PRISM JOHNSON LIMITED
CIN: L26942TG1992PLC014033
Registered Office: 305, Laxmi Niwas Apartments, Ameerpet, Hyderabad – 500 016.
Corporate Office: "Rahejas", Main Avenue, V. P. Road, Santacruz (West), Mumbai – 400 054.

January 7, 2025

INFORMATION SECURITY POLICY

PURPOSE

The purpose of this Information Security Policy is to establish a comprehensive framework for safeguarding all IT assets and information systems from a wide range of threats in order to safeguard business and profits. It is to encourage the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

SCOPE

Information Security Management System (ISMS) is an overall management system, based on a business risk approach to manage sensitive company information so that it remains secure. It encompasses People, Process and Technology. It meets the following objectives:

- Protect the Company's information assets
- Keep confidential information secure
- Allows secure exchange of information
- Ensure compliance with legal obligations
- Manage and minimise risk exposure
- Build a culture of information security

RESPONSIBILITY

Information Security is everyone's responsibility in the Company.

- **Management:** All executives and management are responsible for promoting a culture of security within the Company and within their teams, ensure segregation of duties in compliance and in spirit.
- **IT Security Team**: The IT Security team is tasked with implementing and maintaining security measures, conducting risk assessments and responding to security incidents. They are responsible for enforcing this policy in close coordination with the HR department.

IT Security Officers	Division	Location	Email	Contact No.
Tapovardhan Singh	Cement	Satna	tapovardhan.singh@prismjohnson.in	9584693844
Sutanu Ganguly	HRJ	Mumbai	ganguly.sutanu@hrjohnsonindia.com	9594090254
Shyamsunder Iyer	RMC	Mumbai	shyam.iyer@rmcindia.com	8879321181
Sutanu Ganguly	Corporate	Mumbai	ganguly.sutanu@hrjohnsonindia.com	9594090254

- **Employees and Users**: All personnel must adhere to this policy, follow security guidelines and promptly report any security incident or concern to the IT team.

INFORMATION SECURITY POLICY

I. Data Security & Protection

- Addresses data encryption, password protection and access control
- Ensure that all IT assets which have reached the end of their life are disposed, as per the process outlined in IT asset management policy/procedure document
- Implement strong encryption controls when data is exchanged between two information systems
- Block access to social media to all users (excluding senior management), unless approved by the Department Head and IT Head
- Install anti-virus software on all users' laptops and desktops to ensure security of end computing devices

Data Owners

All information assets with Prism Johnson Limited will have a designated owner. Department Heads responsible for the business processes that generate and utilize the information/data in the systems used by users in that department are considered as owners of that data/information.

Data owners may delegate ownership of some or all the information systems to a designated team member from their department, however owners shall remain accountable and oversee the delegated owners fulfil their responsibility.

Data Owners shall evaluate and classify sensitivity of data, define protection required for the data based on sensitivity, regulatory or business needs and define requirements for access to the data to users.

Data Custodians

Data custodians are individuals or organisations in physical or logical possession of the data of Data Owners. **Data custodian shall be responsible to:**

- Protect the data in their possession from unauthorized access, alteration, destruction or usage
- Ensure IT processes are in place to back up data from the information systems generating and storing the data
- Monitor the usage of IT system by their users

II. Data Retention / Backup Policy

The objective of this policy is to define the minimum guidelines and procedures for backup, recovery and retention of the information systems. Information stored and processed on Information Technology (IT) systems is vulnerable to accidental corruption or deletion caused due to hardware/software failures, and natural or man-made disasters. A backup and restore policy is essential to ensuring recovery of information and the ability to continue IT support of critical applications. System backups also are an essential component of contingency planning strategies.

Backups enable IT support personnel to quickly and reliably recover essential data and software in case of events resulting in data corruption and loss.

