Information Security Policy

DOCUMENT INFORMATION

Document Title	**Information Security Policy**
Document Owner	InfoSec Team (JK Cement)
Information Classification	Public

Document Revision History

Date	Version	Created By	Reviewed By	Approved By	Remarks
28-04-2026	1.0	Infosec Team	Head Security	CDO (Chief Digital Officer)	--

Contents of Document

A.5.26	Learning from Information Security Incidents
A.5.27	Collection of Evidence
A.5.28	Information Security During Disruption
A.5.29	ICT Readiness for Business Continuity
A.5.30	Legal, Statutory, Regulatory, and Contractual Requirements
A.5.31	Intellectual Property Rights
A.5.32	Protection of Records
A.5.33	Privacy and Protection of Personally Identifiable Information (PII)
A.5.34	Independent Review of Information Security
A.5.35	Compliance with Policies, Rules, and Standards for Information Security
A.5.36	Documented Operating Procedures
A.6	People Controls
A.6.1	Screening
A.6.2	Terms and Conditions of Employment
A.6.3	Information Security Awareness, Education, and Training
A.6.4	Disciplinary Process
A.6.5	Responsibilities After Termination or Change of Employment
A.6.6	Confidentiality or Non-Disclosure Agreements
A.6.7	Remote Working
A.6.8	Information Security Event Reporting
A.7	Physical Controls
A.7.1	Physical Security Perimeter
A.7.2	Physical Entry Controls
A.7.3	Securing Offices, Rooms, and Facilities
A.7.4	Physical Security Monitoring
A.7.5	Protection Against Physical and Environmental Threats
A.7.6	Working in Secure Areas
A.7.7	Clear Desk and Clear Screen Policy
A.7.8	Equipment Siting and Protection
A.7.9	Security of Assets Off-Premises
A.7.10	Storage Media
A.7.11	Supporting Utilities
A.7.12	Cabling Security

A.7.13	Equipment Maintenance
A.7.14	Secure Disposal or Reuse of Equipment
A8.1	User End Point Devices
A8.2	Privileged Access Rights
A8.3	Information Access Restriction
A8.4	Access to Source Code
A8.5	Secure Authentication
A8.6	Capacity Management
A8.7	Protection Against Malware
A8.8	Management of Technical Vulnerabilities
A8.9	Configuration Management
A8.1	Information Deletion
A8.11	Data Masking
A8.12	Data Leakage Prevention
A8.13	Information Backup
A8.14	Redundancy of Information Processing Facilities
A8.15	Logging
A8.16	Monitoring Activities
A8.17	Clock Synchronization
A8.18	Use of Privileged Utility Programs
A8.19	Installation of Software on Operational Systems
A8.2	Network Security
A8.21	Security of Network Services
A8.22	Segregation of Networks
A8.23	Web Filtering
A8.24	Use of Cryptography
A8.25	Secure Development Life Cycle
A8.26	Application Security Requirements
A8.27	Secure System Architecture and Engineering Principles
A8.28	Secure Coding and Security Testing
A8.29	Outsourced Development
A8.30	Separation of Development, Test, and Production Environments

A8.31	Change Management
A8.32	Test Information
A8.33	Test Information (Post-Testing Cleanup)
A8.34	Protection of Information Systems During Audit Testing

1.0 Introduction

The security of data and information is of vital importance to JK Cement Limited, and it is therefore a business decision as to what information should be protected and to what level. Information Security is a key imperative of JK Cement vision. It comprises assurance of security of Information Assets belonging to JK Cement, as also the Information that is entrusted to JK Cement by employees and investors. JK Cement is also committed to ensure compliance with relevant laws and regulations.

Information Security translates to preservation of the following goals:

- **Confidentiality:** Assurance that Information is accessible only to those authorized to have access.
- **Integrity:** Assurance of the completeness and accuracy of Information and its processing methods.
- **Availability:** Assurance that authorized user has access to Information and associated assets when required. This is ensured by regular maintenance of hardware, updated and monitored operating systems, redundant critical resources, Information Security Business Continuity Management, capacity management and other information security measures we take.

