INFORMATION SECURITY POLICY
Kirloskar Pneumatic Company Limited

Introduction

Information security is a holistic discipline, meaning that its application, or lack thereof, affects all facets of an organization or enterprise. The goal of the Information Security Program is to protect the Confidentiality, Integrity, and Availability of the data employed within the Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited, while providing value to the way we conduct business.

Protection of the Confidentiality, Integrity, and Availability are basic principles of information security, and can be defined as:

Confidentiality – Ensuring that information is accessible only to those entities that are authorized to have access, many times enforced by the classic "need-to-know" principle.
Integrity – Protecting the accuracy and completeness of information and the methods that are used to process and manage it.
Availability – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorized entity.

Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited, has recognized that our business information is a critical asset and as such our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.

This document establishes the framework from which other information security policies may be developed to ensure that the enterprise can efficiently and effectively manage, control, and protect its business information assets and those information assets entrusted to by its stakeholders, partners, customers and other third parties.

The Information Security Program is built around the information contained within this policy and its supporting policies.

Purpose

The purpose of the Information Security Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to its business partners, and its stakeholders.

Audience

The Information Security Policy applies equally to any individual, entity, or process that interacts with any Information Resource.

Responsibilities

Executive Management

- Ensure that an appropriate risk-based Information Security Program is implemented to protect the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of.
- Ensure that information security processes are integrated with strategic and operational planning processes to secure the organization's mission.
- Ensure adequate information security financial and personnel resources are included in the budgeting and/or financial planning process.
- Ensure that the Security Team is given the necessary authority to secure the Information Resources under their control within the scope of the Information Security Program.
- Designate an Information Security Officer and delegate authority to that individual to ensure compliance with applicable information security requirements.
- Ensure that the Information Security Officer, in coordination with the Security Team, reports annually to Executive Management on the effectiveness of the Information Security Program.

Information Security Officer

- Chair the Security Team and provide updates on the status of the Information Security Program to Executive Management.
- Manage compliance with all relevant statutory, regulatory, and contractual requirements.
- Participate in security related forums, associations, and special interest groups.
- Assess risks to the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of.
- Facilitate development and adoption of supporting policies, procedures, standards, and guidelines for providing adequate information security and continuity of operations.
- Ensure that has trained all personnel to support compliance with information security policies, processes, standards, and guidelines. Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities.
- Ensure that appropriate information security awareness training is provided to District personnel, including contractors.
- Implement and maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices.
- Develop and implement procedures for testing and evaluating the effectiveness of the Information Security Program in accordance with stated objectives.
- Develop and implement a process for evaluating risks related to vendors and managing vendor relationships.

- Report annually, in coordination with the Security Team, to Executive Management on the effectiveness of the Information Security Program, including progress of remedial actions.

Information Security Team

- Ensure compliance with applicable information security requirements.
- Formulate, review, and recommend information security policies.
- Approve supporting procedures, standards, and guidelines related to information security.
- Provide clear direction and visible management support for information security initiatives.
- Assess the adequacy and effectiveness of the information security policies and coordinate the implementation of information security controls.
- Ensure that ongoing security activities are executed in compliance with policy.
- Review and manage the information security policy waiver request process.
- Review information security incident information and recommend follow-up actions.
- Promote information security education, training, and awareness throughout, and initiate plans and programs to maintain information security awareness.
- Report annually, in coordination with the Security Officer, to Executive Management on the effectiveness of the Information Security Program, including progress of remedial actions.
- All Employees, Contractors, and Other Third-Party Personnel
- Understand their responsibilities for complying with the Information Security Program.
- Use Information Resources in compliance with all Information Security Policies.
- Seek guidance from the Information Security Team for questions or issues related to information security.

Policy

- maintains and communicates an Information Security Program consisting of topic-specific policies, standards, procedures, and guidelines that:
    - Serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the organization using administrative, physical, and technical controls.
    - Provide value to the way we conduct business and support institutional objectives.
    - Comply with all regulatory and legal requirements, including: (adjust as appropriate)
        - HIPAA Security Rule,
        - State breach notification laws,
        - PCI Data Security Standard,
        - Information Security best practices, including ISO 27002 and NIST CSF,
        - Contractual agreements,
        - All other applicable federal and state laws or regulations.

The information security program is reviewed no less than annually or upon significant changes to the information security environment.

References

ISO 27002: 5, 6, 7, 18
NIST CSF: ID.AM, ID.BE, ID.GV, PR.AT, PR.IP

Waivers

Waivers from certain policy provisions may be sought following the Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Modified By	Approved Date	Approved By	Reason/Comments
1.0	28 june 2021	Dattatraya Parab	30 june 2021	Mandar Sahasrabudhe	Applicable for KMSPL
1.1	10 june 2023	Parag Kulkarni	16 june 2023	K. Srinivasan	Applicable for KPCL

-s/d-
K. Srinivasan
MD, KPCL

Enclosed –

1) Identity and Access Management Policy
2) Password Protection Policy
3) Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited - Acceptable / End User Policy
4) Physical Security Policy
5) Incident Response Plan

Identity and Access Management Policy

Purpose

The purpose of the Kirloskar Group / Kirloskar Pneumatic Company Limited's Identity & access management policy is to establish the requirements necessary to ensure that access and use of Information Resources, is managed in accordance with business requirements, information security requirements, and other policies and procedures.

Audience

This policy applies to individuals who are responsible for managing Information Resource access, and those granted access privileges, including special access privileges, to any Information Resource within Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited.

Contents

1. Access Control
    - Access to Information Resources must be justified by a legitimate business requirement prior to approval.
    - Where multifactor authentication is employed, user identification must be verified in person before access is granted.
    - Information Resources must have corresponding ownership & responsibilities are identified and documented.
    - Access to confidential information is based on a "need to know".
    - Confidential data access must be logged.
    - Access to the network must include a secure log-on procedure.
    - Workstations and laptops must force an automatic lock-out after a predetermined period of inactivity.
    - Documented user access rights and privileges to Information Resources must be included in disaster recovery plans, whenever such data is not included in backups.

