SAKSOFT

your digital transformation partner

Information Security and Systems Policy

DISCLAIMER

The contents of this document are subject to change from time to time. Although Saksoft uses its best endeavors to ensure the accuracy of the contents, we assume no responsibility for any inadvertent error or omission that may appear in this document.

Approval

Prepared By:					
	Name		Senthil Pandi		12-February-2019
	Title		Sr. IT Manager		
Approved By:					
	Name		Dhiraj Mangala		16-September-2024
	Title		Executive Vice President & CCO		

AMENDMENT HISTORY

Sl. No	Amended By	Amended Date	Version No	Description of the Change
1	Srinivasa Raghavan	15-July-2005	2.0	SysAdmin Organization Chart Updated.
2	Srinivasa Raghavan	23-August-2005	2.1	Password reset procedure updated.
3	Raghavan Srinivasan	16-September-2005	2.2	Update on physical security and key card access system.
4	Saravanan Kadirvelu	22-December-2005	2.3	Total review of the document to reflect the current IT Policy.
5	Saravanan Kadirvelu	10 - April-2006	2.4	Network diagram, organization chart and Document control.
6	Saravanan Kadirvelu	19 - July-2006	2.5	Update on SIRT flow, Network diagram, Data disposal process.
7	Saravanan Kadirvelu	26 - Oct 2006	2.6	Network diagram, Clean desk policy.
8	Saravanan Kadirvelu	11-Jan-2007	2.7	Password policy.
9	Saravanan Kadirvelu	27-Apr-2007	2.8	Software usage.
10	Saravanan Kadirvelu	26-September-2007	2.9	Total review of the document to reflect the current IT Policy.
11	Saravanan Kadirvelu	12-May-2008	3.0	Total review of the document to reflect the current IT Policy.
12	Saravanan Kadirvelu	22-August-2008	3.1	Internet usage and Web.
13	Saravanan Kadirvelu	25-November-2008	3.2	Updation of approval members, Backup.
14	Suyash Jain	24-March-2009	3.3	Sysadmin Admin Organization chart and Network Diagrams for CDC & NDC.
15	Suyash Jain	25-Sept-2009	3.4	Network Diagrams for CDC & NDC.
16	Kamal Sharma	14-Feb-2010	3.5	Sysadmin Organization Chart & Total review of the document reflect the current IT Policy.
17	Kamal Sharma	22-Jun-2010	3.6	Total review of the document to reflect the current IT Policy.
18	Sasi Krishnamoorthy	10-Nov-2010	3.7	Sysadmin Organization Chart & Total review of the document reflects the current IT Policy.
19	Sasi Krishnamoorthy	25-Feb-2011	3.8	Total review of the document to reflect the current IT Policy.
20	Senthil Pandi	15-Sep-2011	3.9	Network Diagram for CDC & NDC & Total review of the document to reflect the current IT Policy.
21	Senthil Pandi	12-Jan-2012	4.0	Sysadmin Organization Chart & IT Support Ticker Process Flow chart.
22	Senthil Pandi	1-May-2012	4.1	Total review of the document and reflect the current IT Policy.
23	Senthil Pandi	24-Apr-2013	4.2	Updated Sysadmin Organization Chart.
24	Senthil Pandi	07-Jan-2014	4.3	Updated Sysadmin Organization Chart.
25	Senthil Pandi	03-Sep-2014	4.4	Updated Sysadmin Organization Chart.
26	Senthil Pandi	18-Dec-2014	4.5	Updated NDC network diagram.