2.0 Objective

The objective of the Information Security at JK Cement is preservation of Confidentiality, Integrity and Availability of its information assets and minimizing business damage by preventing and minimizing the security incidents. It also aims towards continual improvement and will comply with all the applicable requirements as per statement of applicability designed for the ISMS.

3.0 Scope

All employees, partners, customers, suppliers, contractors, and temporary workers to perform work within JK Cement premises or granted access to company information or systems are covered by this policy.

This policy is also applicable to all JK Cement employees including individuals at all locations, computer equipment, network, voice or data communications equipment, computer programs, procedures and support software, data storage devices and media.

4.0 Waiver Criteria and Exceptions

Any exception to this policy will be reviewed and approved through a formal internal process, with appropriate justification and risk consideration. At the completion of the case / period, the need for the waiver will be reassessed and re-approved, if necessary. The waiver will be monitored to ensure its concurrence with the specified period and exception.

Any exception to the Information Security policy shall be formally documented including the following at a minimum:

- Justification for the exception
- Any risk due to the exception
- The mitigation controls to manage the risk
- The validity period of the exception
- Details of assets
- Risk acceptance in case no controls to manage risk

5.0 Policy

A5.1 - Policies for Information Security

- Information security policies shall be formally defined, aligned with business and regulatory and applicable customer requirements.
- All InfoSec policies should be approved by top management/relevant authority to demonstrate leadership commitment.
- Policies must be communicated to all relevant stakeholders and made easily accessible.
- All the InfoSec policies shall be reviewed per the review frequency defined by JK Cement Limited.

A.5.2 – Information security roles and responsibilities

InfoSec team shall ensure:

- Specific information security responsibilities are assigned to relevant roles.
- Roles are documented in job descriptions or internal guidelines.
- Individuals understand their security duties.
- Responsibilities are reviewed and updated as needed.

A.5.3 – Segregation of duties

InfoSec team shall ensure:

- Conflicting duties are separated to reduce risk of fraud or error.
- Checks and balances are implemented through role separation.
- Segregation is enforced through access controls.

- Assignments are regularly reviewed for conflicts.

A.5.4 – Management responsibilities

InfoSec team shall ensure:

- Top management supports the ISMS and allocates necessary resources.
- Policies and controls are enforced across the organization.
- A culture of security awareness is promoted.
- Audit and performance reports are reviewed and acted upon.

A.5.5 – Contact with authorities

InfoSec team shall ensure:

- Procedures exist for timely communication with regulators and law enforcement.
- Specific roles are assigned to handle authority contact.
- Contact details for relevant authorities are maintained.
- Legal and reporting obligations are met.

A.5.6 – Contact with special interest groups

InfoSec team shall ensure:

- Participation in forums or groups to stay updated on threats and best practices.
- Threat intelligence partnerships are leveraged.
- Relevance and trustworthiness of groups are evaluated.
- Engagements are documented.

A.5.7 – Threat intelligence

InfoSec team shall ensure:

- Threat information is gathered, assessed, and applied.
- Threat intelligence informs risk assessments and decisions.
- Reliable threat feeds are subscribed to.
- Intelligence is integrated into incident response.

A.5.8 – Information security in project management

InfoSec team shall ensure:

- Security is integrated early in project lifecycles.
- ISMS controls are included in project plans.
- Risks are assessed for each project.
- Controls are reviewed before go-live.

A.5.9 – Inventory of information and other associated assets

InfoSec team shall ensure:

- All relevant assets are identified and documented.
- Asset ownership is assigned.
- Assets are classified based on sensitivity.
- Inventories are kept up to date.
- An asset inventory shall be maintained and protected in accordance with internal access and control practices.
- JK Cement shall classify and label all information and assets as per the defined information classification scheme
- All organizational assets shall be returned when no longer required or when employment or engagement ends.
- Formal process for the secure disposal of assets shall be defined, and appropriate audit trails shall be maintained.
- Use of removable media shall be restricted.
- A formal process shall be defined for the transfer of IT assets.