III. Physical Security and Access Control

- The physical area hosting the IT servers and applications should be identified and have restricted access by enforcing appropriate access controls to restrict unauthorized access to IT facilities/server room.
- Movement of equipment, hardware, software or information, in and out of the premises shall require permission and will be monitored through registers.
- Physical protection against damage from fire, flood, earthquake, explosion and other forms of natural and man-made disaster shall be continuously evaluated and appropriate action should be taken.
- Power and telecom cables carrying data should be protected from damage and been intercepted
- IT manager or the in-charge should conduct a survey at least once a year and maintain record of these observations
- IT/ Network function shall ensure that any networking equipment, gateways, Wireless access points, telecommunication lines and cabling racks/ distribution points in the office area are not physically accessible to people other than IT/ Technical function

IV. Web Site Security

- Ensure that SSL certificate is installed on all Websites
- VAPT to be done at least one a year, and /or when major changes like website is redesigned
- Ensure SSL Certificate is valid and keep a track of its renewal
- Ensure SSL Certificate should use at least 2048 bit encryption or higher
- Disable support for SSL 2.0, SSL3.0, TLS 1.0 at the server level. Use TLS 1.2
- Disable weak ciphers such as DES, 3DES, RC4; Use Strong Ciphers such as AES, GCM
- All default user names and IIS/apache pages (like admin, default.aspx, index.aspx, etc) should be renamed. The access URL for admin panel/CMS, should also be renamed
- The Web Server processes should not be running under Administrator or Root user Account; A dedicated user account with limited privileges should be used for the Web Server processes
- Ensure that no unauthorised software/cracks, should be installed on the machine

V. Antivirus and Anti-malware

- Servers, desktops, workstations, hand-held devices, gateways and any other access points to PJL's network shall be protected against malicious activities and softwares.
- Anti-virus application and processes shall be put in place to facilitate early detection, efficient containment and eradication of malicious code. Adequate user awareness measures shall be implemented for the same. Updating of anti-virus definition files shall be done on a regular basis.
- Controls shall be considered to prevent unauthorized software execution.
    - Protection software such as anti-virus, anti-malware needs to be installed on information systems controlled / used by PJL.

- The software shall be capable of being updated on a periodic basis from an authentic source of malicious software information.
- The software must provide real time protection.
- Servers, desktops, workstations or gateways shall not be allowed access to PJL's Network without an Enterprise Anti-Virus.
- Malicious activity detected by the software shall be reported to an enterprise system which shall be monitored, and unresolved malicious activity shall be raised as incidents and tracked for closure as per the incident management policy

VI. Network Security

- Prism Johnson deploys perimeter security systems (Firewall, Antivirus) to protect all information assets from unauthorized or illegal access at the network level.
- Users shall only be provided with access to the services that they have been specifically authorised.
- Only authorised users shall be permitted to establish remote connections to the network using secure channels.
- Any connection to Prism Johnson's business critical transaction systems like ERP system shall be require VPN to access from outside

Application Access Controls

- Logical access to the application software shall be restricted to authorized users.
- Access to application functionalities shall be role based
- User access (except administrators) to data repositories shall be approved by functional/department heads
- Application access for critical applications shall be reviewed twice in a year
- Privilege users access shall be reviewed on monthly basis

VII. Third Party & Remote Access

Vendors/contractors engaged for support will be provided remote access. The modes of connectivity to Prism Johnson's Internal Network and Cloud (AWS) should be provided through VPN or other secured network.

Basic information Security principles such as least privilege, role based access and defence in depth shall be applied.

SECURITY INCIDENT MANAGEMENT

- 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.
- Critical servers and network devices shall be configured to log / alert initialization, stopping or pausing of the audit logs.
- Security relevant logging shall be enabled at all times.
- The logs generated shall have relevant event attributes in event entries (e.g. IP address, username, time and date, protocol used, port accessed, method of connection, name of device and object name, etc.)

- Security incidents shall be reported from all relevant sources, including users, audit process, SOC, advisory team, customers, etc.
- All reported security incidents shall be responded and resolved timely, and if not, then escalated
- Security Team shall investigate the cause of all reported security incidents. Wherever required, they shall also verify the implementation of recovery solutions.
- Security Team shall collect significant evidence for conducting necessary investigation. The events and logs shall be retained for a period as required by legal, regulatory or other compliance obligations.
- Security Team shall perform Forensic investigations for incidents requiring investigation for legal purposes and /or severe information security incidents.
- All security incidents and breaches shall be discussed with management on quarterly basis.