27	Senthil Pandi	14-Sep-2015	4.6	Updated NDC - TU Network Diagram
28	Senthil Pandi	26-Dec-2015	4.7	Saksoft new logo updated.
29	Senthil Pandi	21-Sep-2016	4.8	Updated NDC - Network Diagram
30	Senthil Pandi	03-April-2017	4.9	Updated NDC Network Topology Diagram
31	Senthil Pandi	21-August-2017	5.0	Updated Sysadmin Organization Chart
32	Senthil Pandi	08-February-2018	5.1	Updated CDC Network Topology Diagram
33	Senthil Pandi	12-September-2018	5.2	Updated Sysadmin Organization Chart
34	Senthil Pandi	26-December-2018	5.3	Updates in information classifications, Information Security (IS) function roles, Updated Sysadmin organization chart include IS function.
35	Senthil Pandi	14-February-2019	6.0	Updates in Change Management, Incident Management and response sections.
36	Senthil Pandi	20-February-2019	6.1	Updated Sysadmin Organization Chart
36	Senthil Pandi	05-September-2019	6.2	Updated Sysadmin Organization Chart
37	Senthil Pandi	22-April-2020	6.3	Reviewed the entire policy and updated designation changes.
38	Senthil Pandi	15-October-2020	6.4	Updated CDC Network Topology Diagram
39	Senthil Pandi	28-April-2021	6.5	Updated designation changes and Organization Chart.
40	Senthil Pandi	15-December-2021	6.6	Updated Anti-virus / Anti-malware policy, Organization Chart and CDC Network Topology Diagram.
41	Senthil Pandi	02-May-2022	6.7	Updated Organization Chart.
42	Senthil Pandi	05-September-2022	6.8	Updated Organization Chart.
43	Senthil Pandi	31-January-2023	6.9	Cortex XDR and RSA SecureID details are updated.
44	Senthil Pandi	28-July-2023	7.0	Reviewed the entire policy.
45	Senthil Pandi	17-Jan-2024	7.1	Updated Network Topology, Patch Management and Cortex XDR Host Insight details.
46	Senthil Pandi	13-Sep-2024	7.2	Updated Organization Chart.

TABLE OF CONTENT

1. DOCUMENT CONTROL

DOCUMENT INFORMATION:

Document Name:	Information Security Policy
Document Version no:	7.2
Version date:	13-September-2024
Distribution:	All Saksoft Employees
Next Review Date:	September-2025

2. AUTHORIZATION

Name	Designation
Senthil Pandi	Sr. IT Manager
Dhiraj Mangala	Executive Vice President & CCO

3. Information Security Policy Statement

The purpose of the policy is to protect the information systems of Saksoft Limited from all threats.

Saksoft is committed to secure all information systems by maintaining data integrity, confidentiality and ensuring availability of information to only authorized users. This will focus on business continuity and to achieve business goals effectively and efficiently.

It is the policy of Saksoft to ensure that:

- Information will be protected against unauthorized access at all times.
- Confidentiality of the information will be assured.
- Integrity and safety of information will be maintained.
- Information Security training will be provided to all staff
- Employees to read and acknowledge the Information Security Policy document and code of conduct document during HR onboarding and on an annual basis thereafter.
- All breaches of Information Security will be reported and investigated.
- Business requirements for the availability of information and information assets will be met.
- Use of only approved / authorized / licensed software.
- Use of information only by authorized person(s) on a need to know basis.

4. Introduction

This policy document has been developed to protect all Information systems within Saksoft to an adequate level, from events that may affect and jeopardies the IT Infrastructure.

4.1. Need for Security Policy

Saksoft understands that a secure environment requires a systematic co-coordinated approach. An organization must first identify and assess its risk environment, then develop its security plan. To be effective, planning for the management of security risks should become part of an organization's culture.

The function of any information security control mechanism (technical or procedural) is to restrict the risk to an acceptable level. Policies are a risk-control mechanism and must therefore be designed and developed in response to real and specific risks.

Saksoft believes that security should be integrated into the organization's philosophy, practices and plans. It should not be treated as a separate activity. All employees should be encouraged to recognize that risk management and good security practices are a fundamental part of management.

Security policies are intended to supplement, not replace all existing laws, regulations, agreements, and contracts that currently apply to Saksoft computing and networking services. Persons given access to the Saksoft technology and information systems have signed a statement that they have read, understood and agree to abide by this policy.

Employees reasonably believed by the Company to have willfully compromised its information security will be subject to termination.

4.2 Who is affected by the policy

The Policy applies to all employees and subcontractors of Saksoft.

4.3 Where the policy applies

This policy applies to all development centers of Saksoft. The organization must confirm the security policies they operate and meet the security requirements or the risk is understood and mitigated.