A.5.10 – Acceptable use of information and other associated assets

InfoSec team shall ensure:

- Acceptable use is clearly defined and documented.
- Policies are communicated to all users.
- Awareness and technical controls enforce rules.
- Misuse is addressed appropriately.

A.5.11 – Return of assets

InfoSec team shall ensure:

- Assets are returned upon termination or role change.
- Offboarding procedures include formal and complete return of assets.
- Return of assets records are maintained.
- Access credentials and physical assets are recovered.

A.5.12 – Classification of information

InfoSec team shall ensure:

- Information is classified by sensitivity and impact.
- Classification is applied consistently across data types.
- Labels and access rules are used.
- Staff are trained on classification schemes.

A.5.13 – Labelling of information

InfoSec team shall ensure:

- Information is labelled according to classification.
- Labelling tools and formats are consistent.
- Labels are applied during data creation.
- Labels remain accurate over time.
- Information Labelling and Handling Guideline shall be maintained for handling, storing, and communicating information, consistent with the classification of information to protect from unauthorized disclosure or misuse
- The guidelines shall include, but are not limited to the following:
- Access restrictions to prevent access by unauthorized personnel
- Data distribution
- Clear marking of all copies of media for the attention of the authorized recipient etc.

A.5.14 – Information transfer

InfoSec team shall ensure:

- Appropriate security controls shall be used to protect information exchanged with stakeholders. Information shall be shared only with authorized recipients, and suitable safeguards shall be applied for electronic and physical transfers of information.

A.5.15 – Access control

InfoSec team shall ensure:

- User access shall be managed and reviewed in accordance with internal requirements.
- Authentication controls shall be applied for administrative access.
- Password management practices shall be defined and followed.
- User identities shall be managed appropriately, and any exceptions shall be approved through the internal process.
- Remote access shall be controlled and granted only where justified.
- Privileged access shall be granted only to authorized personnel and reviewed periodically.

A.5.16 – Identity management

InfoSec team shall ensure:

- Full lifecycle of user identities is managed.
- Unique IDs are established for all users.
- Identity creation is appropriately approved.
- Identities are revoked promptly when no longer needed.

A.5.17 – Authentication information

InfoSec team shall ensure:

- Passwords and authentication mechanisms are protected.
- Multi-factor authentication is used where applicable.
- Password complexity and expiration policies are enforced.
- Credentials are stored and transmitted securely.

A.5.18 – Access rights

InfoSec team shall ensure:

- Access is granted based on documented approvals.
- Access rights records are maintained.
- Access is reviewed and revoked when roles change.
- Access is audited periodically.

A.5.19 – Information security in supplier relationships

InfoSec team shall ensure:

- Supplier relationships shall include appropriate security requirements and confidentiality obligations where relevant. Supplier access shall be limited to what is necessary, and supplier activity shall be managed in accordance with internal requirements.

A.5.20 – Addressing information security within supplier agreements

InfoSec team shall ensure:

- Security responsibilities are contractually defined.
- Controls and reporting obligations are specified.
- Supplier requirements align with internal security.
- Audit rights are included in agreements

A.5.21 – Monitoring, review, and change management of supplier services

InfoSec team shall ensure:

- Supplier performance and controls are regularly reviewed.
- Security is included in service reviews.
- Changes and transitions are securely planned.
- Risk assessments are updated accordingly.

A.5.22 – Information security for use of cloud services

InfoSec team shall ensure:

- Cloud provider security capabilities are assessed.
- Responsibilities are clearly defined in contracts.
- Compliance with standards is monitored.
- Data is protected in transit and at rest.
- Cloud services may be used to support business requirements, subject to appropriate review and approval. Information shall not be stored in services that have not been authorized by the organization

A.5.23 – Information security incident management planning and preparation

InfoSec team shall ensure:

- A formal incident management process shall be defined to support identification, recording, assessment, escalation, resolution, and closure of incidents.
- Lessons learned from previous incidents shall be utilized to reduce the likelihood of incidents in future.

A.5.24 – Assessment and decision on information security events

InfoSec team shall ensure:

- Events are identified, assessed, and classified.
- Escalation is based on event impact.
- Incident logs are maintained.
- Predefined classification criteria are used.