BASELINE SECURITY AND VULNERABILITY MANAGEMENT

- For all system components and applications standard baseline security parameters will be implemented
- Applications and IT infrastructure shall be subject to periodic technical assessments like Application Security Review, Vulnerability Assessments and Penetration Testing.
- Cyber Security Team shall conduct periodic vulnerability scans as per defined cycle and share report with system owners for closure of findings
- Penetration testing/VAPT of public facing systems as well as other critical applications shall be carried out by professionally qualified teams

TRAINING

- The IT/Cyber Security Team shall conduct periodic sessions to make employees and third-party personnel aware of the procedures for identifying different types of security events.
- Periodically conduct cyber security related awareness campaigns

RISK ASSESSMENT

- Risk assessment exercise is ongoing to identify and evaluate various information security risks faced by the Company.
- The internal audit team reviews and identifies the risk considering the strategic direction of business goals, effectiveness of ITCG controls, regulatory obligations and compliance
- Based on the business impact and the likelihood of risk occurrence, the required controls are prioritized and implemented.
- Prism IT team shall assess, the risks prior to the acquisition or outsourcing of information security services
- Status of Identified risks and corresponding treatment plan shall be reviewed by the management committee on quarterly basis in the IT risk management meeting.
- The management committee reviews the findings of risk reports and breaches of risk tolerances and policies if any.

ACCEPTABLE USE OF IT ASSETS POLICY

Purpose

Technology-based solutions and communication devices are woven into all aspects of our professional and personal lives. The purpose of this document is to provide guidance and information as a framework to consider when making use of the technology related decisions, use of IT services and products provided by Prism Johnson Limited. This will help guide choices or actions that are not acceptable.

This is applicable to all employees, contractors and service providers who are required to use company's IT resources, network and devices.

Guidelines

Usage of Information Systems

- You are responsible for exercising good judgment regarding appropriate use of company's data and IT resources (email, web sites, Internet services, Laptops, Desktops, Mobile Phone, Printers & Scanners etc.).
- Your actions must be conducted with integrity, respect, and prudent judgment. Use of information systems and resources for personal usage or on behalf of a third party (i.e., political or religious or charitable organization, family member, etc.) is strictly prohibited.
- Downloading, printing and distributing of copyrighted articles, documents, disseminating proprietary data, company's confidential or intellectual property or other confidential information is strictly prohibited
- Users should always lock their screen with password protected screen saver while leaving their Desktop, Laptops or mobile phone unattended.
- Users are prohibited from changing their device configuration, removing, de-activation or otherwise tampering with any Virus and Malicious Software prevention / detection and software that has been installed on systems used by them.
- You are responsible for exercising good judgment regarding consumption of information using company resources/devices. Use and distribution of pornographic material, playing computer games is strictly prohibited.
- Prism Johnson Limited has the right to monitor and remotely backup the company owned data/information form applications and data stored on personal devices while they are enrolled with the company

Responsibilities of Employee

- Each user has the responsibility to notify his Department Head and IT Head immediately of any incidence or suspicion of any security violation with regards to:
    - The presence of a virus on a PC.
    - Instances related to any unauthorized disclosure, modification, damage or loss of sensitive company information
- Apparent tampering with any file for which the user is given restricted use or any Information Security controls are tampered with may lead to punitive action against the violator.
- The employee is responsible for protection of all forms of Prism Johnson's data that is contained in the personal device
- Each user is responsible for keeping his devices secured by ensuring strong passwords. Device user Id and passwords should not be shared with anyone. In situations when the devices access has to be provided to third party for valid reasons (e.g. a technician visiting for repairs etc.), then concerned employee should ensure that the device is not left unattended and access to confidential folders, data files are protected.
- Those employees authorized to use social media in the workplace have the responsibility to use

the tools in an appropriate manner. Social media shall be used in a way that adds value to Prism Johnson's business. Prism Johnson's reputation is closely linked to the behaviour of its employees and everything that is reflected on Prism Johnson's social media channels (refer the Social Media Usage policy for more details)

- For sharing information with a group of employees, team within the company, users should use collaboration tools like Google Drive and not through public networks. Protect data using feature of sharing permissions while sharing files/folders.
- Company has automated the process of taking data backup. Each user's device data backup is done daily as per the company policy. It is duty of the user to ensure his device data is backed up daily, in case the backed has failed, intimate the IT department.
- Users should not install or use any unauthorized copies of any software. If they require any such software for official use, they should approach and make a request to their Department Head and IT head.
- Use of any open-source, freeware and shareware applications should be after formal approval process from their Department Head and IT head.

