping or pausing of the audit logs.
12. Security relevant logging shall be enabled at all times.
13. Security-related event logs shall be analyzed regularly to help identify anomalies. Anomalies detected shall generate alerts in SIEM (Security information and event management) tool. Various use-cases to be defined in SIEM to detect security events covering all possible threat landscapes.
14. Security Operations Center (SOC) team shall monitor security alerts generated in the SIEM tool 24x7. Any incident identified or reported shall be handled as per Incident Management process.
15. Information relating to information security threats shall be collected and analyzed to produce threat intelligence.
16. The organization shall also subscribe and connect with special interest groups or other specialist security forums and professional associations with the aim to improve knowledge about best practices, receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities and stay up to date with relevant security information.

14.4.2. Protection of Log Information

1. Log information shall be protected against unauthorized access and alterations. Access tologs shall be provided on ‘need-to-know’ and ‘need-to-have’ basis.
2. The fault logs shall be active always and protected from unauthorized access, modification, or destruction.
3. Any changes to the audit logging configurations and parameter settings shall follow the change management process.
4. A back-up of log information shall be taken in "Read Only" format on a periodic basis and shall be stored at an alternate media / location.

14.4.3. Administrator and Operator Logs

14.4.3.1. Administrator and Operator Logs

1. The activities carried out by information system’s administrators and operators shall be logged
2. It shall be ensured that the system administrators and system operators do not have permissions to modify, erase or deactivate logs of their own activities.
3. Information systems shall have the capability to record, at a minimum the following activities:

- System boot and restart time
- System or application start, stop, re-initialization (with user identity and time of action)
- System configuration changes
- System errors and corrective actions taken
- Production applications start and stop times
- Remote logins outside of business hours / unexpected geographies

4. All administrator and operator logs shall be stored for a definite period and be reviewed on a periodic basis.

14.4.3.2. Fault Logging

1. All critical devices shall be configured to log faults recorded due to problems in information and communication systems.
2. Logs related to fault or inconsistent behavior shall be reviewed by competent personnel.
3. Corrective measures shall be initiated by the concerned system admin in consultation with the Head of IT Infrastructure and ITSD Head, as applicable.

14.4.4. Clock Synchronization

1. Information systems shall have national /regional time defined, based on the official time of the region / country it is supporting. The correct interpretation of the standard date / time format shall be ensured. The format shall be identical across all servers and network devices.
2. The real time clock of systems shall be set accurately to ensure the accuracy of audit logs, which may be required for investigation or as evidence in legal or disciplinary cases.
3. Information systems shall support time synchronization and must be maintained via Network Time Protocol (NTP) and must be configured to retrieve time from an authoritative and trusted single time source. The trusted time source shall be synched with global atomic clocks for accurate timing. Further there shall be a procedure that checks and corrects drift in the real time clock.
4. For legacy systems which do not support NTP synchronization, a weekly review should be carried out by respective asset owners to ensure that the time settings are closest to the adhered NTP settings.

14.5. Control of Operational Software

Objective To ensure the integrity of operational systems.

14.5.1. Installation of Software on Operational Systems

1. The use of software in JSW Group shall be to support business requirements and shall comply withits licensing requirements.
2. Software installation on JSW Group's assets shall be controlled and secured. Only approvedsoftware shall be installed on operational systems and user endpoints.
3. A list of approved and tested software (whitelist) with corresponding versions and prohibited software (blacklist) shall be maintained as applicable in the environment.

4. Vendor supplied software, Open Source and Freeware shall be assessed for any risks before deployment.

14.6. Technical Vulnerability Management

Objective To prevent exploitation of technical vulnerabilities.

14.6.1. Management of Technical Vulnerabilities

14.6.1.1. Secure Configuration

1. A document on Minimum Baseline Security Standards (MBSS) that outlines the minimum-security controls to be implemented on any information system shall be defined and implemented.
2. JSW Group's systems shall be configured as per applicable MBSS for providing security, reliability, and stability. Systems shall follow standard naming conventions for efficient identification.

14.6.1.2. Patch Management

1. Security operations team, Server team, Network Administrators, Database administrators and Application administrators are responsible for identification and validation of all patches related issues concerning their domain of work.
2. A formal Patch Management Process shall be established for applying patches to the information systems.
3. System owners shall be responsible for deployment of patches.
4. Patches shall be applied periodically to ensure that the systems are running at their optimum level.
5. Patches shall be applied to ensure that threats from the spread of viruses, worms and malicious activities are reduced to an acceptable level.
6. Delay in security patch deployment shall be tracked.
7. Application and System owners shall ensure that all patches applicable to applications and systems used by JSW Group are identified.
8. New devices shall be patched to the current patch level, as defined by the operating system vendor and supported by the application, prior to the device being connected to the production network.
9. IT infrastructure team shall submit the patch management report on periodic basis to the respective Business Units.
10. Respective system owners shall be responsible for patching of their systems.
11. The IT Security Team shall track all security patch implementations using the patch dashboard or patch status report. This is to ensure that all patches are installed on all system and also to keep a track of patches which are not installed.

14.6.1.3. Vulnerability Assessment & Penetration Testing

1. The technical vulnerabilities of information systems and infrastructure shall be identified and evaluated to ensure adequate measures are taken to address the associated risks.
2. All information systems shall be assessed and tested periodically for existing or newly discovered weaknesses / vulnerabilities by conducting Security Testing. It shall include Vulnerability Assessments, Internal / External Penetration Testing, Application Security Testing, Source Code Review, Secure Network Architecture Review, Configuration review etc. Information systems shall include, but not limited to, applications, servers, databases, operating systems, network & security devices, endpoint systems, etc.
3. All discovered vulnerabilities shall be reported and addressed appropriately to mitigate the identified risks within specified timelines.
4. Penetration testing of public facing critical applications shall be carried out by professionally qualified teams.

14.6.1.4. Application Security

1. All in-house developed applications shall be reviewed for security controls and any vulnerability found shall be mitigated before deploying in a production environment. Applications shall have controls to secure input, output, processing, and storage.
2. Application owner shall ensure that the vendor performs application security assessment of applications / modules /functionalities / APIs supplied to the JSW Group and shares findings along with closure status before deploying it for JSW Group's productive use.

14.6.1.5. Operating System Security

The operating system of all devices shall be configured to secure overlying technologies against known vulnerabilities.

14.6.1.6. Database Security

All databases shall be configured to ensure the security and integrity of data stored and processed.

14.6.1.7. Website Security

JSW Group's websites shall be hosted in a controlled and secure environment and configured to ensure the security of the information processed and published.

14.6.1.8. Virtualization

JSW Group shall ensure the protection of information during use of virtual platform within its infrastructure. Software patching, remote access, security controls including but not limited toinstalling antivirus, disabling shared or guest accounts, user account controls, monitoring andlogging, disk and network encryption, backups, and other relevant policies shall be followed for virtualized systems as well.

14.6.2. Installation of Software on Operational Systems

The installation of such software shall be carried out only by authorized personnel, wherever

possible it shall be done in a centralized manner. Users shall not install new or upgrade operating systems / applications / software on JSW Group systems.

14.7. Information Systems Audit Considerations

Objective To minimize the impact of audit activities on operational systems.

14.7.1. Information Systems Audit Controls

14.7.1.1. System Audit Controls

1. Audit requirements for access to systems and data along with the scope should be agreed with appropriate management.
2. System audits involving operational systems should be carefully planned and agreed tominimize the risk of disruption to business process.
3. Wherever access to operational system is required, it should be limited to read only access to software and data.
4. Access other than read-only should only be allowed for isolated copies of system files, which should be erased when audit is completed.
5. Complete audit procedures, requirements and responsibilities should be documented.

14.7.1.2. Protection of System Audit Tool

1. Any software audit tool used should be in isolated environment and only till the audit period.
2. All such audit tools should be deleted from operational system as audit is completed.
3. Access list of all systems should be reviewed after the audit and any special access given for audit purpose should be removed.
4. Any data extracted from operational systems for audit purpose should be deleted from the test systems.

15. Anti-Virus Policy

1. All servers, desktops and laptops shall have anti-virus agent installed. Infrastructure Team shall ensure that all new systems including desktops, laptops, and servers have anti-virus agent installed, pre-loaded and configured before provisioning.
2. Anti-virus agent installation shall be password protected to ensure that end users cannot uninstall the agent. The anti-virus agent shall be configured in such a way that end users will not have privileges to change any settings or to disable the agent.
3. Anti-virus agent shall be configured to scan all removable disks before use.
4. Anti-virus agent shall be configured to quarantine virus infected files if they cannot be cleaned.
5. Access to websites and other resources on the internet known to host malicious content shall be prevented using the web content filtering tool. Antivirus software shall be installed on the

Internet Proxy and if feasible configured to scan downloads/uploads for malicious code.

6. JSW Group shall employ anti-malware signature auto update features. After applying an update, automated systems shall verify that each system has received its signature update. JSW Group shall monitor anti-virus console logs to correct any systems that failed to be updated.
7. The infrastructure team shall submit reports on the status of the Anti-Virus protection to the IT Security Team.
8. Provisions shall be made for real-time triggering and monitoring of alerts related to virus/malware detection and necessary actions shall be taken to remediate the same.