2. Account Management

- All personnel must sign the Information Security Policy Acknowledgement before access is granted to an account or Information Resources.
- All accounts created must have an associated, and documented, request and approval.
- Segregation of duties must exist between access request, access authorization, and access administration.
- Information Resource owners are responsible for the approval of all access requests.
- User accounts and access rights for all Information Resources must be reviewed and reconciled at least annually, and actions must be documented.
- All accounts must be uniquely identifiable using the username assigned by IT and include verification that redundant user IDs are not used.
- All accounts, including default accounts, must have a password expiration that complies with the Authentication Standard.
- Only the level of access required to perform authorized tasks may be approved, following the concept of "least privilege".
- Whenever possible, access to Information Resources should be granted to user groups, not granted directly to individual accounts.
- Shared accounts must not be used. Where shared accounts are required, their use must be documented and approved by the Information Resource owner.
- User accounts set up for third-party cloud computing applications used for sharing, storing and/or transferring confidential or internal information must be approved by the resource owner and documented.
- Upon user role changes, access rights must be modified in a timely manner to reflect the new role.
- Creation of user accounts and access right modifications must be documented and/or logged.
- Any accounts that have not been accessed within a defined period will be disabled.
- Accounts must be disabled and/or deleted in a timely manner following employment termination, according to a documented employee termination process.
- System Administrators or other designated personnel:
    - Are responsible for modifying and/or removing the accounts of individuals that change roles with or are separated from their relationship with.
    - Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes.

- Must have a documented process for periodically reviewing existing accounts for validity.
- Are subject to independent audit review.
- Must provide a list of accounts for the systems they administer when requested by authorized IT management personnel.
- Must cooperate with authorized Information Security personnel investigating security incidents at the direction of executive management.

3. Administrator/Special Access

- Administrative/Special access accounts must have account management instructions, documentation, and authorization.
- Personnel with Administrative/Special access accounts must refrain from abuse of privilege and must only perform the tasks required to complete their job function.
- Personnel with Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Shared Administrative/Special access accounts should only be used when no other option exists.
- The password for a shared Administrative/Special access account must change when an individual with knowledge of the password changes roles, moves to another department or leaves altogether.
- In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency.
- Special access accounts for internal or external audits, software development, software installation, or other defined need, must be administered according the Authentication Standard.

4. Authentication

- Personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed and implemented according to the rules:
- Must meet all the requirements established in the Authentication Standard, including minimum length, complexity, and rotation requirements.
- Must not be easily tied back to the account owner by using things like username, social security number, nickname, relative's names, birth date, etc.

- Should not include common words, such as using dictionary words or acronyms.
- Should not be the same passwords as used for non-business purposes.
- Password history must be kept preventing the reuse of passwords.
- Unique passwords should be used for each system, whenever possible.
- Where other authentication mechanisms are used (i.e., security tokens, smart cards, certificates, etc.) the authentication mechanism must be assigned to an individual, and physical or logical controls must be in place to ensure only the intended account can use the mechanism to gain access.
- Stored passwords are classified as confidential and must be encrypted.
- All vendor-supplied default passwords should be immediately updated, and unnecessary default accounts removed or disabled before installing a system on the network.
- User account passwords must not be divulged to anyone. support personnel and/or contractors should never ask for user account passwords.
- Security tokens (i.e., Smartcard) must be returned on demand or upon termination of the relationship with, if issued.
- If the security of a password is in doubt, the password should be changed immediately.
- Administrators/Special Access users must not circumvent the Authentication Standard for the sake of ease of use.
- Users should not circumvent password entry with application remembering embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the IT Management.
- If a password management system is employed, it must be used in compliance with the Authentication Standard.
- Computing devices should not be left unattended without enabling a password protected screensaver or logging off the device.
- IT Support password change procedures must include the following:
    - authenticate the user to the helpdesk before changing password.
    - change to a strong password.
    - require the user to change password at first login.
- If a user's password is compromised or discovered, the password must be immediately changed, and the security incident reported to IT support.

5. Remote Access

- All remote access connections to the networks will be made through the approved remote access methods employing data encryption and multi-factor authentication.

- Remote users may connect to the networks only after formal approval by the requestor's manager or Management.
- The ability to print or copy confidential information remotely must be disabled.
- Users granted remote access privileges must be given remote access instructions and responsibilities.
- Remote access to Information Resources must be logged.
- Remote sessions must be terminated after a defined period of inactivity.
- A secure connection to another private network is prohibited while connected to the network unless approved in advance by IT management.
- Non- computer systems that require network connectivity must conform to all applicable IT standards and must not be connected without prior written authorization from IT Management.
- Remote maintenance of organizational assets must be approved, logged, and performed in a manner that prevents unauthorized access.

6. Vendor Access
    - Vendor access must be uniquely identifiable. and comply with all existing policies.
    - External vendor access activity must be monitored.
    - All vendor maintenance equipment on the network that connects to the outside world via the network, telephone line, or leased line, and all Information Resource vendor accounts will remain disabled except when in use for authorized maintenance.

References

- ISO 27002: 6, 7, 8, 9, 12, 15
- NIST CSF: PR.AC, PR. IP, PR.MA, PR.PT, DE.CM

Waivers

Waivers from certain policy provisions may be sought following the Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Password Protection Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of Kirloskar Group / Kirloskar Pneumatic Company Limited's entire network. As such, all Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited employees (including contractors and vendors with access to Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password. (See Physical Protection Policy for additional information).

2.0 Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited facility, has access to the Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited network.

4.0 Policy

4.1 General

- All systems-level passwords (e.g., root, enable, network administration, application administration accounts, server administration, database administration, local administration, Infosec administration etc.) must be changed at least every 180 days.
    - These passwords must then be carefully saved in an envelope & sealed and to be kept in custody of the IT head.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and cannot be reused the past 5 passwords.
- ·User accounts with privileges must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.

- All user-level, system-level, and access level passwords must conform to the guidelines as described below.