5. Objectives

The objective of this document is to promulgate and implement a security policy that ensures business continuity of Saksoft to minimise damage to information systems due to security incidents against all internal, external, deliberate and accidental threats out of Saksoft's approach to commitment and security.

The policy objectives are to:

- Protect the organization's business information and any client or customer information within its custody by safekeeping or safeguarding its confidentiality, integrity and availability.
- Security measures for information systems.
- Establish safeguards to protect the organization's information resources from misuse and any form of damage.
- Meet the organization's operational purpose.
- Establish responsibility and accountability for Information Security in the organization.
- Be practical and useable while providing adequate security.
- Provide general guidance on security roles and responsibilities.
- Clear definitions of responsibility for the protection of classified material, whether electronic or hard copy.
- Clear definitions of security processes.
- Where necessary, more detailed guidance for specific systems or services.
- User awareness and education.
- Encourage management and staff by awareness and training to maintain an appropriate level of alertness, knowledge and skill to allow them to minimize the occurrence and severity of Information Security incidents.
- Provide suitable coverage of International Standards like ISO 27001.

6. Physical Security

Saksoft physical security compliance shall involve the following.

6.1. Monitoring the personnel movement

Employees should wear identification badges at all times inside the Saksoft building.

Visitors should sign in and wear temporary badges that identify them as visitors and will be escorted by authorized security personnel through the facilities.

The authorized security personnel will escort contractors and vendors who are allowed for short-term purposes to the facilities and are given temporary badges appropriate for their assignments. If badges are not used, they do not gain entry.

When individuals change responsibilities or terminated, their user ids and access cards will be deactivated.

CCTV has been installed to monitor physical movement at specific locations and is monitored 24x7 basis. The video from CCTV is recorded and stored for 90 days.

The security guards are placed to monitor the access to the building on 24x7 basis.

6.2. Physical Security

Saksoft premises have restricted access for all the personnel through the use of access cards, whose issuance or modification shall be a controlled, monitored process and would be subject to respective approvals. Saksoft shall maintain regular backup of access cards logs.

The following computer environmental controls have been installed:

- Fire suppression equipment and extinguishers
- Uninterruptible power supply (UPS)
- Emergency Power System (EPS) (e.g., generators)
- Temperature and humidity controllers
- Emergency power cut-off switches
- Emergency lighting

The building fire suppression system has been certified and reviewed periodically.

The data center, production operations center or equivalent areas shall be fully secured to ensure restricted access. All entry and exit to the data center shall be restricted by access card system, which shall have the entry / exit time.

The data center access logs shall be subjected to a monthly review signed by the administration team.

The access privileges to data center shall warrant the approvals from IT Manager or above for the respective data center.

6.3. Access Card

Employee shall sign a requisition form and submit the same to administration team to obtain the access cards. Administration team shall maintain the records of access cards issued, revoked and logs pertaining to successful entry and exit timings. The administration department does periodic review and audit of logs.

Saksoft will ensure only authorized persons are allowed to access the Saksoft work areas using access cards. Access Card issuance or modification shall be a controlled, monitored and would be subject to approval.

The data center hosting the router or other network devices is fully secured and the access card ensures restricted access. All entry and exit to the data center shall be logged and reviewed periodically, which shall have the entry/exit time for the authorized personnel.

The physical access into the data center is limited to those individuals whose primary business functions require them to have access.

The System Admin representative will escort contractors/vendors who are allowed for short-term purposes to the data center.

The authorization procedure for entry into the data center exists and applies to all Saksoft employees.

7. CLEAN DESK POLICY

Saksoft practices “Clean Desk Policy” in relation to confidential information. All documents marked as confidential shall always be stored in central servers with strict access control procedures.

Employees are required to lock the workstations when they are away from their desk.

The process for the disposal of confidential information stored on paper shall be through paper shredder only. No offsite paper destruction shall be performed.

All staff members shall be trained and encouraged to leave their desks "neat and tidy".

Administration staff will inspect desks in all areas periodically on a pre-defined interval as well as on a random basis. The administration department will use a clean desk checklist for this purpose. A log of the checks and findings will be maintained and will be submitted to senior management on periodic basis. Any lapses will be escalated to senior management promptly and action will be taken to rectify the same.