A.5.25 – Response to information security incidents

InfoSec team shall ensure:

- Incidents are promptly contained and mitigated.
- Documented procedures are followed.
- Affected stakeholders are informed.
- Evidence is preserved when necessary.

A.5.26 – Learning from information security incidents

InfoSec team shall ensure:

- Post-incident reviews are conducted.
- Root causes and control gaps are identified.
- Lessons learned are applied across systems.
- Policies and training are updated.

A.5.27 – Collection of evidence

InfoSec team shall ensure:

- Evidence collection procedures are defined.
- Chain of custody and evidence integrity are preserved.
- Staff are trained in forensic principles.
- Evidence is securely stored.

A.5.28 – Information security during disruption

InfoSec team shall ensure:

- Business continuity plans include security measures.
- Critical systems and data are protected during disruptions.
- Continuity plan security elements are evaluated.
- Roles and responsibilities are clearly communicated.

A.5.29 – ICT readiness for business continuity

InfoSec team shall ensure:

- ICT services support continuity goals.
- Redundancy and failover mechanisms are in place.
- Recovery objectives shall be defined for critical services where applicable
- Recovery procedures are regularly tested.

A.5.30 – Legal, statutory, regulatory, and contractual requirements

InfoSec team shall ensure:

- Compliance obligations are identified.
- Obligations are mapped to policies and controls.
- Responsibility for compliance is assigned.
- Obligations are reviewed regularly.
- Compliance with all Legal, Regulatory and Contractual Requirements shall be identified and compliance status with these requirements shall be maintained.
- Necessary corrective actions shall be initiated and tracked in case of non-compliance.
- JK Cement shall ensure Privacy and protection of personally identifiable information as required by the relevant legislation and regulations.

A.5.31 – Intellectual property rights

InfoSec team shall ensure:

- IPRs (e.g., patents, copyrights) are protected.
- Software and content licensing is compliant.
- Staff are trained on IP compliance.
- Potential violations are monitored.

A.5.32 – Protection of records

InfoSec team shall ensure:

- Records are protected from loss, alteration, or destruction.
- Retention and access policies are defined.
- Secure storage systems are used.
- Legal retention periods are complied with.

A.5.33 – Privacy and protection of personally identifiable information (PII)

InfoSec team shall ensure:

- Privacy-by-design principles are applied.
- Collection and use of PII is minimized.
- Data subject rights are provided.
- PII security controls are implemented.

A.5.34 – Independent review of information security

InfoSec team shall ensure:

- Regular independent ISMS reviews are scheduled.
- Internal or external auditors are engaged.
- Findings and recommendations are addressed.
- Audit trails are maintained.

A.5.35 – Compliance with policies, rules, and standards for information security

InfoSec team shall ensure:

- Adherence to internal requirements is monitored.
- Technical and managerial controls are used.
- Violations are investigated and addressed.
- Compliance metrics are reported.

A.5.36 – Documented operating procedures

InfoSec team shall ensure:

- Procedures for key operations are documented.
- Procedures are accessible to personnel.
- Security and business needs are supported.
- Procedures are reviewed and tested periodically.

A.6– People Controls

A.6.1 – Screening

InfoSec team shall ensure:

- Pre-employment background checks are conducted in accordance with applicable laws and regulations.
- Verification of candidates' identities, qualifications, and references is performed.
- Screening processes are proportionate to the role's responsibilities and associated risks.
- Background verification shall be performed on all candidates (on-roll/ off-roll) considered for employment before on-boarding, in accordance with relevant laws, regulations and ethics.
- The terms and conditions of employment signed by JK Cement's employees shall include the employees' responsibilities for information security and related obligations, both during and after employment. The employee induction process shall include training and awareness sessions on information security.

A.6.2 – Terms and Conditions of Employment

InfoSec team shall ensure:

- Employment contracts clearly define information security responsibilities.
- Employees acknowledge and agree to security policies and procedures.
- Confidentiality and non-disclosure agreements are signed where necessary.
- Security obligations are communicated during onboarding.