4.2 Guidelines

Password Construction Requirements

i. Be a minimum length of eight (8) characters on all systems.

ii. Not a dictionary word or proper name.

iii. Not be the same as the User ID.

iv. Expire within a maximum of 90/180 calendar days as per privilege categories mentioned in 4.1.

v. Not to be identical to the previous five (5) passwords.

vi. Not to be transmitted in the clear or plaintext outside the secure location in digital format.

vii. Not be displayed when entered.

viii. Ensure passwords are only reset for authorized users.

4.3 Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

- When a user retires, quits, is reassigned, released, dismissed, etc.
- Default passwords shall be changed immediately on all equipment.
- Contractor accounts, when no longer needed to perform their duties.

When a password is no longer needed, the following procedures should be followed:

· Employee should notify his or her immediate supervisor.

· Contractor should inform his or her point-of-contact (POC).

· IT team of Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited, will then delete the user's password and delete or suspend the user's account.

4.4 Password Protection Standards

Do not use your User ID as your password. Do not share Kirloskar Group / Kirloskar Pneumatic Company Limited's system passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited information.

Here is a list of "don'ts."

· Don't reveal a password over the phone to anyone

- Don’t reveal a password in an email message.
- Don’t reveal a password to the boss.
- Don't' talk about a password in front of others.
- Don’t hint at the format of a password (e.g., “my family name”)
- Don’t reveal a password on questionnaires or security forms.
- Don’t share a password with family members.
- Don’t reveal a password to a co-worker while on vacation.
- Don’t use the "Remember Password" feature of applications
- Don’t write passwords down and store them anywhere in your office.
- Don’t store passwords in a file on ANY computer system unencrypted.
- If someone demands a password, refer them to this document or have them call [Information Security Officer (ISO)].
- If an account or password is suspected to have been compromised, report the incident to ISO or POC and change all passwords.
- Password cracking or guessing may be performed on a periodic or random basis by the MSP/FBI or [agency Security Department or POC]. If a password is guessed or cracked during one of these scans, the user will be required to change it.

4.5 Application Development Standards

Application developers must ensure their programs contain the following security precautions:

· Should support authentication of individual users, not groups.

· Should not store passwords in clear text or in any easily reversible form

· Should provide some sort of role management, such that one user can take over the function of another without having to know the other’s password.

· Should support Terminal Access Controller Access Control System+ (TACACS+), Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval, wherever possible.

4.6 Remote Access Users

Access to the Kirloskar Group / Kirloskar Pneumatic Company Limited’s networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.).

5.0 Penalties

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited Acceptable / End User Policy

I. INTRODUCTION

This policy applies to all users of Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited information technology resources and systems.
Kirloskar Group / Kirloskar Pneumatic Company Limited'S information technology resources and systems include but are not limited to computer networks, systems, servers, software, databases, data and information, equipment and devices, email, WiFi, network, and the corporate internet connection.

All Users of Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited's information technology resources and systems must review, acknowledge and adhere to the contents of this policy.
A User is defined as anyone who has access or uses information technology resources and systems of Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited including but not limited to:

- All employees engaged full-time, part-time or hourly basis
- All contractors and third-party agents paid directly by the company or another party to work on behalf of Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited
- All employees of partners, customers, consultants, vendors and visitors of Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited

II. OBJECTIVES

- To provide guidelines, that ensure Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited's IT resources and systems are used in a professional manner and in a way that does not compromise or damage Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited and/or its business partners or employee's reputation in any way and maintains the confidentiality, integrity and availability of all information and systems.
- To provide clear guidelines for usage of storage medium, terms of acceptable internet and email use.
- Minimize threat of accidental, unauthorized, or inappropriate access to either electronic or paper-based information owned by Kirloskar Group / Kirloskar Pneumatic Company Limited / Kirloskar Pneumatic Company Limited or temporarily entrusted to it.

III. TERMS OF POLICY

A. General Requirements

i. Users are responsible for exercising good judgment regarding appropriate use of Kirloskar Group / Kirloskar Pneumatic Company Limited's IT resources and systems in accordance with Kirloskar Group / Kirloskar Pneumatic Company Limited's policies, standards and guidelines. Kirloskar Group / Kirloskar Pneumatic Company Limited's IT resources and systems must not be used for any unlawful or prohibited purposes.

ii. For security, compliance and maintenance purposes, authorized personnel may monitor and audit IT Assets including equipment, systems and network traffic as per the Information Security Policy. Devices that interfere or disrupt the working of other devices or users on Kirloskar Group / Kirloskar Pneumatic Company Limited's network may be disconnected. Information Security prohibits actively blocking authorized audit scans.

B. System Accounts

i. Access to Kirloskar Group / Kirloskar Pneumatic Company Limited's IT Resources and Systems including all data, systems, applications is controlled using User ID and password for each user.

ii. Users are responsible for the security of data, accounts and systems under their control. Users need to ensure that passwords are secure and account or password information is not shared with anyone. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

iii. User shall not allow anyone else to use their user ID and password on any Kirloskar Group / Kirloskar Pneumatic Company Limited IT Assets including systems and applications.

iv. Users must maintain system-level and user-level passwords in accordance with the password requirements of the respective application.

v. Users must ensure that proprietary information always remains within the control of Kirloskar Group / Kirloskar Pneumatic Company Limited. Conducting Kirloskar Group / Kirloskar Pneumatic Company Limited's business that results in the storage of proprietary information on personal or non-Kirloskar Group / Kirloskar Pneumatic Company Limited controlled environments (eg., copying Kirloskar Group / Kirloskar Pneumatic Company Limited data on a third-party service provider's machine or vise versa while fixing a hardware issue on a Kirloskar Group / Kirloskar Pneumatic Company Limited machine), including devices maintained by a third party with whom Kirloskar Group / Kirloskar Pneumatic Company Limited does not have a contractual agreement or on personal devices, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by Kirloskar Group / Kirloskar Pneumatic Company Limited, or its customer and partners, for company business.