It is the responsibility of all employees to ensure that the following is adhered to:

- Sensitive and confidential papers, media and other assets should be locked in cabinets when not in use.
- Sensitive information, laptops and other valuable items should be locked away when not in use.
- Personal Computers and computer terminals should be protected by authentication codes.
- Personal Computer should be shut down when individuals are away from the work area for an extended period of time.
- In the event of the computer not being operated for certain period, a timeout period has been configured to lock the computer.
- Software CDs and installation manuals should be stored securely to help protect the Saksoft licensing rights.

8. System Management

Saksoft has well-established standards for the base configuration of internal server / workstation. Effective implementation of this policy will minimize unauthorized access to proprietary information and technology.

8.1. Systems / Windows

- Employees shifting from one team to another team – request has to be initiated by the respective project manager by duly placing change request in IT Tech support system.

- Users will only be given sufficient rights to all systems to enable them to perform their job function. However, user rights will be kept to minimum at all times. An annual review of the user accounts and access privileges will be performed.

- IT Team Support team will ensure regular security patching and vulnerability fixes on all the relevant IT infrastructure.

- IT Tech support team will check the latest patches on a weekly basis on WSUS server, analyze its applicability and deploy the same in a test server/desktop. After successful testing the same will get applied on respective servers and workstations.IT Support Team will control network / server passwords and system passwords.

- Access to the network/servers and systems will be by individual username and password.

- Administrator account in Domain Controllers should be renamed.

- Passwords will expire every 30 days and must be unique. When prompted or when necessary users will change their domain password accordingly. A password should have at least 3 combination characters from alphanumeric characters, lowercase, uppercase and numerical/symbol in the password. Last 10 passwords cannot be used when changing the password.

- The user account will be locked after 3 incorrect attempts. The account has to be manually unlocked by the IT Support team after the identification of the user.

- All central system password (like domain controller, Router, Mail server etc.,) would be changed one day prior to an employee leaving IT Support team or the organization and the same will be verified the next day.

- All central system passwords would be hand written and stored securely in a sealed envelope and given to Senior Management.

- Users will be given a username and password to login to the Saksoft Network. When an employee leaves, his/her account will be disabled immediately and will be deleted after 2 months.

- Auditing will be implemented on all systems to record login attempts/failures, successful logins and changes made to all systems.

- Default username and password created by the software at the time of installation will be changed after installation.

- File systems will have the maximum security implemented that is possible. Where possible users will be given Read-Only rights to directories, files will be flagged as read only to prevent accidental deletion.

- Appropriate encryption control measures are implemented to protect information system resources against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of such information system resources.

- Standard cryptography mechanisms are followed to protect confidential information like encrypting the relevant data during transmission using portable media, secure layer certificate implementation for URLs etc.

- We have deployed RSA SecureID for Windows Servers. RSA SecurID Access provides a solution for maintaining a consistent multi-factor authentication.

8.2. Anti-Virus / Anti-Malware Protection

Saksoft has ensured that all available measures have been taken to prevent Saksoft's Network from being exposed to possible attack from cyber threats. Management strongly endorses the Company's endpoint security policies and will make the necessary resources available to implement them.

Palo Alto Cortex XDR is the industry's first extended detection and response platform that stops modern attacks by integrating data from any source. With Cortex XDR, we can harness the power of AI, analytics, and rich data to detect stealthy threats. Our SOC team can cut through the noise and focus on what matters most with intelligent alert grouping and incident scoring. Cross-data insights accelerate investigations so that we can streamline incident response and recovery.

The Cortex XDR agent offers a complete prevention stack with cutting-edge protection for exploits, malware, ransomware, and fileless attacks. It includes the broadest set of exploit protection modules available to block the exploits that lead to malware infections. Every file is examined by an adaptive AI-driven local analysis engine that's always learning to counter new attack techniques. A Behavioral Threat Protection engine examines the behavior of multiple related processes to uncover attacks as they occur.