A.6.3 – Information Security Awareness, Education, and Training

InfoSec team shall ensure:

- Regular training programs are conducted to raise security awareness.
- Training content is updated to reflect current threats and policies.
- Attendance and completion of training are tracked and recorded.
- Effectiveness of training programs is evaluated periodically.

A.6.4 – Disciplinary Process

InfoSec team shall ensure:

- A formal disciplinary process is established for security breaches.
- Employees are informed about consequences of non-compliance.
- Disciplinary actions are applied consistently and fairly.
- Records of incidents and actions taken are maintained securely.

A.6.5 – Responsibilities After Termination or Change of Employment

InfoSec team shall ensure:

- Access rights are revoked promptly upon employment termination or role change.
- All organizational assets are returned by departing employees.
- Confidentiality obligations continue post-employment as per agreements.
- Exit procedures are documented and followed consistently.

A.6.6 – Confidentiality or Non-Disclosure Agreements

InfoSec team shall ensure:

- NDAs are implemented for employees and third parties handling sensitive information.
- Agreements clearly define the scope and duration of confidentiality obligations.
- Compliance with NDAs is monitored and enforced.
- Breaches of confidentiality are addressed through established procedures.

A.6.7 – Remote Working

InfoSec team shall ensure:

- Remote work policies are established, covering security requirements and acceptable use.
- Secure communication channels and authentication methods are used.
- Remote access is granted based on role and necessity.
- Remote work environments comply with organizational security standards.

A.6.8 – Information Security Event Reporting

InfoSec team shall ensure:

- Clear procedures are in place for reporting security events and weaknesses.
- Employees are trained to recognize and report incidents promptly.
- Reports are logged, assessed, and addressed in a timely manner.
- Feedback is provided to reporters to encourage continued vigilance.

A.7 – Physical Controls

A.7.1 – Physical Security Perimeter

InfoSec team shall ensure:

- Physical boundaries are defined to protect information processing facilities.
- Access points are controlled and monitored to prevent unauthorized entry.
- Perimeter security measures are appropriate to the level of risk.
- Security perimeters are reviewed and updated, as necessary.

A.7.2 – Physical Entry Controls

InfoSec team shall ensure:

- Access to secure areas is restricted to authorized personnel.
- Entry logs are maintained and reviewed regularly.
- Visitors are supervised and their access is limited.
- Access rights are reviewed and revoked when no longer needed.

A.7.3 – Securing Offices, Rooms, and Facilities

InfoSec team shall ensure:

- Workspaces are secured against unauthorized access.
- Sensitive areas are locked when unattended.
- Security measures are proportionate to the sensitivity of information managed.
- Regular inspections are conducted to ensure compliance.

A.7.4 – Physical Security Monitoring

InfoSec team shall ensure:

- Surveillance systems are implemented to monitor sensitive areas.
- Monitoring equipment is maintained and functioning correctly.
- Recorded footage is stored securely and retained as per policy.
- Monitoring data is reviewed to detect and respond to incidents.

A.7.5 – Protection Against Physical and Environmental Threats

InfoSec team shall ensure:

- Facilities are protected against natural disasters and environmental hazards.
- Fire detection and suppression systems are installed and maintained.
- Environmental controls (e.g., temperature, humidity) are monitored.
- Contingency plans are in place for physical emergencies.

A.7.6 – Working in Secure Areas

InfoSec team shall ensure:

- Access to secure areas is limited to authorized individuals.
- Activities within secure areas are supervised and logged.
- Security procedures are followed diligently within these areas.
- Regular audits are conducted to ensure compliance.

A.7.7 – Clear Desk and Clear Screen Policy

InfoSec team shall ensure:

- Employees clear desks of sensitive information when unattended.
- Computer screens are locked when not in use.
- Policies are communicated and enforced across the organization.
- Compliance is monitored through periodic checks.

A.7.8 – Equipment Siting and Protection

InfoSec team shall ensure:

- Equipment is positioned to minimize unauthorized access and damage.
- Cables and devices are secured against tampering.
- Environmental factors are considered in equipment placement.
- Regular maintenance is performed to ensure equipment integrity.