C. End User Devices

i. Company owned devices are provided to users to perform business related functions. Users shall ensure that company devices are not used for any unofficial, illicit or unauthorized purpose. The usage of the device includes both hardware and software installed on these devices. The policy applies to all end user devices that access or interact with company data and information systems.

ii. Users are responsible for ensuring the protection of assigned Kirloskar Group / Kirloskar Pneumatic Company Limited's IT resources and systems. Laptops left at Kirloskar Group / Kirloskar Pneumatic Company Limited's premises overnight must be properly secured or placed in a locked drawer or cabinet. Any loss or theft of Kirloskar Group / Kirloskar Pneumatic Company Limited's IT resources and systems must promptly be reported to the Information Security Group. In case of loss of laptop, it is the primary responsibility of the User to immediately lodge a FIR with the nearest police station and also inform the IT team on immediate basis. This responsibility of User is to be read in conjunction with the Laptop Policy separately issued by Kirloskar Group / Kirloskar Pneumatic Company Limited.

iii. All laptops and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Users must lock the screen or log off when the device is unattended.

iv. Users must not interfere with corporate device management or security system software, including, but not limited to antivirus, system updates and device monitoring in case any.

v. Users must not:
   - Use the device for purposes that are illegal, unethical and harmful to the Company. Examples of what users must not do are as given below,
   - Secondary business use: Conducting a personal business using the companies end user device.
   - Excessive personal use: Excessive use of an end user device for personal use, which then interferes with business functions being performed by the device.
   - Store non-business-related media files (games/music/movies/photographs) on Kirloskar Group / Kirloskar Pneumatic Company Limited owned devices.

D. Internet and E-mail Usage

i. Internet and e-mail facilities are provided by Kirloskar Group / Kirloskar Pneumatic Company Limited primarily for official business purpose only. Legitimate private and personal use in moderation will be tolerated, subject to the rules detailed in this policy. The email signature for official emails should be in compliance with the Corporate Identity Manual (CIM) as prescribed by Kirloskar Proprietary Limited.

ii. Employees and other authorized users may access internet and e-mail sites through the company's network or personal network on company provided end user devices for

conducting the company's business. Users are responsible for ensuring that the internet accessed outside company premises should be secure, effective, ethical and lawful.

iii. Kirloskar Group / Kirloskar Pneumatic Company Limited shall not accept any liability arising from the use of unsecured internet, e-mail and web content including social networking sites when accessed for private use and the user hereby indemnifies the company against any such liability.

The following are strictly prohibited and are considered as Unacceptable Use:

a) Inappropriate use of communication vehicles and equipment, including, but not limited to supporting illegal activities and procuring or transmitting material that violates Kirloskar Group / Kirloskar Pneumatic Company Limited's policies against harassment or the safeguarding of confidential or proprietary information.
b) Receive, send, store, download, print, distribute, or access any content that is offensive, harassing, fraudulent, racist, illegal or obscene (including any form of pornography).
c) Spam: Sending Spam via e-mail, text messages, instant messages, voice mail, or other forms of electronic communication.
d) Storing and Sharing unnecessary Information: Share (Send forward) and store media (e.g. Music, Video or similar content) and games or similar content.
e) Incorrectly represent company: Represent individual opinions as that of the company via e-mail or publication of unauthorized statements onto web sites, blogs, wikis, bulletin boards, discussion areas or newsgroups etc.
f) Modifying e-mail messages: Modify received e-mail message and forwarding/replying it, for example, deletions or modification of the received content such that they violate the integrity of the original message.
g) Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
h) Sharing and Disclosure of company confidential information: Transmit confidential information to any person in or outside Kirloskar Group / Kirloskar Pneumatic Company Limited, not authorized to receive it. Sharing PII (personally identifiable information) with external parties that do not have a contractual agreement with Kirloskar Group / Kirloskar Pneumatic Company Limited to access the PII.
i) Obtaining and sharing restricted information: Obtain or use copyrighted or restricted information to which the user does not have a right to obtain or use.
j) Public email services: Using public email services like personal Gmail, Yahoo, Hotmail, Outlook etc. is not allowed.
k) Peer-to peer (p2p) and Torrents: Usage of peer-to peer (P2P) and torrent sites within the Kirloskar Group / Kirloskar Pneumatic Company Limited infrastructure or its assets.
l) Online/cloud file storage and sharing services: Use of online/cloud file storage services like Personal Google drive, Dropbox, WeTransfer, Box to store company data.
m) Messenger, Chat and IRC services: Use chat and IRC services like WhatsApp on Kirloskar Group / Kirloskar Pneumatic Company Limited devices.

n) Proxy and VPN services: Using unofficial proxy or VPN services including TOR.
o) Software as a Service (SAAS), Platform as a Service (PAAS) and Infrastructure as a Service (IAAS): Use of any unauthorized SAAS, PAAS, IAAS services like Google Cloud Platform (GCP), Amazon Web Services (AWS), Microsoft Azure, Salesforce.com which are not approved by Kirloskar Group / Kirloskar Pneumatic Company Limited.
p) Use of a Kirloskar Group / Kirloskar Pneumatic Company Limited's e-mail or IP address to engage in conduct that violates Kirloskar Group / Kirloskar Pneumatic Company Limited's policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a Kirloskar Group / Kirloskar Pneumatic Company Limited e-mail or IP address represents Kirloskar Group / Kirloskar Pneumatic Company Limited to the public; therefore, Users must exercise good judgment to avoid misrepresenting or exceeding authority in representing the opinion of the company.
q) Use of any third party intellectual property rights including any third party trademark / logo / brand, etc. in the Kirloskar Group / Kirloskar Pneumatic Company Limited official email, which can be deemed as violation of such third party trademark / logo / brand, etc.
r) Refrain from transmitting or publishing any lascivious material or anything that appeals to the prurient interest that is likely to deprave and corrupt every person who reads, sees or hears the matter
s) Ensure not to commit the offence of cyber terrorism or any other offence under Information Technology Act, 2000.
t) Use the Kirloskar Group / Kirloskar Pneumatic Company Limited internet or email to make personal gains or conduct a personal business.
u) In any way infringe any copyright, database rights, trademarks or other intellectual property.