16. Communications Security

16.1. Network Security Management

Objective To ensure the protection of information in networks and its supporting information processing facilities.

16.1.1. Network Controls

1. Protection of JSW Group's information in wired and wireless networks and its supporting information processing facilities shall be ensured.
2. Network configuration diagrams shall be maintained for all JSW Group sites. These documents shall be maintained up to date and shall be considered as 'Confidential' information.
3. All inbound and outbound points shall be protected at a minimum by means of firewalls and Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) or Threat Intelligence. Firewall configurations and rules shall be reviewed annually.
4. Access control shall be deployed to protect all resources on JSW Group’s network from both external and internal users. The devices shall be configured and managed in such a manner that access to resources is allowed after due validation and restricted to authorizedsystems and services.
5. Access to JSW Group network with non-JSW Group computing devices shall be provided with valid business justification.
6. Security attributes, service levels with vendors and other management requirements of all in-house or outsourced network services shall be agreed and implemented.
7. Strong controls including cryptographic controls, secure protocols etc. shall be used to safeguard the confidentiality, integrity and availability of data passing over public networks to connected systems.
8. Adequate redundancy shall be provided for JSW Group's network links and network & security devices.
9. Appropriate logging shall be enabled on network & security devices for recording security events.

16.1.2. Security of Network Services

1. JSW Group shall regularly monitor the ability of the network service provider to manage agreed services in a secure manner and to detect potential cyber security threats and events.
2. The security arrangements necessary for particular services, such as security features of network services, service levels, and management requirements, shall be identified where necessary. JSW Group shall ensure that network service providers implement these measures via contractual controls.

16.1.3. Segregation in Networks

1. JSW Group's network shall be segregated from external networks. All connections to external networks, known or unknown (including internet, networks of vendors), shall be authorizedand provided in a secure manner.
2. JSW Group shall ensure segregation of network for production, development / test systems.
3. Network services for shall be segregated into separate categories, groups and domains based on access and security requirements along with the respective information classification.
4. Controls shall be implemented in networks to segregate server and user segments, wired and wireless networks.
5. Information in transit and information systems using the JSW Group network shall be appropriately protected using perimeter firewall controls, network segregation and Virtual Local Area Networks (VLANs).

16.1.4. Remote Network Access

1. Network management controls shall be established to protect JSW Group's networks during remote access. All remote access to JSW Group’s network shall be highly restricted and allowed based on business requirements. Remote access shall be controlled by appropriate identification and authentication.
2. Access to the JSW Group’s IT facilities via public or other external networks shall be provided via multi-factor authentication and approved VPN(Virtual Private Network) infrastructure.
3. Remote privileged access shall be logged, monitored, and reviewed periodically.
4. Remote access request for third party vendor/consultant shall be raised by the JSW Group employee responsible for the vendor /consultant engagement along with proper business justification. The request needs to be approved by BU SPOC and Cyber Security Manager.
5. Remote user sessions shall be locked after a maximum period of 15 minutes of inactivity.

16.1.5. Wireless Security

1. The wireless network shall be deployed after assessing the security risks, implementation of mitigating controls and approval.
2. Wireless network devices shall be configured as per the security settings provided in the MBSS.
3. Strong authentication and encryption techniques shall be used to ensure the protection of wireless networks.

16.1.6. Internet Access

1. Users shall use the internet resources of JSW Group in ethical and lawful manner exclusively forbusiness purpose.
2. Unless approved by appropriate authority, no office shall have its independent internet connectivity for the purpose of web browsing by staff.
3. JSW Group shall provide the necessary protection when browsing and connecting to the Internet, and restrict access to suspicious websites, file storage sharing sites, and remote access sites.

16.1.7. Access to Third Party Users

1. The designated manager within JSW Group shall authorize and supervise access requirements for non-employees.
2. Basic information Security principles such as least privilege, Separation of duties and defense in depth shall be applied.

16.2. Information Transfer

Objective To maintain the security of information transferred within an organization and with any external entity.

16.2.1. Information Transfer Policies and Procedures

1. Process shall be defined, established, and implemented to protect exchanged information from interception, copying, modification, misrouting, and destruction.
2. Electronic information must be protected in a manner commensurate with its level of sensitivity.
3. Process for the detection of and protection against malicious code that may be transmitted using electronic communications shall be identified and implemented.
4. Personnel, external party, and any other user's responsibilities not to compromise the organization through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing etc.
5. Wherever possible, use of cryptographic techniques to protect the confidentiality, integrity, and authenticity of information.

6. Retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant JSW Group's business / contractual requirements, legislation and regulations.
7. Not leaving messages containing confidential information on answering machines since these may be replayed by unauthorized persons, stored on communal systems, or stored incorrectly as a result of misdialing
8. Advising about the problems of using facsimile machines or services, namely:
   - Unauthorized access to built-in message stores to retrieve messages
   - Deliberate or accidental programming of machines to send messages to specific numbers
   - Sending documents and messages to the wrong number either by misdialing or using the wrong stored number
9. Personnel should be reminded that they should not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.

16.2.2. Agreements on Information Transfer

1. Exchanges of information between JSW Group and any third-party shall be accompanied by a written agreement that specifies the terms of the exchange, and the way the software or information is to be handled and protected.
2. Exchanges of software between JSW Group and any third party shall be accompanied by arrangements pertaining to End User License Agreements (EULA), code ownership and intellectual property rights. The contract shall have escrow arrangements, wherever applicable and feasible.
3. Software that performs unattended file transfer to or from other systems must authenticate the user credentials unless the information being transferred is classified as Public.
4. Wherever applicable, below clauses, may be included:
   - Non-disclosure of information
   - Any special controls that may be required to protect sensitive items such as cryptography
   - Maintaining a chain of custody for information while in transit
   - Acceptable levels of access control

16.2.3. Electronic Messaging

1. The information involved in electronic messaging such as internet, intranet, email, and fax shall be protected from misuse of information, unauthorized access, modification, or denial of service.
2. An approved disclaimer shall be appended to all e-mails for external domains.
3. An Email service shall be configured in such a way that data leakage and entry of any spam and/or malicious code into JSW Group's infrastructure shall be prevented. All

official email messages and logs shall be retained as per legal and regulatory requirements.

4. All official email messages originated by users shall be retained as per legal and regulatory requirements.
5. Anti-virus software shall be configured to scan attachments in all emails. If a virus is found in an incoming SMTP mail, then the appropriate actions shall be taken to delete or quarantine the attachment.
6. JSW Group shall implement technologies to protect e-mail by analyzing and filtering e-mail messages and block suspicious messages such as spam and phishing emails.
7. Access to e-mail messages shall be restricted to JSW Group employees, consultants & contractors only.
8. JSW Group shall ensure that email systems are only accessed by individual users via their user IDs.
9. JSW Group shall prohibit the System Administrator to access the e-mail contents of any employee without prior permission.
10. JSW Group shall ensure that JSW Group's email is only used for business purposes.
11. Multi-Factor Authentication shall be required to access the email service remotely or through a Webmail page.
12. JSW Group emails that contain classified information shall be encrypted.
13. JSW Group shall archive the emails and perform backups periodically and according to business requirements.
14. Limits shall be defined for email attachments to ensure appropriate capacity management for each user's mailbox.
15. Incoming and outgoing email attachment shall be filtered at the email gateway. JSW Group email gateway shall be protected against Advanced Persistent Threats and Zero Day attacks shall be implemented.
16. Third party vendors shall not be allowed to send emails to external domains.
17. The organization shall prohibit:
    - Automatic email diversion to external email addresses.
    - Unauthorized private encryption of email or attachments.
    - JSW Group shall disable the Open Mail Relay service.

16.2.4. Confidentiality or Non-Disclosure Agreements

1. All users, including but not limited to employees, contractors, suppliers / third-party personnel shall sign confidentiality agreements.
2. Without specific written exceptions, all programs and documentation created by any employee for the benefit of the JSW Group, are JSW Group's property and all the employees providing such programs or documentation shall sign a standard Non-Disclosure Agreement (NDA)or a confidentiality clause authorized by Legal department.

3. Whenever communication / interaction with third parties necessitates the controlled release of sensitive information; a standard Non-Disclosure Agreement (NDA) or a confidentiality clause authorized by Legal department shall be signed with the third party prior to the release of the information.

17. Information Security Requirements information Systems

17.1. Security Requirements of Information Systems

Objective

To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

17.1.1. Information Security Requirements Analysis and Specification

1. Information security requirements shall be integrated throughout the information system development or integration project lifecycle, from initiation to completion. Security requirements and controls for new information systems shall be identified.
2. When developing information systems or evaluating vendor software packages, the requirements specification shall incorporate the automated controls and consider the need for supporting manual controls.
3. When any system or software is procured, the product and vendor shall be evaluated based on the business needs, and JSW Group standards and requirements. This evaluation criterion shall include appropriate security related considerations including input validations, process integrity controls and output validations.
4. Where the security functionality in a proposed product does not satisfy the specified requirement, then the risks introduced, and associated controls shall be reconsidered through in the risk assessment exercise.
5. Where additional functionality supplied with a product causes additional security risks, these functionalities shall be disabled, or the proposed control structure shall be reevaluated to determine if there are advantages from the enhanced functionality.
6. Contracts with the third-party vendors identified for development or maintenance of information systems shall address the identified security requirements.