A.7.9 – Security of Assets Off-Premises

InfoSec team shall ensure:

- Policies govern the use of organizational assets outside premises.
- Portable devices are encrypted and protected against loss or theft.
- Employees are trained on secure handling of off-site assets.
- Incidents involving off-premises assets are reported and investigated.

A.7.10 – Storage Media

InfoSec team shall ensure:

- Storage media are protected against unauthorized access and damage.
- Media handling procedures are established and followed.
- Access to media storage areas is controlled.
- Media inventories are maintained and audited regularly.

Management of Removable Media

- Usage of removable media is discouraged as part of best security practices However, for a business requirement, removable media shall be issued only after the approved “Security Exception”.
- Employees shall obtain the ‘Security Exception’ from Manager and Lead InfoSec for the use of removable media for business purposes.

- Employees shall not transfer any information from removable media to any personal device without the consent of the Manager and Lead Infosec.
- In the event of loss of removable media, the user shall inform the function head and Infosec.

B. Disposal of Media

- Media containing critical and sensitive information shall be disposed of in a secure manner as per the Media Disposal Procedure.
- The technique used for disposal depends on the type of media and the classification of information that is contained in the media.
- Disposal shall be done only by authorized users and a record shall be maintained by the media disposal.
- The previous contents of any re-usable media that are to be removed shall be erased in such a way so that it cannot be recovered. Such disposals shall be authorized by Functional Heads and Infosec.
- Damaged storage devices containing sensitive data may require a risk assessment to determine if the items must be destroyed, repaired, or discarded.

A.7.11 – Supporting Utilities

InfoSec team shall ensure:

- Utilities supporting information systems (e.g., power, cooling) are dependable.
- Backup systems are in place for critical utilities.
- Utility failures are detected and addressed promptly.
- Maintenance schedules are established for utility systems.

A.7.12 – Cabling Security

InfoSec team shall ensure:

- Cables are protected against interception and damage.
- Cable routes are documented, and access is restricted.
- Regular inspections are conducted to detect unauthorized modifications.
- Cable management practices minimize risk of disruption.

A.7.13 – Equipment Maintenance

InfoSec team shall ensure:

- Equipment is maintained according to manufacturer guidelines.
- Maintenance activities are scheduled and documented.
- Only authorized personnel perform maintenance tasks.
- Security controls are reinstated after maintenance.

A.7.14 – Secure Disposal or Reuse of Equipment

InfoSec team shall ensure:

- Data is securely erased from equipment before disposal or reuse.
- Disposal methods comply with organizational policies and regulations.
- Records of disposal activities are maintained.
- Equipment is checked to ensure all data has been removed.

A8.1 - User end point devices

InfoSec team shall ensure:

- that security policies and procedures are established and implemented for the secure configuration, deployment, and use of user end point devices (e.g., laptops, desktops, mobile devices).
- that appropriate security controls (e.g., anti-malware, endpoint detection and response) are implemented on user end point devices to protect against threats.
- that users are provided with guidance and training on the secure use of their end point devices.

A8.2 - Privileged access rights

InfoSec team shall ensure:

- that the assignment and use of privileged access rights are restricted to authorized personnel based on the principle of least privilege.
- that privileged access is regularly reviewed, monitored, and controlled through strong authentication and authorization mechanisms.
- that activities performed with privileged access are logged and audited.

A8.3 - Information access restriction

InfoSec team shall ensure:

- that access to information is restricted based on business requirements and the principle of least privilege, considering the sensitivity and criticality of the information.
- that access control mechanisms (e.g., role-based access control, attribute-based access control) are implemented and enforced.
- that access rights are regularly reviewed and updated.

A8.4 - Access to source code

InfoSec team shall ensure:

- that access to source code is restricted to authorized personnel involved in development and maintenance activities.
- that secure repositories and access control mechanisms are in place to protect the integrity and confidentiality of source code.
- that changes to source code are managed through a controlled versioning system.