E. **Network Use**

i. Users are responsible for the security and appropriate use of Kirloskar Group / Kirloskar Pneumatic Company Limited's network resources under their control. Using Kirloskar Group / Kirloskar Pneumatic Company Limited's resources for the following is strictly prohibited:
ii. Causing a security breach to either Kirloskar Group / Kirloskar Pneumatic Company Limited's or other network resources, including but not limited to accessing data, servers, or accounts to which Users are not authorized; circumventing user authentication on any device; or sniffing network traffic.
iii. Causing a disruption of service to either Kirloskar Group / Kirloskar Pneumatic Company Limited's or other network resources, including but not limited to ICMP floods, packet spoofing, denial of service, heap or buffer overflows and forged routing information etc. for malicious purposes.
iv. Introducing honeypots, honeynets, or similar technology on Kirloskar Group / Kirloskar Pneumatic Company Limited's network.
v. Violating copyright law, including but not limited to illegally duplicating or transmitting copyrighted pictures, music, video and software.

vi. Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.
vii. Use of the Internet or Kirloskar Group / Kirloskar Pneumatic Company Limited's network that violates Kirloskar Group / Kirloskar Pneumatic Company Limited's policies, or local laws.
viii. Intentionally introducing malicious code, including but not limited to viruses, worms, Trojan horses, e-mail bombs, spyware, adware, keyloggers etc.
ix. Port scanning or security scanning on a production network unless authorized in advance by Information Security.

F. Physical Security

It is company policy to protect Kirloskar Group / Kirloskar Pneumatic Company Limited IT Infrastructure and Assets physically and prevent misuse, theft, fraud and unauthorized access from physical and environmental hazards. Care must be taken to safeguard electronic equipment and IT Assets assigned to users. Users will be accountable for any loss or damage.

Users must:

a) **Securely store IT Assets and data:** All users that have been provided with company assigned laptops shall safeguard them appropriately. All confidential and sensitive information shall be safeguarded using appropriate controls.
b) **Refrain from use of Hazardous substances:** Hazardous substances that could cause damage to hardware such as food, liquids, chemicals, etc.
c) **Refrain from making Changes to equipment:** Any changes like equipment installations, disconnection, modifications and relocations shall be done by IT Team only and not by the user themselves unless approved by IT Team.
d) **Taking equipment offsite:** No equipment shall be taken out of the office unless approved by the reporting manager or department head.
e) **Unauthorized equipment:** Users shall not connect any equipment (that is not property of Kirloskar Group / Kirloskar Pneumatic Company Limited) to Kirloskar Group / Kirloskar Pneumatic Company Limited network.

User must not remove or disable anti-virus software or attempt to remove virus-infected files or clean up an infection without coordinating with IT Department.

G. Software Copyright and License Agreements

All software acquired/developed by Kirloskar Group / Kirloskar Pneumatic Company Limited employees or contract personnel on behalf of the Kirloskar Group / Kirloskar Pneumatic Company Limited shall be deemed Kirloskar Group / Kirloskar Pneumatic

Company Limited's property. All such software must be used in compliance with applicable licenses, notices, contracts and agreements.

Users shall therefore ensure the following things,

a) **Copyright protection:** Not to create copy or share the software with any unauthorized person or third party.
b) **Software installation:** Software that is licensed or owned by the company must be installed on company devices only.
c) **Refrain from Downloading and installing software:** Not to download and install software without approval from IT team and must not use any unlicensed software.

H. Digital Signatures

a) Ensure not to fraudulently or dishonestly make use of electronic signatures.
b) Ensure not to knowingly create, publish or otherwise make available Electronic Signature Certificate for any fraudulent or unlawful purpose.
c) Use digital signatures or electronic signatures with prior approval of Business Head and keep a track of documents and communications where digital signatures or electronic signatures are used.
d) The custodian of the digital signature will be solely responsible and accountable for use /misuse of the digital signature by self or by other who are authorized by the custodian to use the signature.

I. Mobile Devices and Home Computing Usage

a) Use of Kirloskar Group / Kirloskar Pneumatic Company Limited Owned Devices

This section of the policy applies to any users with a company owned laptop, tablet or equivalent mobile device used to access the company's network or information resources whilst within or outside Kirloskar Group / Kirloskar Pneumatic Company Limited network (travelling, working from home or any remote location). Users shall take due care to ensure that the devices are not lost or stolen, and data is accessed by authorized users only. To ensure the safety of the mobile device and data users need to be vigilant of the environment in which they are working in.

b) Use of Personal Devices

Users using their personal devices to access Kirloskar Group / Kirloskar Pneumatic Company Limited data and systems are required to enroll their devices with the organizational mobile device management solution which provides Kirloskar Group / Kirloskar Pneumatic Company Limited the

ability to control and monitor the use of such data and applications with an objective to prevent loss of sensitive data.

Users shall therefore ensure the following when using mobile devices:

Password protection: Ensure that access to information contained on the mobile device will be protected by a password.

Encryption: Ensure that all business-related data on personal devices is encrypted by using appropriate means of encryption.

Prevent Unauthorized users: Ensure that under no circumstances any unauthorized user can use the mobile device, this includes lending the device or handing over physical possession of the device to an unauthorized person for known or unknown use.

Use of Secure communication channel: Ensure the use of company assigned VPN (Virtual Private Network) when accessing company network remotely.

Ensure privacy of Screens: While travelling and in public areas users need to prevent visual exposure of Kirloskar Group / Kirloskar Pneumatic Company Limited data and ensure the privacy of data that screens are not visible to general public.

Passwords security: Do not save any passwords or access codes anywhere on the device. This includes taping notes onto the device or keeping it inside the carry case of the device.

Do not share passwords and non-public information on the phone, in public places

Loss of Asset - Theft reporting: In the event of theft/loss of a mobile device, immediately report the theft to the company IT Security teams in addition to supervisor/manager.