17.1.2. Securing Application Services on Public Networks

1. All JSW Group information, classified as 'Restricted and Confidential', which is interchanged between the end user and the externally facing application shall be encrypted.
2. Adequate controls shall be identified and implemented to protect internet facing or externally facing applications. Such controls shall be designed and implemented to prevent any unauthorized access to information, ensure its availability and integrity, and protect

itagainst misuse.

3. Vulnerability Assessments (VA) and Penetration Testing (PT) shall be performed for all external facing applications, prior to implementation and thereafter on a periodic basis.

17.2.Security in Development and Support Processes

Objective To ensure that information security is designed and implemented within the development lifecycle of information systems.

17.2.1. Secure Development Policy

1. All software developed or customized for use by JSW Group shall follow industry good practicesto ensure it meets functional, security and performance requirements.
2. Procedures for secure development of systems and applications shall be established and implemented by JSW Group.

17.2.2. System Change Control Procedures

Changes to information systems shall be performed in accordance with the defined change management process.

17.2.3. Technical Review of Applications after Operating System Changes

1. Notification of operating system changes shall be provided in time to allow appropriate tests and reviews to take place before implementation.
2. Process for review and testing shall be carried established and implemented.
3. Upon making changes to operating systems, business critical applications shall be reviewed and tested to ensure there is no adverse impact on the organization's operations or security.

17.2.4. Restrictions on changes to software packages

1. Prior to being installed, new or different versions of the operating system and related systems software for multi-user production computers shall go through the defined change management process.
2. Vendor-supplied software packages shall not be modified without consulting the vendor.
3. Any requirement for change to such software shall undergo the change management process. If changes are essential, then original software shall be retained, and changes could be applied to a clearly identified copy.

17.2.5. Secure System Engineering Principles

1. Appropriate controls shall be implemented to ensure proper processing of applications. These would include audit trails, control totals and other validations that provide assurance over the accurate processing of applications.

2. Appropriate input and output data validations controls shall be identified and implemented to protect applications against accidental or deliberate errors. Bypassing data validation controls shall be prohibited.
3. Where applicable, authenticity and message integrity controls shall be implemented to ensure that sensitive application data in transit is not intercepted or altered.
4. Application shall be designed / configured to ensure:
    - All tasks associated with a particular process are completed in its correct sequence and cannot be manipulated or bypassed.
    - All pre-requisites are met before triggering a particular process.
    - Prevent multiple sessions with same login credentials from different machines.
    - Prevent multiple sessions of the application using different login credentials in the same machine.
    - Session timeout in case of inactivity and prompt for credentials while logging back in.

17.2.6. Secure Development Environment

1. JSW Group shall establish secure development environment for specific system development efforts including people, processes, and technology associated with system developmentand integration.
2. For applications to be designed and implemented with proper security requirements, secure coding practices and a focus on security risks shall be integrated into day-to-day operations and the development processes.
3. Secure programming techniques shall be incorporated in the entire Software Development Lifecycle (SDLC).

17.2.7. Outsourced Development

1. Third party developers should be subject to the same standards of secure coding practices at JSW Group and shall be bound by contract.
2. All outsourced software development activities shall be closely supervised, regularly monitored, and periodically audited.
3. The software developed by third parties, arrangements pertaining to licensing, code ownership and intellectual property rights shall be documented in the contract between JSW Group and the third party.
4. The development firm or the developer should provide reasonable assurance to JSW Group thatthe software package is free of bugs and vulnerabilities by performing a detailed vulnerability assessment / application security review. The results of the same shall be shared with JSW Group in case of bug release or a security fix release.

17.2.8. System Security Testing

Process for testing security functionality for new or updated information systems shall be defined and implemented.

17.2.9. System Acceptance Testing

Acceptance criteria for new information systems, upgrades / patches, and new versions shall be established and suitable tests of the system(s) shall be carried out prior to acceptance of the information system. Process for system acceptance testing for new or updated information systems shall be defined and implemented.

17.3. System Acquisition, Development, Planning and Maintenance Policy

1. JSW Group shall ensure that cybersecurity requirements are included in the entire lifecycle of information systems & applications, whether acquired or developed, and integrated as early as possible.
2. Security engineering principles should be established, documented and applied to information system engineering activities. Security should be designed into all architecture layers.
3. The IT Security function shall perform activities such as vulnerability assessments, configurations' review, for newly developed/acquired systems/applications. All findings shall be mitigated before going live in production environment.
4. The Application team shall perform activities such as secure configuration, hardening and patching of new applications prior to go live.
5. JSW Group change management process shall be followed when attempting to perform system maintenance and updates.

17.4. Test Data

Objective To ensure the protection of data used for testing.

17.4.1. Protection of Test Data

1. Data from the live / production shall not be utilized for testing purposes without an approval from the information / application owner.
2. If live / production data is used, the data shall be masked / sanitized such that no sensitive information exists on the data (including personal information) prior to moving it to the development / testing environments. Proper audit trail shall be maintained to identify copying and use of such data.
3. Test data shall be erased from the test system immediately after the testing is complete. Access controls implemented on the operational application systems, shall also apply to test application systems.

18. Supplier Relationship

18.1. Information security in Supplier Relationships

Objective To ensure protection of the organization's assets that is accessible by suppliers.

18.1.1. Information Security Policy for Supplier Relationships

1. Third parties shall ensure that information security is an integral part of their service delivery processes.
2. Restricted personal data including but not limited to; financial information, employee's details, customer details, which is in custody of the third parties, shall be adequately protected as per local laws and regulations and as per JSW Group's data protection policies andencryption schemes.
3. Third parties shall be responsible for developing and implementing security policies and procedures to safeguard restricted personal data from unauthorized access, damage, use, modification, disclosure, or impairment, as specified by JSW Group and applicable laws and regulations.
4. Supplier's access to information systems shall be limited as per the business requirements.
5. In the event of interconnection of business information systems with external entities such as third-party organizations, adequate measures shall be implemented to protect the information within the information systems.
6. To prevent loss, modification, destruction, or misuse of information, JSW Group must protect andcontrol exchange of critical business information assets and software with third parties andoutside organization.
7. Contracts shall also outline clauses for notification and reporting of unauthorized disclosure or confidential information leakage to JSW Group within the agreed timeframe.
8. Processes to ensure security controls are in effect and promptly acted upon must be developed and implemented.
9. For all major contracts, the third-party must name the functions responsible for information protection (both information security and data privacy) and provide contact details for the individuals serving in these lead roles within these functions and are responsible for protecting JSW Group data.
10. Appropriate due diligence shall be exercised in the selection and approval of new vendor/supplier before contracts are agreed.
11. The information security provisions in place with existing suppliers (where due diligence was not undertaken as part of initial selection) shall be clearly understood and improved where necessary.

18.1.2. Addressing Security within Supplier Agreements

1. The information security requirements of outsourcing the management and control of all or some on information systems, applications, equipment, network, and security devices shall be addressed in a contract agreed between the third-party and JSW Group.
2. Formal agreements must be established for the exchange of critical business information assets or software with outside organizations. The department requiring this exchange must be responsible for the formal agreements.
3. These agreements must include both physical and electronic exchanges of information.
4. These agreements must reflect the sensitivity of the critical business information assets being exchanged and must describe any protection requirements.
5. These agreements must specify management responsibilities, notification requirements, packaging and transmission standards, courier identification, responsibilities and liabilities, data and software ownership, protection responsibilities and measures.
6. Applicable clauses pertaining to information security shall be identified and incorporated into the legal agreements while outsourcing any service/work to a third-party.
7. Service levels are defined in the agreements shall be monitored and reported by third parties.
8. Third parties shall be subject to independent reviews at least on a periodic basis for their compliance with information security requirements.
9. Confidentiality and non-disclosure of JSW Group data shall be addressed in vendor contracts using legally enforceable terms.
10. Appropriate legal advice shall be obtained to ensure that contractual documentation is valid within the country in which it is to be applied.
11. If required, then separate non-disclosure agreement shall be made on Government stamp paper and it shall be used where a more specific level of control over confidentiality is required.
12. Contracts with third-party vendors shall include terms for complete deletion of data/ information at the end of the Agreement.
13. JSW Group shall have all rights to audit the information security practices of the vendor/supplier and, where appropriate, subcontractors.

18.1.3. Information and Communication Technology Supply Chain

1. Agreement/ contract with supplier should include requirements to address the information security risks associated with information and communication technology services.
2. Supplier shall be required to propagate the JSW Group's security requirements and appropriate security practice throughout the supply chain even if supplier subcontract for parts.

3. Implement a monitoring process and acceptable method of validating that delivered information and communication technology products and services are adhering to stated security requirements.
4. Identification of product and service components critical for maintaining functionality and therefore required increased attention and scrutiny when built outside of JSW Group.
5. Rules for sharing of information between supplier and JSW Group shall be defined along with potential issues such as compromise of information.

18.2. Supplier Service Delivery Management

Objective To maintain an agreed level of information security and service delivery in line with supplier agreements.