A8.5 - Secure authentication

InfoSec team shall ensure:

- that strong authentication methods (e.g., multi-factor authentication) are implemented to verify the identity of users accessing systems and information.
- that password policies are enforced, including complexity, rotation, and prevention of reuse.
- that authentication mechanisms are protected against bypass and compromise.

A8.6 - Capacity management

InfoSec team shall ensure:

- that the capacity requirements of information processing facilities are planned, monitored, and adjusted to meet current and future business needs, considering security implications of resource constraints or overloads.
- that adequate capacity is maintained to support secure operations and prevent denial-of-service conditions.

A8.7 - Protection against malware

InfoSec team shall ensure:

- that measures are implemented to protect against malware (e.g., viruses, worms, ransomware) through the use of anti-malware software, user awareness training, and secure handling of removable media and external content.
- that anti-malware solutions are kept up to date with the latest signatures and that regular scans are performed.

A8.8 - Management of technical vulnerabilities

InfoSec team shall ensure:

- that technical vulnerabilities in information systems and software are identified, assessed, and managed through a systematic process, including regular vulnerability scanning, timely patching, and the implementation of mitigating controls.
- that a vulnerability management policy and procedures are established and followed.
- Scope for technical vulnerability assessments shall be defined and performed on a periodic basis. The risks identified during these assessments shall be recorded and an action plan shall be developed.

\

A8.9 - Configuration management

InfoSec team shall ensure:

- that the security configurations of information systems and services are defined, documented, implemented, and maintained, and that changes to these configurations are managed through a controlled process.
- that baseline security configurations are established and enforced.

A8.10 - Information deletion

InfoSec team shall ensure:

- that information is securely deleted when it is no longer needed according to defined retention policies and procedures, preventing unauthorized access or recovery.
- that appropriate methods for data sanitization are used based on the sensitivity of the information and the storage media.

A8.11 - Data masking

InfoSec team shall ensure:

- that data masking techniques are used to protect sensitive data, replacing real data with realistic but anonymized or pseudonymized data.
- that the data masking process is appropriately controlled and monitored.

A8.12 - Data leakage prevention

InfoSec team shall ensure:

- that data leakage prevention (DLP) measures are implemented to monitor and control the transmission and storage of sensitive information to prevent unauthorized disclosure or loss.
- that DLP policies are defined and enforced across relevant channels

A8.13 - Information backup

InfoSec team shall ensure:

- that backups of critical information and software are performed regularly and stored securely in accordance with a defined backup policy, considering retention periods and recovery requirements.
- that backup procedures are evaluated to ensure reliable restoration capabilities.

A8.14 - Redundancy of information processing facilities

InfoSec team shall ensure:

- that appropriate redundancy is implemented for critical information processing facilities to maintain availability in case of failures or disruptions.
- that failover mechanisms are in place and regularly evaluated.

A8.15- Logging

InfoSec team shall ensure:

- that relevant activities and events on information systems are logged to provide an audit trail for security monitoring, incident analysis, and accountability.
- that log data is securely stored and protected from tampering and unauthorized access.
- Guidelines for identifying information systems and the events to be logged within the information system shall be defined.

- Logging shall be enabled on the identified information systems to ensure that all identified events are logged
- Log information shall be protected against unauthorized access, alterations, and operational problems. Access to logs shall be provided on 'need-to-know' and 'need-to-have' basis.

A8.16- Monitoring activities

InfoSec team shall ensure:

- that information systems and security controls are continuously monitored for suspicious activity, security incidents, and performance issues.
- that monitoring tools and processes are in place and that alerts are generated and responded to appropriately.

A8.17- Clock synchronization

InfoSec team shall ensure:

- that the clocks of relevant information processing systems within the organization are synchronized to a common and reliable time source to support accurate logging, incident analysis, and the effectiveness of time-sensitive security controls.

A8.18 - Use of privileged utility programs

InfoSec team shall ensure:

- that the use of privileged utility programs is restricted to authorized personnel and for legitimate operational and maintenance purposes only.
- that the execution of privileged utility programs is logged and monitored.