IV. PROTECTION OF INFORMATION

- To perform regular duties and assigned tasks, users may be provided with access to information about Kirloskar Group / Kirloskar Pneumatic Company Limited's business services and its clients. Users must ensure information/knowledge they gain is used only for business purpose. All users must:
- Protect Information in digital or paper format as per the information classification guidelines. (Reference to Information Classification guidelines policy document)
- Printouts and paper copies of sensitive and critical information shall be handled properly and must not be left unattended or in common areas. These should be locked securely (in file cabinets) when not in use. Documents must be shredded if not required or beyond their retention period.

V. CIRCUMVENTION OF SECURITY

Using company-owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security, or otherwise access information for unauthorized purposes is expressly prohibited.

VI. MONITORING

Kirloskar Group / Kirloskar Pneumatic Company Limited reserves the right to monitor computer system, internet and email usage, to read and copy all files or data contained on any computer/storage at any time, with or without prior notice, except where prohibited by law.

VII. ENFORCEMENT

- Any deviation from this policy is strictly prohibited. Any deviation to or non-compliance with this policy shall be reported to the Information Security Group formulated by the Company more particularly defined as 'IT Council'.
- It is the User's responsibility to immediately report suspected breaches of security policy without delay to your Manager, the IT Department, the IT helpdesk or IT Council.
- Any user found to have violated this policy may be subject to disciplinary action, up to and including termination employment or contract.
- In case of termination of employment or contract, following actions will be taken:

a) All Kirloskar Group / Kirloskar Pneumatic Company Limited IT Assets, equipment and data, such as laptops and mobile devices, USB Memory devices, CDS / DVDs, etc, must be returned to Kirloskar Group / Kirloskar Pneumatic Company Limited at termination of contract and handed over to Kirloskar Group / Kirloskar Pneumatic Company Limited IT Department in good condition at the time of leaving from the employment of Kirloskar Group / Kirloskar Pneumatic Company Limited or in case of termination / expiry of Contract with Kirloskar Group / Kirloskar Pneumatic Company Limited.

b) All data or intellectual property developed or gained during the period of employment remains the property of Kirloskar Group / Kirloskar Pneumatic Company Limited and must not be retained beyond termination or reused for any other purpose.

VIII. EXCEPTION TO THE POLICY

Any exceptions to this policy must be approved by the Managing Director of the Company.

Physical Security Policy

Purpose

The purpose of the Kirloskar Group / Kirloskar Pneumatic Company Limited's Physical Security Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities.

Audience

The Kirloskar Group / Kirloskar Pneumatic Company Limited's Physical Security Policy applies to all Kirloskar Group / Kirloskar Pneumatic Company Limited's individuals that install and support Information Resources, are charged with Information Resource security and data owners.

Policy:

General:

- Physical security systems must comply with all applicable regulations including but not limited to building codes and fire prevention codes.
- Physical access to all restricted facilities must be documented and managed.
- All Information Resource facilities must be physically protected in proportion to the criticality or importance of their function at .
- Access to Information Resources facilities must be granted only to support personnel and contractors whose job responsibilities require access to that facility.
- All facility entrances, where unauthorized persons could enter the premises, must be controlled.
- Secure areas must be protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. This includes:
    - information processing facilities handling confidential information should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use;
    - controls should be adopted to minimize the risk of potential physical and environmental threats;
    - environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities.

- Directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorized.

- Equipment must be protected from power failures and other disruptions caused by failures in utilities.
- Restricted access rooms and locations must have no signage or evidence of the importance of the location.
- All Information Resources facilities that allow access to visitors will track visitor access with a sign in/out log.
- Card access records and visitor logs for Information Resource facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- Visitors in controlled areas of Information Resource facilities must be accompanied by authorized personnel at all times.
- Personnel responsible for Information Resource physical facility management must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

Access Cards

- The process for granting card and/or key access to Information Resource facilities must include the approval of a member of the physical security committee.
- Each individual that is granted access rights to an Information Resource facility must sign the appropriate access and non-disclosure agreements.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to personnel responsible for Information Resource physical facility management. Cards must not be reallocated to another individual, bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for Information Resource physical facility management physical security committee as soon as possible.
- Physical security committee must remove the card and/or key access rights of individuals that change roles within (District/Organization) or are separated from their relationship with (District/Organization).
- Physical security committee must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Incident Response Plan

Purpose

This document outlines the plan for responding to information security incidents at the Kirloskar Group / Kirloskar Pneumatic Company Limited, including defining the roles and responsibilities of participants, the overall characterization of incident response, relationships to other policies and procedures and guidelines for reporting requirements.

Due to the wide variety of incidents that could face the Kirloskar Group / Kirloskar Pneumatic Company Limited and the rapid advancement of threats against the group, its data and systems, this document is designed to provide guidance in reacting to data security incidents, determination of their scope and risk, and ensuring an appropriate response to information security incidents, including communication of incidents to the appropriate stakeholders, and reducing the incident from reoccurring.

This protocol is not to be considered as policy due to the varied nature of incidents that can occur within a group environment. This variation in incidents may cause deviations from this protocol that are meant to provide the Kirloskar Group / Kirloskar Pneumatic Company Limited's ability to respond to incidents in an optimal manner.

Anyone suspecting an exposure of group data or systems should immediately contact:

Manoj Gaikwad (KPCL) – manoj.gaikwad@kirloskar.com:9922937118

Parag Kulkarni (KPCL) – parag.kulkarni@kirloskar.com: 7796690039

Mandar Sahasrabudhe (KMSPL): mandar.sahasrabudhe@kirloskar.com: 9881464860

Scope

This plan applies to all information systems, institutional data, and networks of The Kirloskar Group / Kirloskar Pneumatic Company Limited and any person or device accessing these systems or data.

The Group's Information Security Office (ISO) acts on behalf of the Kirloskar Group / Kirloskar Pneumatic Company Limited and will request cooperation and assistance in investigating incidents from group entities as required. The ISO will also work closely with other Kirloskar Group / Kirloskar Pneumatic Company Limited such as in the investigation of incidents as necessary.

Maintenance

The Group's Information Security Office (ISO) is responsible for the maintenance and revision of this document.