18.2.1. Monitoring and Review of Supplier Services

1. JSW Group shall ensure that all services to be provided by the outsourced party are clearly identified and the relationship with the outsourced party is managed through clearly identified point of contacts in JSW Group and the outsourced party.
2. A formal legally binding contract should be entered between JSW Group and all third parties providing service to JSW Group or using JSW Group's information systems. The services to be provided
   by the outsourced party must be covered by a strong Service Level Agreement (SLA) that takes into consideration expected levels of service, security, monitoring, contingency, and other stipulations as appropriate.
3. Security controls and service levels specified in the service level agreement should be implemented, operated, and maintained by the third-party.
4. Contracts shall include information security requirements to ensure compliance to JSW Group's security policies and procedures, and disciplinary action in case of violation of informationsecurity.
5. Non-Disclosure or Confidentiality agreements to protect JSW Group's information assets must besigned by suppliers, third parties and contractors to include the clauses on privacy, protection, security, and compliance with JSW Group's information security policy.

18.2.2. Managing Changes to Supplier Services

1. Any changes to the agreement / contract shall approved. The approval shall be provided based on valid business case, including at a minimum the following:
   - Reason for the change
   - Impact due to change
   - Criticality of the information / information assets, systems, applications, equipment and network and security devices, etc.
   - Exit plan (in cases of existing vendor change)

19. Information Security Incident Management

19.1. Management of Information Security Incidents and Improvements

Objective

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

19.1.1. Responsibilities and Procedures

1. The Head of ITSD is primarily responsible for ensuring adherence to this Information Security Incident Management Policy.
2. ITSD Head shall or by delegating define, establish, and implement an information security incident management procedure.
3. The responsibilities and process shall be in place to report and handle information security events and weaknesses effectively once these are reported. A process of continual improvement shall be applied to the detection, response, monitoring, evaluating, and overall management of information security incidents.
4. Appropriate detective mechanism shall be designed for timely detection of information security incidents. Preventive controls shall be put in place to minimize the occurrence of information security incidents.
5. All information security incidents shall be recorded, and learnings shall be available on a centralized platform.

19.1.2. Reporting Information Security Events

1. An incident is defined as the occurrence of any exceptional situation that could compromise the confidentiality, integrity and / or availability of information and information systems of JSW Group. It is related to exceptional situations or a situation that warrants intervention of senior management, which has the potential to cause injury or significant property damage.
2. JSW Group shall implement process for detecting and reporting incidents and responding to incidents related to exceptional situations in day-to-day administration of the IT / Non-IT and information security related areas.
3. Escalation matrix and communication processes shall be established
4. The incidents shall be reported in time to the appropriate authorities and corrective actions shall be taken immediately to avoid the recurrence of such events in future.
5. All employees, contractors, supplier / third-party personnel shall be made aware of the process for reporting different types of incidents (like security breach, threat, weakness, ormalfunction) that might have an impact on the security of JSW Group assets.

6. All personnel shall report any suspected information security incident or weaknesses to his/her reporting manager and Cyber Security team.
7. Security incidents shall be reported from all relevant sources, including users, audit process, SOC, advisory team, customers, etc.
8. All reported incidents shall be logged, analyzed, and classified according to the criteria.

19.1.3. Reporting Information Security Weaknesses

1. Security weaknesses (vulnerability in the information system, which could be exploited to compromise the confidentiality, integrity and / or availability of the system), software malfunctions (any abnormality or deviation in the functioning of a software application) and violations of JSW Group's security policies and procedures shall also be considered an incident.
2. All employees, contractors, suppliers / third-party personnel of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services including violation of JSW Group policies and procedures.

19.1.4. Assessment of and Decision on Information Security Events

1. Incidents shall be detected / reported, followed by classification and investigation based on the type of incidents and their respective frequency. ITSD shall act on the incidents once incident ticket is raised.
2. All incidents shall be categorized based on their criticality. The guidelines for prioritization of the incident shall be established
3. The classification of incidents shall be done based on business impact and should have the priority level assigned to them.
4. For critical incidents that need communication to be sent out to employees or customers shall be performed as soon possible.
5. For Incidents that need to be reported to CERT-In, same shall be reported as per JSW Group Information Security Incident Management Procedure.

19.1.5. Response to Information Security Incidents

1. Management responsibilities and process shall be established to ensure a quick, effective, and orderly response to information security incidents.
2. There shall be mechanisms in place to learn from incidents and enable the types, impacts, and costs of incidents and malfunctions to be quantified and monitored.
3. The notification and resolution timelines shall be defined based on the incident category.
4. An escalation process shall be established for timely resolution of incidents.
5. Where a follow-up action against a person or organization after an information security

incident involves legal action (either civil or criminal), chain of custody shall be maintained for evidence collected and retained.

6. IT Security Team shall verify all reported security incidents for closure and conduct post-incident analysis by reviewing the appropriateness of actions taken for closure, developing corrective actions and reassessing risk, and adjusting controls suitably to reduce the related risks in the future.
7. IT Security Team shall investigate the cause of all reported security incidents. Wherever required, they shall also verify the implementation of recovery solutions.

19.1.6. Learning from Information Security Incidents

1. Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
2. A mechanism shall be put in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
3. With due care of confidentiality aspects, anecdotes from actual information security incidents shall be used in user awareness training.
4. All security incidents and breaches shall be discussed with management bi-annually.

19.1.7. Collection of Evidence

1. JSW Group shall identify, collect, and acquire information which can serve as evidence for any information security incident.
2. JSW Group shall preserve such evidence for a definite period as per the business / contractualor any legal / regulatory requirements.
3. Where a follow-up action involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the legal requirements.
4. Third-party shall ensure appropriate forensic methods shall be utilized, whenever required, to collect evidence during investigation of information security incidents.
5. Where available, certification or other relevant means of qualification of personnel and tools shall be used, to strengthen the value of the preserved evidence
6. Forensic evidence shall transcend JSW Group or jurisdictional boundaries, in such cases, JSW Group shall ensure that it is entitled to collect the required information as forensic evidence.

20. Information Security Aspects of Business Continuity Management

20.1. Information Security Continuity

Objective Information security continuity should be embedded in the organization's business continuity management systems.

20.1.1. Planning Information Security Continuity

1. JSW Group shall define, document, and implement business continuity management processes throughout the organization.
2. A comprehensive Business Continuity Plan (BCP) must be developed and implemented to maintain or restore business operations in the required time scales following interruption to, or failure of, critical business processes.
3. The BCP must include effective Disaster Recovery procedures for quickly recovering from an emergency with minimum impact to JSW Group's operations. The Disaster recovery plan mayinclude, but not limited to current state assessment, threat and risk assessment, businessimpact assessment, disaster recovery strategy, disaster declaration plan and business continuity plan for all the critical applications and infrastructure.
4. The business continuity management processes shall include information security requirements to help ensure that confidentiality, integrity, and availability of critical information assets are preserved even in the event of a business disruption or disaster.
5. The ITSD shall be consulted for their input into the Business Continuity Plan and Disaster Recovery plan development. All the plans developed shall have consistent information with business and information security priorities clearly identified.
6. The scope of the Business Continuity Plan (BCP) shall consider applicable factors including customer requirements, legal regulations, and industry requirements. The following but not limited to; shall be considered while implementing any BCP program:
    - Identify critical business functions, applications and supporting technologies
    - Develop an appropriate cost-effective recovery strategy
    - Identify alternate / backup locations with the necessary infrastructure to support the recovery needs
    - Identify the management and membership of the disaster response and recovery teams
    - Identify and document the required recovery actions, identify, and ensure the availability of required resources, and compile this information as the recovery plan
    - Train the recovery teams in the performance of their specific tasks
    - Develop an ongoing testing and maintenance program to ensure that all processes are in a constant state of recovery readiness.

20.1.2. Implementing Information Security Continuity

1. Events that can cause potential disruptions shall be identified and a risk-based approach (in accordance with the 'Information Security Risk Management Framework') shall be adopted for the development of the various BCP plans.

2. Procedures, systems, and solutions (BCP and DR Plans) shall be developed, implemented, and maintained to continue or restore operations and ensure availability of the required information at the required time. Such procedures, systems and solutions implemented shall ensure that confidentiality and integrity requirements of JSW Group information and information systems are also preserved at all times.
3. BCP and DR plans shall be identified and documented. All roles and responsibilities within the BCP and DR plans, including those related to information security, shall be explicitly defined, and assigned to specific individual (s).
4. BCP and DR plan shall be protected and considered confidential information. BCP and DR plan shall be stored securely.
5. DR plan documents shall be accessible and available to respective stake owners and teams in case the same needs to be referred in an event of an incident/disaster.
6. Business Functional Heads shall identify and document the Recovery Time Objective [RTO] and Recovery Point Objective [RPO] for critical business applications and processes.
7. Business Functional Heads along with IT Team shall conduct DR drills/tests on an annual basis to verify the appropriateness of the DR plan. Business Heads shall maintain all records with respect to DR drills for a minimum period of 2 years.
8. Training & Awareness program shall be established for all JSW Group functions and facilities. Relevant records shall be kept for a minimum period of 2 years for reporting purpose and to identify areas of improvement.
9. Business Heads shall document and maintain all records in case of incidents/disasters where DR needs to be invoked. Same shall be retained for a minimum period of 2 years.
10. Business Functional Heads shall work together with the IT Team to improve Recovery Time taken on the DR Setup for critical business applications.