Use of Internet & Emails

Implied restrictions on Internet

- Sending emails to non-authorized individuals or accounts or services via an auto forwarding feature
- Users should be aware of the sites that are using. They should avoid using sites unless a secured connection is already established
- Company resources, devices network connectivity, email and other collaboration tools are meant for official purpose. Use of these resources for personal use are prohibited
- Users should use only their own official e-mail account for official correspondence and should not allow anyone else to access their email account. Users should identify themselves by their real name; pseudonyms that are not readily attributable to actual users should not be allowed.
- There are endless array of technology services and websites to consume. It is not possible to specifically list only those sites that can be accessed. User should act responsibility while consuming the content available on the internet. Any inappropriate use of company's resources may be grounds for appropriate discipline.
- Prohibited activities with e-mail include Jokes or language that may be considered discriminatory, harassing, unlawful, defamatory, obscene, offensive, insensitive or otherwise inappropriate. Employees may either communicate with the originator of the offensive emails, asking him/her to stop sending such messages, or report such offensive emails to the Head of Department.
- Users should not open any attachments to the email from an unknown, suspicious or untrustworthy source OR whose subject line is questionable or unexpected.
- Users should delete chain/junk emails and not forward or reply to any of the chain/junk mails. These types of email are considered Spam, which is unsolicited and intrusive that clogs up the network. User should follow strict discipline in this regard.
- Users should exercise caution when downloading files from the Internet and should download only from a legitimate and reputable source. Verify that an anti-virus program checks the files on the download site. If you're uncertain, don't download the file.
- Excessive personal surfing, utilizing streaming services for personal use such as listening to music or watching video, and downloading of music and video files
- Users should not send unsolicited bulk mail messages (also known as "junk mail" or "spam").

Use of Printers

- Use of printers is for official purpose only. Access to printer/s shall be controlled.
- Additional print outs should be avoided. Colour printouts should be avoided. User should

ensure that any wrong printout, sensitive or confidential in nature is immediately shredded
- IT team reserves the right to monitor the usage of printouts taken by the users

User Identification and Password Management

- A User-ID or account shall be assigned to each individual user to authorize a defined level of access to information assets and shall be protected by authenticating the user to the User-ID upon requesting access
- Each User-ID or account shall uniquely identify only one user or process. The permissions granted to him/her will be based on his role
- At least one in six months, IT will get the roles and permissions reviewed with respective Department/Functional heads
- In ERP application, user account shall be locked, after certain period of inactivity defined in the respective applications
- Generic User-IDs shall be created if necessary for business reasons
- Access rights of employees shall be revoked within when intimated by HR regarding termination of employment of the employee.
- **Privileged User Accounts:** Privileged user accounts are accounts with administrative access to applications, operating systems, network devices, databases components and other information systems enabling a user to modify system configurations including metadata, user records and other functions and override security and controls within the system to which administrative access applies. Privileged user account includes (but not limited to), system default administration account. "Administrator" or "root" or equivalent operating system accounts or any User-IDs capable of creating, modifying or deleting other User-IDs or their privileges or access logs. Privileged user accounts shall be limited to individuals with specific business justification for this level of access. Such access shall only be granted upon authorization from IT Head.
- An initial password shall be provided to the users / individuals securely during the user creation process and the system shall be configured to force the users to change the initial password immediately after the first logon.
- For Generating One Time Password, password will be in numeric value. Below password configuration will be followed for applications.
    - Minimum Password Length (6)
    - Combination of uppercase, lowercase, numbers and special characters
- Sharing of passwords with anyone is strictly forbidden.

CONSEQUENCE MANAGEMENT AND NON-COMPLIANCE

All violations of security policies, standards and/or guidelines are subject to disciplinary action.

The specific disciplinary action depends upon the nature of the violation, the impact of the violation on informational assets and related facilities, etc. Violations will be handled as per the existing HR processes and could range from verbal reprimand to termination of employment/contract and/or legal action.

If a department or function is unable to comply with any requirements detailed within this policy, an exception shall be obtained. Such exceptions shall be documented and approved by the management team in Enterprise Risk Management meeting indicating the rationale for the exception and the related risks.

POLICY REVISION

This policy will be periodically reviewed in order to ensure its continued adequacy and relevance. It may be amended at any time with the approval of the Chief Financial Officer (CFO) of the Company.

POLICY ENDORSEMENT

Mr. Rupesh Nirgude, the Chief Information Officer of the Company, is responsible for overseeing the implementation of the policy.