Definitions

Event

An event is an exception to the normal operation of IT infrastructure, systems or services. Events may be identified through the use of automated systems; reported violations to the ISO, Compliance/Privacy or other entities; or in the course of normal system reviews including system degradation/outage. It is important to note that not all events become incidents.

Incident

An incident is an event that, as assessed by ISO staff, violates the Acceptable Use Policy, Access Control Policy, Confidential Data Policy or other Kirloskar Group / Kirloskar Pneumatic Company Limited policy, standard, or Code of Conduct or threatens the confidentiality, integrity, or availability of Information Systems or Institutional Data.

Regulated Data Classification

Regulated Data may have additional reporting and regulatory requirements when dealing with incidents. Examples of the various types of regulated data that may reasonably be found in the Kirloskar Group / Kirloskar Pneumatic Company Limited environment are further detailed in Appendix C.

Roles and Responsibilities

Chief Information Security Officer (CISO)

Throughout the course of the protocol, the CISO is broadly responsible for:

1. Coordinating efforts to manage an information security incident;
2. Ensuring the prompt investigation of a security incident;
3. Determining what Kirloskar Group / Kirloskar Pneumatic Company Limited data may have been exposed;
4. Securing any compromised systems to prevent further damage;
5. Providing guidance to the institutional stakeholders

Executive Response Team

The Executive Response Team (ERT) consists of Kirloskar Group / Kirloskar Pneumatic Company Limited Officials with the authority to make key decisions in managing an incident related to data with regulatory requirements for reporting. The ERT shall be comprised of the following standing members (note: other members may be asked to collaborate where appropriate):

- CISO
- General Counsel
- Representative from the Office of the promoters
- Kirloskar Group / Kirloskar Pneumatic Company Limited Communications
- Compliance and Risk Management (Cyber Liability Insurance)
- Director, or Department Head of the entity where the exposure is determined to have occurred

Incident Response Coordinator

Throughout the course of the protocol, the Incident Response Coordinator is broadly responsible for:

1. Directing efforts to gather appropriate information
2. Providing expertise in the procedural aspects of gathering information and documentation of process
3. Updating CISO and other leadership as necessary

Incident Response Handler

Throughout the course of the protocol, Incident Response Handlers are broadly responsible for:

1. Gathering data from systems
2. Providing specific expertise in technology and data
3. Entering appropriate data for Incident Management including procedural information

Incident Response Methodology

This plan outlines the general tasks for Incident Response. Due to the ever-changing nature of incidents and attacks upon the Kirloskar Group / Kirloskar Pneumatic Company Limited this incident response plan may be supplemented by specific internal guidelines, standards and procedures as they relate to the use of security tools, technology, and techniques used to investigate incidents.

Scope

The Information Security Office represents all Kirloskar Group / Kirloskar Pneumatic Company Limited provided Information System(s) and Institutional Data including data residing in cloud-based services. The Kirloskar Group / Kirloskar Pneumatic Company Limited operates in a partially decentralized environment with its entities maintaining their own IT staffs. To the extent possible during an investigation, the ISO will attempt to coordinate investigation efforts with other groups in ensuring the security of Kirloskar Group / Kirloskar Pneumatic Company Limited systems and data in relation to the activities in support of the group. Specific actions and resources utilized in the investigation of an incident will be in alignment with the type, scope and risk of the threat to group systems and data.

Evidence Preservation

The primary goals of incident response are to contain the scope of an incident and reduce the risk to systems and data and to return affected systems and data back to an operational state as quickly as possible. The ability to quickly return systems to operation may at times be hampered by the collection of data necessary as evidence in the event of an exposure of data.

Operational-Level Agreements

In today's technology centered world many individuals have expectations about the availability of systems and data for themselves and the constituents they serve. The interruption of services can cause hardship and the ISO will cooperate with the affected groups to ensure downtime is minimized. However, Kirloskar Group / Kirloskar Pneumatic Company Limited leadership supports the priority of investigation activities where there is significant risk, and this may result in temporary outages or interruptions.

Training

The continuous improvement of incident handling processes implies that those processes are periodically reviewed, exercised and evaluated for process improvement.

Incident Response Phases

The Incident Response process encompasses six phases including preparation, detection, containment, investigation, remediation and recovery. In the execution of responding to an incident, the Incident Response Team will focus on the detection, containment, investigation, remediation and recovery of the specific incident.

Preparation

Preparation for incident response includes those activities that enable the organization to respond to an incident and include the creation and review of policies, standards and guidelines supporting incident response; security and technology related tools; effective communication plans and governance. Preparation also implies that the organizations across the Kirloskar Group / Kirloskar Pneumatic Company Limited have implemented the controls necessary to enable the containment and investigation of an incident. As preparation happens outside the official incident process, process improvements from prior incidents should form the basis for continuous improvement at this stage.

Detection

Detection is the identification of an event or incident whether through automated means with security tools or notification by an inside or outside source about a suspected incident. This phase includes the declaration and initial classification of the event/incident.

Containment

Containment of an incident includes the identification of affected hosts or systems and their isolation or mitigation of the immediate threat. Communication with affected parties is established at this phase of incident response.

Investigation

Investigation is the phase where ISO/ITS personnel determine the priority, scope, risk and root cause of the incident.

Remediation

Remediation includes the repair of affected systems and services, addressing residual attack vectors against other systems, communication and instructions to affected parties and an analysis that confirms the threat has been contained.

If the CISO or Privacy Officer reasonably believes that an exposure of regulated data may have occurred, the CISO or Privacy Officer will contact the Office of theKirloskar leadership team to provide situational information in determining a proper response at this stage.

Apart from any formal reports, the after-action analysis will be completed at this stage.

Recovery

Recovery is the analysis of the incident for possible procedural and policy implications. Recovery also includes the incorporation of any “lessons-learned” from the handling of the incident into future exercises and/or training initiatives.

Appendix A – Executive Response Team

The Executive Response Team is responsible for actions such as communication, information sharing, and minimizing impact from an exposure of regulated data. As Kirloskar Group / Kirloskar Pneumatic Company Limited responses to each incident may vary, this section provides an overview of those actions that the Executive Response Team may take in responding to an incident in which regulatory data has been exposed.