20.1.3. Verify, Review and Evaluate information Security Continuity

1. JSW Group shall verify the established and implemented information security continuity controlsat regular intervals in order to ensure that they are valid and effective during adverse situations.
2. JSW Group shall verify information security management continuity by:
   - Exercising and testing the functionality of information security continuity processes, procedures, and controls to ensure that they are consistent with the information security continuity objective.
   - Exercising and testing the knowledge and routine to operate information security continuity processes, procedures, and controls to ensure that their performance is consistent with the information security continuity objective.
   - JSW Group review the validity and effectiveness of information security continuity

measures when information systems / security / processes / procedures changes.

20.2. Redundancies

Objective To ensure availability of information processing facilities.

20.2.1. Availability of Information Processing Facilities

1. For information systems where the availability cannot be guaranteed using the existing systems architecture, redundant components or architecture shall be identified and implemented.
2. Alternative sites or other processing arrangements shall be identified and made readily available to enable recovery of business-critical IT operations in the event of a significant disaster or loss of service.
3. Redundancies in information systems and information processing facilities shall be documented in the BCP and DR plans which shall be subject to periodic review and testing.
4. In case where redundant components or architecture cannot be implemented, suitable risk assessment shall be carried out and risk shall be accepted along with approval from Group CIO.

21. Operational Technology (OT) Policy

1. In case of a need to connect OT network with internal corporate network, necessary security controls shall be implemented, before establishing the connection. Approved connections shall be restricted and limited to identified secure services / protocols.
2. JSW Group shall ensure strict physical and virtual segmentation when connecting industrial production networks to other networks within the organization (e.g., corporate network)
3. OT systems should be patched periodically basis OEM recommendations.
4. JSW Group shall perform periodic vulnerability assessments for OT systems.
5. JSW Group shall restrict access to OT locations and devices to authorized personnel only, the access shall be provided in compliance with physical security policy.
6. Up-to-date anti-virus and malware protection solutions for OT shall be implemented. JSW Group shall ensure that monitoring for malware detection is performed continuously.
7. OT systems shall be securely configured and hardened, as per OEM recommendations, prior to production deployment. OT systems shall be periodically reviewed to ensure compliance.
8. JSW Group shall restrict unauthorized traffic to OT networks by configuring proper security controls (e.g. proxy servers, firewalls, etc.)
9. JSW Group shall implement necessary controls for continuous monitoring of

cybersecurity event logs on OT network.

10. External storage media, mobile devices or any other external devices shall not be connected to OT technology components and OT networks.
11. OT Systems shall not have direct unsecured internet connectivity.

22. Compliance

22.1. Compliance with Legal and Contractual Requirements

Objective To avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements

22.1.1. Identification of Applicable Legislation and Contractual Requirements

1. All applicable regulatory requirements to JSW Group shall be identified and reviewed by Compliance Officer. The laws, regulations and contractual requirements shall be defined explicitly and documented.
2. All identified requirements shall be tracked for its compliance by respective departments.
3. Ensure compliance to Information Security and IT requirements defined in the 'IT Act' and mandatory cyber security guidelines issued by 'CERT-In' and same shall be reviewed periodically
4. All employees shall adhere to the policies and procedures to maintain and keep up to date all relevant statutory, regulatory, and contractual requirements.
5. Compliance violations shall be documented, reported and investigated by authorized personnel or a team.
6. All relevant statutory, regulatory and contractual documents and records shall be retained by resp departments of the Business Units for a period as per the required documentation/contracts.
7. A review of compliance with legal and regulatory requirements that affect information security shall be performed regularly and when new legislation or regulatory requirements come into effect.

22.1.2. Intellectual Property Rights

1. JSW Group shall ensure that terms and conditions and license requirements of the copyrighted software or any other proprietary information used within JSW Group are complied with.
2. All intellectual property, such as patents, copyrights and code developed by a user (including but not limited to employees, contractors, supplier / third-party personnel) while employed by JSW Group, shall be the property of JSW Group. All the employees shall sign a standard Non-Disclosure Agreement (NDA), or a confidentiality clause as authorized by JSW Group's Legal department to this effect as part of employment letter or the onboarding process.
3. At the time of termination, all employees, contractors, supplier / third-party personnel shall return any intellectual property provided or developed during the employment period

4. All JSW Group intellectual property shall be classified as per the information classification and scheme.
5. Unless provided in the applicable license, notice, or agreement, copyrighted software shall not be duplicated, except for backup and archival purposes. Any software that is acquired illegally or does not have a valid license shall not be deployed or used in JSW Group. A license compliance assessment shall be carried out on a periodic basis.
6. The employees, contractors, supplier / third-party personnel shall not copy, or reproduce in any way, copyrighted material from the internet on information systems provided by JSW Group.
7. Information Owners shall be responsible for maintaining and retaining proof of entitlement and usage of licenses of identified IP.
8. Intellectual Property shall be acquired only through Original Equipment Manufacturers (OEMs) or authorized resellers and only licensed IP shall be used.
9. Media containing Intellectual Property shall be removed from or securely overwritten prior to disposing.
10. Information Owners shall disclose the Intellectual Property owner credentials on the Intellectual Property utilized for official purposes.

22.1.3. Protection of Records

1. JSW Group's important records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
2. All JSW Group records and information, such as personnel details, legal documents, shall be retained and disposed only in accordance with the retention period as per the applicable local laws and regulations or business / contractual requirements.
3. Mechanism used for storage and handling of legal records shall ensure clear identification of the records.
4. The information classification, labelling, handling, and disposal guidelines shall be applicable to all JSW Group records. All restricted and confidential information shall be destroyedin a secure manner.

22.1.4. Privacy and Protection of Personally Identifiable Information

1. JSW Group shall ensure adequate security controls are implemented for protection and privacy of personal information.
2. JSW Group shall implement controls for collecting, processing, and disseminating personal information.
3. Personally Identifiable Information (PII), Sensitive Personal Data or Information (SPDI) and end user's information shall only be collected and used for business purposes, and

in line with applicable privacy laws and regulations and its privacy and security shall be ensured.

4. Personal information shall not be shared without due consent of the concerned individual, except where JSW Group may be obligated to share such information with law-enforcement, government, and regulatory authorities, or to prevent imminent loss or harm to the concerned individual or others.
5. Data protection techniques such as data masking, pseudonymization or anonymization shall be implemented taking applicable legislation into consideration.

22.1.5. Regulation of Cryptographic Controls

1. IT Infrastructure shall identify cryptographic controls as per the relevant agreements, laws, and regulations.
2. Only the encryption algorithms allowed for use by local laws and regulations and approved by the ITSD shall be used.
3. Legal advice shall be sought to ensure compliance with all laws and regulations which may include:
   - Restrictions on import / export of computer hardware and software for performing cryptographic functions.
   - Restrictions on import / export of computer hardware and software which is designed to have cryptographic functions added to it.
   - Restrictions on usage of encryption.
   - Mandatory / Discretionary methods of access by relevant authorities (e.g., regulations, laws, legislations, government, etc.) to information encrypted by hardware / software to provide confidentiality of content.
   - JSW Group shall ensure that the use of cryptographic controls is compatible to the laws of India and as well as the laws of its clients' country if any.

22.2. Information Security Reviews

Objective To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

22.2.1. Independent Review of Information Security

1. The information security controls at JSW Group shall be independently reviewed periodically to ensure the continuing suitability, adequacy, and effectiveness of JSW Group's approach to information security management.
2. The results of the independent review shall be recorded and reported to the top management who initiated the review and records shall be maintained. Management shall ensure appropriate corrective actions for the reported observations during the independent review are implemented within a definite timeframe.

22.2.2. Compliance with Security Policies and Standards

1. Managers and supervisors shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
2. Head of ITSD shall ensure compliance with the JSW Group information security and related policies at all the times and prepare plan to ensure its information assets are compliant with JSW Group's management systems requirements.
3. Periodic reviews and random tests shall be performed on information systems to assess compliance with the information security policies.

22.2.3. Technical Compliance Review

1. All the relevant functional units shall conduct technical compliance checking at regular intervals either manually or with the assistance of automated tools, which generate a technical report for subsequent interpretation by a technical specialist in accordance with the 'Management of Technical Vulnerabilities Policy'.
2. All functions shall obtain a security clearance for activities such as all new projects, products, applications, services, from the ITSD during their initiation and prior to deployment in the production environment.

23. Cloud Computing / Security Policy

1. Cloud computing technologies such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), if have to be leveraged from external service providers, then the risks pertaining to that shall be assessed and approved by Group CIO in coordination with the ITSD Head.
2. For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the Group CIO in coordination with the ITSD Head.
3. JSW Group shall ensure that the information processed, transmitted, and stored on the cloud architecture is secure.
4. A detailed analysis of the requirement and benefits associated with cloud adoption shall be performed, and the cost-benefit analysis report shall be submitted to JSW Group management for review and approval.
5. JSW Group shall perform an assessment of the cloud service provider (CSP) prior to onboarding.
6. A formal agreement with Cloud Service Provider (CSP) which covers business requirements to protect confidentiality, integrity and availability of the information assets shall be established.
7. When hosting data on the cloud, JSW Group shall ensure that all core business records & PII (Personally Identifiable Information) is hosted within India.