A8.19 -Installation of software on operational systems

InfoSec team shall ensure:

- that the installation of software on operational systems is controlled and authorized to prevent the introduction of malware or unauthorized functionality.
- that a formal process for software installation and testing is in place.

A8.20 - Networks security

InfoSec team shall ensure:

- that the organization's networks are designed, implemented, and managed securely, with appropriate segmentation, access controls, and security measures to protect against unauthorized access, modification, or disruption.
- that network security controls (e.g., firewalls, intrusion detection/prevention systems) are properly configured and maintained.

A8.21 - Security of network services

InfoSec team shall ensure:

- that network services are securely configured and managed, minimizing unnecessary services and ensuring appropriate access controls are in place.
- that network services are monitored for vulnerabilities and unauthorized activity.
- Networks shall be adequately managed and controlled to be protected from threats and to maintain security for the systems and applications using the network, including information in transit on and off cloud.
- All end user systems connected to the JK Cement's infrastructure must be hardened, patched, and installed with updated anti-malware software.

A8.22 - Segregation of networks

InfoSec team shall ensure:

- that networks are logically or physically segregated based on sensitivity levels and business requirements to limit the impact of security incidents and restrict unauthorized access between different network segments.

A8.23 - Web filtering

InfoSec team shall ensure:

- that web access is controlled and filtered to prevent access to malicious or inappropriate websites, reducing the risk of malware infections and policy violations.

A8.24 - Use of cryptography

InfoSec team shall ensure:

- that cryptographic controls are used appropriately to protect the confidentiality, integrity, and availability of information, in accordance with a defined cryptographic policy.
- that appropriate algorithms, key lengths, and key management procedures are implemented.

A8.25 - Secure development life cycle

InfoSec team shall ensure:

- that a secure development lifecycle (SDLC) is implemented for the development of software and systems, incorporating security considerations at each stage, including requirements gathering, design, coding, testing, and deployment.
- that secure coding practices and vulnerability assessments are integrated into the SDLC.
- JK Cement shall ensure that information security requirements are included at the design phase for new systems acquisition/ development. The testing of the security functionality of the system(s) shall be carried before Go-Live.

A8.26 - Application security requirements

InfoSec team shall ensure:

- that security requirements are defined and documented for all application software, addressing confidentiality, integrity, and availability.
- that these requirements are considered throughout the application development lifecycle.

A8.27 - Secure system architecture and engineering principles

InfoSec team shall ensure:

- that information systems are designed and engineered based on secure architecture principles, minimizing vulnerabilities and maximizing resilience.
- that security is considered as an integral part of the system design and engineering process.

A8.28 - Secure coding and security testing in development and acceptance

InfoSec team shall ensure:

- that secure coding practices are followed during software development and that code is reviewed for security vulnerabilities.
- that security testing (e.g., static, and dynamic analysis) is performed throughout the development and acceptance phases.

A8.29 - Outsourced development

InfoSec team shall ensure:

- that security requirements are clearly defined and agreed upon with outsourced development providers.
- that the security practices of outsourced development providers are monitored and assessed.

A8.30 - Separation of development, test, and production environments

InfoSec team shall ensure:

- That different types of environments are logically or physically separated to prevent unauthorized access or changes to production systems and data.

A8.31- Change management

InfoSec team shall ensure:

- that a formal change management process is established and implemented to control all changes to information systems, applications, and infrastructure, minimizing the risk of disruptions and security incidents.

A8.32 - Test information

InfoSec team shall ensure:

- that test data is managed appropriately and protected where necessary.

A8.33 - Test information (Post- Cleanup)

InfoSec team shall ensure:

- that all test accounts, data, and access privileges used during testing in the production environment are promptly removed or disabled upon completion of testing.
- that any configuration changes or software deployments made during testing in the production environment are thoroughly reviewed, approved, and documented before being finalized.

A8.34 - Protection of information systems during audit testing

InfoSec team shall ensure:

- that audit-related testing is planned and controlled to minimize disruption and protect information.

ASHISH TANDON
Digitally signed by ASHISH TANDON
Date: 2026.04.28 14:46:48 +05'30'

---------- **END OF DOCUMENT**----------