1. Once it is determined that enough information about the situation and the extent of the exposure has been collected, the Privacy Officer and CISO will collaborate with the Office of theKirloskar leadership team to determine if the incident rises to the level of a security breach. In the event that this is determined, appropriate members of the ERT should work together to determine what, if any, level of notification is required, how individuals impacted by the exposure should be notified and what, if any, services should be offered to the individuals impacted by the data exposure to help protect themselves from potential or actual identity theft. As part of this analysis, If it is determined that notification and credit monitoring protection is appropriate and/or required, the Privacy Officer and Procurement may engage the Kirloskar Group / Kirloskar Pneumatic Company Limited's designated vendor to provide notification and credit monitoring services on the Kirloskar Group / Kirloskar Pneumatic Company Limited's behalf. When applicable, the Kirloskar Group / Kirloskar Pneumatic Company Limited may engage with our cyber-liability insurance carrier for assistance. Unless an exception is determined to be appropriate by the ERT, the office or department responsible for the data that was lost or exposed shall be responsible for the costs associated with remediating the exposure, including but not limited to notification and credit monitoring services.
2. Where necessary or appropriate, the ERT will expeditiously collaborate to develop press releases, letters to affected individuals. Where appropriate, the CISO will coordinate with Kirloskar Group / Kirloskar Pneumatic Company Limited Communication to create web page(s) with information regarding the exposure and how individuals can take steps to protect themselves.
3. The ERT will also designate a single point of contact to address questions/concerns of individuals concerned about the exposure. The ERT may decide to set up a special toll-free phone number line for individuals to call with questions/concerns or to utilize services provided by our cyber-liability insurance carrier, when applicable. The Privacy Officer will ensure that appropriate offices (i.e., Kirloskar Group / Kirloskar Pneumatic Company Limited board, Kirloskar Group / Kirloskar Pneumatic Company Limited Communications, Office of the Promoters, office who lost or who is responsible for the data that has been compromised) are made aware of the single point of contact to whom questions/concerns should be directed.
4. In the course of managing and remediating the exposure, as expeditiously as possible:
    1. The Privacy Officer will work with Purchasing and the department responsible for the costs of remediating the exposure to process necessary paperwork to engage

the Kirloskar Group / Kirloskar Pneumatic Company Limited's designated vendor to provide notification and/or credit monitoring services.

2. The Privacy Officer will work with the vendor to process any appropriate paperwork (i.e., SOW, PO, etc.) to engage the vendor's services.
3. The Privacy Officer will work with appropriate Kirloskar Group / Kirloskar Pneumatic Company Limited staff, the board member and the vendor to draft notification letters, and where appropriate, FAQ's regarding the incident.
4. The Privacy Officer and/or CISO will work with appropriate Kirloskar Group / Kirloskar Pneumatic Company Limited staff to collect the names and last known addresses of individual who will need to be notified.
5. Notification letters will be sent to impacted individuals or organizations by First Class Mail, email and/or other methods required by law.
6. Press releases will be finalized and issued by Kirloskar Group / Kirloskar Pneumatic Company Limited Communications where appropriate. The main Kirloskar Group / Kirloskar Pneumatic Company Limited website(s), faculty/staff webpage and/or student web page will include a link to the news release.
7. A special website, containing information regarding the exposure, how to get more information, and how to protect one's credit, may be posted as appropriate by Kirloskar Group / Kirloskar Pneumatic Company Limited Communications. A mechanism for logging calls and/or inquiries received, as well as responses and/or assistance given, shall be created and implemented.
8. Once proper notifications have been sent and posted and the matter has been contained and handled, debriefing meeting(s) should be held with all of the individuals involved in the incident investigation, management and remediation. Additional follow-up activities should occur as appropriate.

Appendix B – Guidelines for Incident Response

Each incident presents a unique set of challenges and problems. This section provides some common guidelines for preferred actions in these types of events. For any issues outside of these guidelines, the Chief Information Security Officer or Kirloskar leadership team should be consulted.

Incidents within Chain of Command

In incidents where a member of the incident response team, their leadership or the leadership of the Kirloskar Group / Kirloskar Pneumatic Company Limited is being investigated, appropriate resources will be selected to remove any conflicts of interest at the direction of or in conjunction with either Kirloskar leadership team or the Board of Directors.

Interactions with Law Enforcement

All communications with external law enforcement agencies are made after consulting with the Office of Kirloskar leadership team.

Communications Plans

All public communications about an incident or incident response to external parties outside of the Kirloskar Group / Kirloskar Pneumatic Company Limited are made in consultation with the Office of Kirloskar leadership team and Kirloskar Group / Kirloskar Pneumatic Company Limited Communications. Private communications with other affected or interested parties should contain the minimum information necessary as determined by the Incident Coordinator or Chief Information Security Officer.

Privacy

The Kirloskar Group / Kirloskar Pneumatic Company Limited respects the privacy of all individuals, and wherever possible the incident response process should be executed without knowledge of any individual identities until necessary.

Documentation, Tracking and Reporting

All incident response activities will be documented to include artifacts obtained during any investigation. As any incident could require proper documentation for law enforcement action, all actions should be documented, and data handled in an appropriate manner to provide a consistent chain of custody for the validity of the data gathered.

Escalation

At any time during the incident response process, the Incident Response Commander or the Chief Information Security Officer may be called upon to escalate any issue regarding the process or incident.

The Chief Information Security Officer in consultation with the Office of Kirloskar leadership team will determine if and when an incident should be escalated to external authorities.

Appendix C – Primary Types of Regulated Data

Personally Identifiable Information (PII)

PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Aadhar card number
- State-issued driver's license number
- PAN Card number
- Bank account number
- Medical and/or health insurance information

Protected Health Information (PHI)

PHI is identified as "individually identifiable health information" transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium by a Covered Entity. PHI is considered individually identifiable if it contains one or more of the following identifiers:

- Name
- Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89) Computer Security Incident Response Plan Page 5 of 11
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Bank Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints.
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic or code that could identify an individual