8. For each cloud service that JSW Group consume a clearly documented monitoring shall be performed in place in line with existing JSW Group policies, procedures, standards, requirements,etc.
9. Roles and responsibilities for protecting the cloud environment should be agreed with the CSP, including shared responsibilities and the need for collaboration.
10. Information security awareness, education and training programs about cloud services shall be provided to employees and the supervising managers, including those of business units.
11. Data processed by cloud services should be protected, which includes encrypting sensitive data by using the CSP default encryption solution, configuring customer-managed key encryption or implementing customer-supplied key encryption.
12. The Data Owner/Custodian shall classify the data being hosted/stored at the CSP as per the 'JSW Group Information Classification Guidelines'.
13. The IT team should implement the necessary cryptography controls for the data as per the data classification and on the network channel.
14. Contracts with CSP shall include clauses for complete deletion of data/ information at the end of the Agreement. Contract shall also include clauses for the return of data to the organization and that there is no vendor-lock in period defined by the CSP.
15. Wherever applicable, JSW Group shall align its Cloud Security controls with industry good practices such as CIS benchmark.
16. The organization performs scans to identify vulnerabilities in the cloud environment as well as applications hosted in the cloud as per JSW Group's Vulnerability Management Policy. The organization shall perform penetration testing at a defined frequency on cloud information systems and application hosted.

24. Cyber Security Policy

1. Information shall be protected against known and future cyber security threats by designing, implementing, and continually improving security controls.
2. Confidentiality, integrity, availability, and privacy of the information assets of JSW Group shall bemaintained all the time. Regulatory and legislative requirements for cyber security will be met.
3. A process / guideline document shall be established defining the cyber crisis response methodology.
4. Periodic information security training shall be conducted for all employees and specifically for personnel to combat cyber security incidents.
5. All suspected breaches of cyber security will be reported and investigated as per the process defined for Information Security Incident Management.

6. JSW Group shall periodically review the effectiveness of the cyber security controls deployed andtake corrective and preventative action as appropriate.
7. JSW Group shall monitor significant changes in exposure of information assets to major threats,changes in the way JSW Group conducts its business and changes in the way it uses technology,and to accordingly take appropriate action.

25. Social Media Policy

25.1. Introduction

Social media includes all platforms using the internet that allows posting, collaborating, and sharing of information and content (including but not limited to social networking sites, blogs, forums, discussion boards, photo and video sharing sites, wikis, virtual worlds, etc.). This includes personal, public and JSW Group associated pages.

Social media is constantly changing the way the world connects. Online collaboration tools help to start new relationships and engage in discussion with customers and colleagues from around the globe. This Social Media Policy is created in order to protect JSW Group's reputation, to comply with applicable law and regulations and empower JSW Group employees to be advocates ofthe company. JSW Group employees are encouraged to engage in and enjoy social media, but to use sound judgment while doing so.

25.2. Purpose

The purpose of the is document is to ensure that JSW Group employees protect the interests and reputation of JSW Group and its personnel. This document also outlines areas where employees should feel safe in participating on online / social media in such a way that their personal opinions are not attributed to JSW Group.

The broad objectives of this policy are enlisted below:

1. Support appropriate use of social media for JSW Group business purposes
2. Clarify the boundaries between work-related and private use of social media
3. Safeguard the interests and privacy of JSW Group employees and stakeholders and retain theirtrust
4. Promote e-safety and privacy online for JSW Group employees
5. Promoting honesty about oneself on Social media
6. Clarity that employee's opinion are opinion and not JSW Groups
7. Awareness to employees that what they say is permanent on social media
8. Respect & humility in all social media communications
9. Following good judgement in sharing only public information – including financial data

10. Maintain JSW Group's reputation through effective social media practices
11. Confirmation of what is acceptable and what is unacceptable behavior in terms of social media usage at JSW Group

25.3. Definition: Social Media

Media tools designed primarily for social interaction and collaboration, often featuring communications designated for a broader group (e.g., one-to-many postings and submissions) with the option for continued interaction, sharing, evolution, and 'socialization' of the content. Examples of Social Media sites and tools include but are not limited to Wikipedia, Facebook, Myspace, Orkut, Xing, Linked-In, Twitter, Yammer, Google, Quora, YouTube, WhatsApp Chaton, BBM etc. mobile messaging, blogs, ratings and reviews sites, and/or other local 'applications' promoting social interaction within a community via any device (computer,laptop, tablet, smartphone, cell phone, etc.). An example of such a Social Media application would be a video or photo upload tool that features user generated content, and which is hosted on a website, mobile site, or mini site. Social media also includes platforms with similarfunctions as those indicated above, which are used internally such as Facebook Workplace, etc.

25.4. Policy

25.4.1. Corporate Social Media Content

Posting of content to corporate sponsored social media (e.g., the corporate Facebook page) is permitted only for the employees authorized to publicly represent JSW Group.

25.4.2. Awareness to Employee

All employees of JSW Group shall be made aware on the Acceptable Usage Policy and all employees shall provide a confirmation / acknowledgement stating that one has read and understood the policy and shall comply with the policy.

25.4.3. Inappropriate Content

While social media contains legitimate business and personal content, it also includes content that is inappropriate for the workplace including nudity, violence, abused drugs, sex, and gambling, etc. Therefore, this inappropriate content restrictions that applies to the internet access, also applies to content found within social media. Employees should not access inappropriate content while at work, or while using JSW Group provided assets.

25.4.4. Social Media Acceptable Use Policy

Employees are required to adhere to all of JSW Group policies, standards, procedures, guidelines, circulars, instructions, etc. at all times, whether blogging / social networking for business or personal reasons, via JSW Group's system / accounts or user's own private accounts and personal devices. Following points should be taken care during social media interaction:

1. Users shall not establish / form / promote any group / community on any internet site which uses the name or logo of JSW Group or shall become member of any such group or

community unless such group is created by authorized personnel from JSW Group.

2. User shall create any social network profile in his/her real name and should not create any profile by using name of company name or on behalf of other users.
3. User shall not use the business email address on personal blogs or public social networking sites. Employees shall not link from personal sites to any JSW Group hosted websites,blogs, or social media sites.
4. User shall not post / express any remarks / views in any internet site, chat messenger or social media (e.g., WhatsApp, Facebook, Twitter etc.) which may be defamatory to JSW Group or officials or its employees in their official capacity.
5. User shall not criticize the management of JSW Group or the business processes or strategies ofJSW Group or its policies on any internet site or social media.
6. User shall not disclose any information about any employee or customer of JSW Group includingtheir personal details on any internet site or social media.
7. User shall not express authority using the name of JSW Group while expressing any views in anyof the internet sites / social media.
8. User shall not engage in collusive behavior on any internet site or social media, with JSW Group's competitors or employees. Employees should not post content that is defamatory, discriminatory, harassing, or in violation of JSW Group's policies against discrimination, harassment, or hostility on account of age, race, religion, sex, ethnicity, nationality, disability, or other protected class, status, or characteristic. Employees shall not unlawfullydisparage JSW Group products or services, or the products or services of JSW Group's vendors or competitors.
9. Users shall not write about, comment on, or answer questions regarding any legal matter, litigation, or party to a lawsuit involving JSW Group.
10. User shall not canvass for any donation, lottery, or supplier marketing / business promotional activities / affairs of JSW Group on any internet site or social media.
11. When using JSW Group's blogs, social media sites, or internet system, employees shall have noexpectation of privacy.

25.4.5. Content Publishing and Confidentiality

1. When employees are participating on social networking sites using your personal social media accounts, they need to be transparent that thoughts are personal thoughts, if discussing official JSW Group business.
2. Employees shall use real identity and no aliases and disclose one's affiliation with JSW Group. Ifemployee believes posting might lead to any confusion with viewers about whether employee is speaking on behalf of JSW Group, employee should clearly and specifically state asfollows:
   - **Twitter disclaimer:** 'These tweets are my own, not JSW Group's.
   - **Disclaimer for blogs sponsored by JSW Group:** 'Some of the individuals posting

to this site, including the moderators, work for JSW Group. Opinions expressed here and in any corresponding comments are the personal opinions of the original authors, not those of JSW Group.'

- **Third-party blog disclaimer:** 'The opinions expressed in this blog are my own views and not those of JSW Group.'

3. User shall not publish any official information / circulars / memorandum / documents etc. which are of the record of JSW Group, without obtaining prior written approval from designated authority.
4. If employee is representing oneself as a JSW Group employee on social networking sites like LinkedIn, employee may not provide professional references for any current or former JSW Groupemployee, contractor, vendor, or contingent worker on JSW Group's behalf. However, employeemay provide a personal reference or recommendation for current or former JSW Group employees, contractors, vendors, and contingent workers provided:
   - the statements made and information provided in the reference are factually accurate
   - Employee shall include the following disclaimer: 'This reference is being made by me in a personal capacity. It is not intended and should not be construed as a reference from JSW Group or any of its affiliated entities.'
5. Employees shall not post any business-related confidential or internal-use only information (marked 'Restricted and Confidential' and 'Internal') that employee has obtained or learned as part of job duties with JSW Group. Such information includes the following examples: information regarding the development of systems, products, processes, and technology; personally, identifiable information (such as telephone numbers, PAN, or financial account numbers) of the JSW Group's employees, customers, vendors, or competitors; nonpublic financial information; marketing strategies; inventions not yet patented; or other business-related confidential or proprietary information.
6. Employees shall not write / express anything in any internet site or social media that may damage the reputation of JSW Group or any of its employees.
7. Employees shall respect the financial disclosure laws and be very careful when making statements about JSW Group's financial performance and shall not make statements that in anyway could violate laws such as the disclosure of material, nonpublic information. For example, it is illegal to communicate or give a 'tip' on inside information to others so that they may buy or sell stocks or securities.

25.4.6. Malware & Online Crime Prevention

Social media is commonly used by the online criminal community to deliver malware and carry out schemes designed to damage property or steal confidential information. To minimize risk related to such threats, employees shall adhere to the following guidelines. While these guidelines help to reduce risk, they do not cover all possible threats and are not a substitute for good judgment:

1. Employees shall not use the same passwords for social media that you use to access company computing resources.

2. Employees shall not follow links or download software on social media pages posted by individuals or organizations that employee does not know.
3. JSW Group can use a security application such as Defense (www.defensio.com) to protect personal and company social media pages.
4. If an employee finds any content on any social media web page that looks suspicious in any way, employee shall close the browser and shall not return to that page.
5. Employee shall configure social media accounts to encrypt sessions whenever possible. Facebook, Twitter, and others support encryption as an option. This is extremely important for roaming users who connect via public Wi-Fi networks.

25.4.7. Recommended Technical Controls

JSW Group's Social Media Acceptable Usage Policy as described in above section is monitored and enforced by a Secure Web Gateway system. The Secure Web Gateway inspects inbound andoutbound employee web communications to enforce acceptable usage policy, prevent confidential data loss and block web-based attacks (malware, phishing, etc.). The Secure WebGateway may be deployed on premise, as a Security-as-a-Service (SaaS) solution, or as a hybrid on premise / SaaS system. The Secure Web Gateway shall secure all JSW Group internet connected, company-owned employee computers including mobile laptop computers with direct Internet connections. The Secure Web Gateway shall include the following capabilities.

1. Content-Aware Social Media Policy – The ability to apply JSW Group's Social Media AcceptableUsage Policy to content within all social media pages and do so across all content categories (e.g., sports, games, adult). It is not enough to classify social media at the domain or URL level. Social media content classification shall be tested at a minimum by visiting a selection (>25) popular social media page.
2. Composite Risk Scoring – The ability to combine information from multiple content security analytics to classify content and identify attacks in real-time. Analytics should include URL database, reputation, content signatures, antivirus, and content analysis. Composite risk scoring enables a Secure Web Gateway to identify malicious content such as Facebook phishing schemes and zero-day malware in real-time.
3. Context-Aware Confidential Data Detection – The ability to account for the context of confidential data strings when identifying outbound data confidentiality violations. For example, the solution should differentiate between an employee social security number posted alone (not a violation), and a social security number posted in combination with an employee name (a violation). Keyword dictionaries and regular expression matching capabilities do not meet this requirement.
4. Custom Document and Database Fingerprinting – The ability to identify custom database records (e.g., customer's records) and documents (e.g., business plans).

26. Disclaimer

Various information technology (IT) assets are made available for use by JSW Group Group Company personnel for legitimate and authorized business purposes. All those authorized toaccess IT assets must accept responsibility for their conduct regarding appropriate use and safeguarding of JSW Group Group Company information and IT assets.

The JSW Group Group Company retain exclusive right, title and interest in IT assets and information and reserves the right to monitor, review, regulate and audit the use of JSW Group Group Company managed IT and information assets to maintain its integrity. All JSW Group Group Company Personnel must recognize that JSW Group Group Company may exercise thisright at any time without prior notice.

Subject to compliance with applicable laws or regulations, the JSW Group Group Company may review and examine Company IT assets upon demand; JSW Group Group Company has the rightto collect, use and disclose information, including but not limited to processing personal information and data in respect of JSW Group Group Company personnel, within and outside of JSW Group Group Company as is reasonably required in connection with the protection and use of JSW Group Group Company IT assets, or the management, administration and enforcement ofJSW Group Group Company policies and programs.

JSW Group Group Company reserve the right to discipline any JSW Group Group Company personnelfor breaches of laws, regulations, or policy, including but not limited to termination of employment or other contract and initiating appropriate legal action. Following the cessation of employment or otherwise as directed, the user shall immediately deliver and return to the JSW Group Group Company all IT assets, communication system, devices, and data of JSW Group Group Company, without erasing any data or reformatting disk drives and without retainingany copy including the backup copies.

By accepting the above, the user acknowledges and consents JSW Group Group Company's ownership, monitoring, and audit rights with respect the JSW Group Group Company's IT and information assets, communication devices, digital systems etc. which is fair and reasonable.

27. Reference

Standards	:	ISO/IEC 27001:2022 – ISMS Cl. 6.1 and Cl. 8
JSW Group Framework	:	PO-001-Information Security Management System Framework
JSW Group Policy	:	• PO-004-Risk Management Framework • PO-003-Acceptable Usage Policy
JSW Group Procedures	:	NA
JSW Group Templates	:	• JSW Group-ISMS-Information Gathering File Template • JSW Group-ISMS-Risk Register Template
JSW Group Records	:	• Information Asset Register • JSW Group-ISMS-Information Gathering File • JSW Group-ISMS-Risk Register

28. User Comments and Feedback

As a user you can have a significant impact on the quality of the Information Security Policies & Guidelines manual. Any comments or suggestions for improvements will be much appreciated. Please detail your proposed changes as specifically as possible.

Your comments / suggestions will be considered during the periodic review of this manual. Please provide your e-mail address, so that we can contact you, if necessary, for any further explanation. A copy of this form must be sent by fax or e-mail or internal mail to:

Office of Information Security, JSW Group Group,

JSW Group Center, Near MMRDA Grounds, Kolivery Village, MMRDA Area, Bandra Kurla Complex, Bandra East, Mumbai – 400098, Maharashtra, India
M: +91- 7304263250 / +91-9920135606. Email: JSW Group-ISM (JSW Group-ism@JSW Group.in)

29. Annexure

29.1. Annexure A – Definitions

Term	Definition
Asset	Anything tangible or intangible that can be owned controlled andproduce value through its use.
Authentication	Provision of assurance that a claimed characteristic of an entity iscorrect.
Authenticity	Property that an entity is what it claims to be.
Availability	Property of being accessible and usable on demand by an authorized entity.
Backup	The saving of files onto alternate storage or other offline mass storage media for preventing loss of data in the event of equipmentfailure, destruction, or accidental deletions.
Bring Your Own Device	Bring your own device – also called bring your own technology, bringyour own phone, and bring your own personal computer – refers tobeing allowed to use one's personally owned device, rather than being required to use an officially provided device. There are two major contexts in which this term is used.
Business Continuity	Organization's ability to ensure operations and core business functions are not severely impacted by a disaster or unplanned incident that take critical systems offline.
Capacity Management	Capacity Management is a set of processes that allow an organization to manage its critical infrastructure resources in a wayto that business requirements and agreed service levels are met.
CCTV	Closed Circuit Television (CCTV) is the use of cameras to transmit a signal to a specific, limited set of monitors and records images of identifiable individuals or information relating to individuals.
Cloud Computing	Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Cloud computing entrusts remote services with user'sdata, software, and computation.

Term	Definition
Communication	It is the process of meaningful interaction amongst persons of an organization and external interested parties related to the Information Security Management System.
Confidentiality	Property that information is not made available or disclosed tounauthorized individuals, entities, or processes.
Control	Controls include any process, policy, device, practice, or other actions which modify risk.
Copyright	Copyright is a legal right that protects the expression of ideas.
Corrective Action	Action to eliminate the cause of nonconformity and to prevent arecurrence.
Criticality	The importance assigned to a service or item which allows prioritization monitoring and maintenance.
Cryptography	The science of secret writing that enables storage and transmissionof data in a form that is available only to the intended individuals
Demand Management	Demand management helps a business understand and predictdemand for capacity requirements.
Denial of Service	Any action, or series of actions, that prevents a system, or its resources, from functioning in accordance with its intended purpose
Devices	The device includes all servers, network devices and endpoints.
Document	A document is something that is being currently worked upon and istherefore subject to editing and change.
Disaster Recovery Plan	A documented and structured approach to minimize the effects of adisaster so the organization can continue to operate or resume its critical functions.
Effectiveness	The extent to which planned activities are realized and plannedresults achieved.
Encryption	The transformation of plaintext into unreadable cipher text.
Endpoints	Terminal devices used by end-users like a laptop, desktop, mobilephones, tablets, and any other smart device.
End Users	End Users include all JSW Group employees and non-employees includingsupplier / third party personnel, trainees, consultants, advisors having access to JSW Group Information Systems and network.

Term	Definition
End User License Agreements (EULA)	An end-user license agreement is a legal contract entered into between a software developer or vendor and the user of the software, often where the software has been purchased by the userfrom an intermediary such as a retailer.
Exploit	Exploits are the means through which vulnerability can be leveragedfor malicious activity by hackers
External Network	Any network including the Internet, outsourced suppliers, and business partners.
External user	Users with access to JSW Group systems outside of JSW Group network. Forexample, suppliers, customers.
Heating, Ventilating,and Air Conditioning (HVAC)	HVAC refers to the different systems used for moving air between indoor and outdoor areas, along with heating and cooling both residential and commercial buildings.
IaaS	Infrastructure as a Service (IaaS) is a cloud computing model thatprovides users with unfettered access to a cloud device.
Impact	The influence and effect of risk.
Information Asset	Knowledge or information that is retained in electronic form (such asemails, documents, etc.) or physically tangible material (such as printed documents, etc.).
Information processing facilities	Facilities processing customer and business-sensitive information.
Information Security Continuity	Processes and procedures for ensuring continued informationsecurity operations.
Information Security Event	The identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant.
Information Security Management System	Information Security Management System (ISMS) is a managementsystem based on a systematic business risk approach to establish,implement, operate, monitor, review, maintain, and improveinformation security.
Information Security Incident	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising businessoperations and threatening information security.

Term	Definition
Information system	Set of applications, services, information technology assets, or otherinformation-handling components.
Integrity	Property of accuracy and completeness of the information.
Intellectual property rights	Intellectual property rights include trademarks, patents, source codelicenses, software copyrights, document copyrights.
Internal Audit	The process of providing independent assurance that an organization's risk management, governance, and internal control processes are operating effectively.
Internal user	Users with access to JSW Group systems through JSW Group network.
Intrusion Detection Systems (IDS)	An intrusion detection system is a device or software application thatmonitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management system.
Intrusion Prevention Systems (IPS)	An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.
JSW Group network	The network of JSW Group, including local area network, wide areanetwork connecting all JSW Group's information assets.
Key Management	Key management is the secure administration and distribution of cryptographic keys throughout the entire key life cycle. Keys are generated, distributed, stored, used, recovered, and eventually terminated or possibly archived.
Log	Record of the events occurring within an organization's systems and networks.
Malware	Malware is the short form for malicious software; is software used orprogrammed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems.
Minimum BaselineSecurity Standards	Minimum Baseline Security Standards (MBSS) defines a set of essential security objectives which must be met by any given serviceor system. All systems/services must be implemented and deployedin compliance with their corresponding MBSS.

Term	Definition
Mobile device	Any device which is connected to JSW Group network and is mobile likelaptop, tablet, mobile.
Mobile DeviceManagement (MDM)	Mobile device management is the administration of mobile devices,such as smartphones, tablet computers and laptops. MDM is usuallyimplemented with the use of a third-party product that has management features for particular vendors of mobile devices
Network devices	Network device includes switches, routers, hub, modems and security devices like IDS, firewalls, IPS, SIEM, NBAD, DAM and HIPS.
Network TimeProtocol (NTP)	NTP is a protocol used to synchronize computer clocks across multiple systems. It supports synchronization over local area networks and the Internet.
Non-DisclosureAgreement	Non-Disclosure Agreement (NDA) is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certainpurposes but wish to restrict access to or by third parties.
Non-Repudiation	A cryptographic service that legally prevents the originator of a message from denying authorship at a later date. A security serviceby which evidence is maintained so that the sender of data and recipient of data cannot deny having participated in the communication.
PaaS	Platform as a Service (PaaS) is a cloud computing model thatprovides users access to a computing platform.
Password	A protected word or string of characters which serves as authentication of a person's identity, or which may be used to grantor deny access to private or shared data.
PII	Personally, Identifiable Information (PII) is any information relatingto an identifiable person.
Privacy Law	Protection and privacy of organizational data should be ensured asrequired in legislation, regulations, and contracts. The legislations placing controls on the collection, processing, and transmission of personal data should be strictly followed.
Privilege Identity Management (PIM) / Privilege Access Management (PAM)	PIM / PAM is an information security (infosec) mechanism that safeguards identities with special access or capabilities beyond regular users. Like all other infosec solutions, PIM / PAM works through a combination of people, processes, and technology.

Term	Definition
Ransomware	Ransomware is a type of malware that prevents or limits users fromaccessing their system, either by locking the system's screen or bylocking the users' files unless a ransom is paid.
Record	Text that is generated to provide objective evidence that somethinghas occurred or is effective.
Redundancy	The solution to prevent any disruption of system operation in the case of a technical malfunction or disaster, thereby maintaining continuity of service.
Review	The activity was undertaken to determine the suitability, adequacy, and effectiveness of the subject matter to achieve establishedobjectives.
Risk	A potential event or action that would harm the organization.
Risk analysis	The process to comprehend the nature of risk and to determine thelevel of risk.
Risk assessment	The overall process of risk identification, risk analysis and riskevaluation.
Risk evaluation	Process of comparing the results of risk analysis with risk criteria todetermine whether the risk and/or its magnitude is acceptable or tolerable.
Risk identification	Process of finding, recognizing, and describing risks.
Risk management	Coordinated activities to direct and control an organization concerning risk.
Risk acceptance	A formally documented and Informed decision by an appropriate stakeholder not to remediate a level of risk that exceeds an organization’s risk appetite/tolerance.
Risk Deviation	A formal and documented condition that is not aligned with formal security expectations as defined by the policy, standard, and/or procedure
SaaS	Software as a Service (SaaS) provides the capability for customersto use the Provider’s applications running on a cloud infrastructure.
SPDI	Sensitive Personal Data or Information (SPDI) is a specific set of “special categories” of PII that must be treated with extra securitydue to its sensitivity.
SLA	Service Level Agreement (SLA) is a commitment between a serviceprovider and a client. Particular aspects of the service

Term	Definition
	such as quality, availability, responsibilities etc. are agreed between the service provider and the service user.
SOD	A controlled document that lists the exceptions/ deviations from thedefined JSW Group policies, procedures, and risk mitigation controls, set norms, etc. as approved.
Sub-contractor	A person or business which has a contract (as an 'independent contractor" and not an employee) with a contractor to provide someportion of the work or services on a project based on agreement.
Suppliers	Any third-party service providers, vendors, contractors, and theirsub-contractors are referred to as supplier.
Surveillance	Act of monitoring of behavior, activities, or information.
System	Any machine used for computation which includes endpoints, servers, application.
Teleworking	Working/access of JSW Group network for an official purpose other than from base location. This includes Work from Home provisions as well.
Third-Party	Third parties include suppliers including advisors, consultants, service providers (contractors and their sub-contractors), vendors and other personnel having access to JSW Group information assets.
Threat	A threat is a potential for a particular threat-source to exploit aparticular vulnerability successfully.
Trojan horse	A malicious program, such as a virus or a worm, hidden in an innocent-looking piece of software, usually for unauthorized collection, alteration, or destruction of information.
Undertaking	Undertaking in general means an agreement to be responsible forsomething.
User Account	Collection of standard information known about the user which includes account name, an associated password, and a set of access permissions for network resources. The record of the user profile in the user accounts database is known as User Account.
Virtualization	Virtualization is the process of creating a software-based, or virtual,representation of something, such as virtual applications, servers, storage, and networks. It is the single most effective way to reduce IT expenses while boosting

Term	Definition
	efficiency and agility for all size businesses.
Virtual Local AreaNetworks (VLANs)	A virtual LAN is any broadcast domain that is partitioned and isolated in a computer network at the data link layer. LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic.
Virus	A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its code.
Vulnerability	Vulnerability is a weakness with an organization's assets that has the potential to allow a threat to occur with higher frequency, more significant impact, or both.
Worm	An independent program that replicates complete copies of itself from machine to machine across network connections, often clogging networks and Information Systems as it spreads.

29.2. Annexure B – Acronyms

Acronym	Term
CIO	Chief Information Officer
ISMS	Information Security Management Systems
ISP	Information Security Policy
ITSD	IT Security Department
HR	Human Resource
HRD	Human Resource Department
ITSD	IT Security Department
MDM	Mobile Device Management
PIM	Privilege Identity Management
PAM	Privilege Access Management
UPS	Uninterruptible Power Supply
HVAC	Heating, Ventilating, and Air Conditioning
NTP	Network Time Protocol
MBSS	Minimum Baseline Security Standards
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
VLAN	Virtual Local Area Networks
EULA	End User License Agreements
NDA	Non-Disclosure Agreement
VA	Vulnerability Assessments
PT	Penetration Testing
SDLC	Software Development Lifecycle
SLA	Service Level Agreement
BCP	Business Continuity Plan
DR	Disaster Recovery
PII	Personally, Identified Information
SDPI	Sensitive Private Data or Information

Acronym	Term
SaaS	Software-as-a-Service
PaaS	Platform-as-a-Service
IaaS	Infrastructure-as-a-Service
CSP	Cloud Service Provider
BYOD	Bring Your Own Device