Safeguarding endpoints starts with getting a clear picture of all the endpoint settings and contents to understand the risk. Once identified a threat, need to stop it quickly and ensure it hasn't spread to multiple endpoints. With Host Insights, an add-on module for Cortex XDR™, get all these capabilities and more. Host Insights combines Vulnerability Management, Host Inventory, and a powerful Search and Destroy feature to help you identify and contain threats. Host Insights offers a holistic approach to endpoint visibility and attack containment, helping reduce exposure to threats so you can avoid future breaches.

Cortex XDR centralized cloud monitoring console is Manage Detection and Response (MDR) team by Security Operation Centers (SoC).

- 24x7 monitoring as events/incidents happen
- Review of all detections in Cortex XDR and Deep Visibility on metadata
- Important notifications will be sent to IT Security Team for follow-up
- Emergency communications will be notified to IT security team and Senior Management team.

Any machine brought in for demonstration by the vendor/customer will not be connected to the network.

New commercial software will be scanned before it is installed.

The IT Support Team takes the backups for all critical servers on a daily basis and review by restoring backup of any tape every Monday.

Users will be kept informed of current procedures and policies.

Employees will be held accountable for any breaches of the Company's cyber threats policies and suitable disciplinary action as deemed fit would be initiated.

8.3. Monitoring

All Internet and Email usage and/ or content should be monitored and / or logged.

Suspected inappropriate use of services and/ or security violations should be investigated.

8.4. Data disposal

- Saksoft outlines the following methods to expunge data from storage media / removable media (like CD, DVD, etc.). Removal of data must be performed on hard drives to ensure that information is removed from the hard drive in a manner that gives assurance that the information cannot be recovered. Before the removal process begins, the computer must be disconnected from any network to prevent accidental damage to the network operating system or other files on the network.

- There are two acceptable methods to be used for the hard drives:

  - **Formatting** - formatting the hard disk is carried out while moving hard disks from one development project to other and it is always at the low level. This is used when the hard drives or PC the hard drive is given to other project teams / departments.

  - **Overwriting** – Overwriting is an approved method for removal of data from hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. This is also used when the hard drives or PC with the hard drive is given to other project teams / departments.

- **Physical Destruction** – Digital storage devices, which contain licensed/unlicensed software programs and data, must be reliably erased and should be physically removed. Physical destruction must be accomplished to an extent that preludes any possible further use of the equipment.

8.5. Disposal of computers and other digital storage media

The policy for disposal of equipment is as follows:

All data contained on computers and storage media are subject to Saksoft Policy on Document Retention and needs to be archived for appropriate period of time.

All surplus / old computers and any associated storage devices are to be sent IT services department.

All removable storage media (e.g. CDs, DVDs,) no longer required by a department's retentions policy are to be destroyed. Bulky removable storage media may be sent to IT services department for disposal.

Any computer not meeting the minimum computer standard will be put into storage to be destroyed.

Refer Media Disposal and Data Destruction Policy Annexure 1 for detailed steps and procedures.

Sanitizing Hard Drives and Backup Tapes

Specialized software is available to sanitize a hard drive before it is disposed or repurposed. This software makes several passes over the entire surface area of every platter of the hard drive.

Magnetic tapes be erased using a degaussing device which randomizes the magnetic pattern on the media rendering it unreadable.

Destroying Storage Media

Some media cannot be sanitized. For instance, a CD-R and DVD-R permanently retain the data initially written to the disc. Physical destruction is the only solution. For CD-R and DVD-R discs and other optical media.

8.6 Software Usage

- Software that is installed and used should be related to accomplishing a user’s daily tasks as it relates to his or her job description. Installing software for personal or entertainment use is prohibited.
- Software that is installed and used for personal profit or other related activities are strictly prohibited.
- User installation of any operating system (e.g. Windows, Linux etc.) is strictly prohibited.
- Usage of Freeware/Shareware/trial version software’s at all times is strictly prohibited as it comes under the copyright protection. Any deviation has to be approved by the senior management.
- Users cannot install and use any software without prior approval.
- Unauthorized copying, use of unauthorized copies, distributing, or use of Saksoft’s software is strictly prohibited.
- Persons engaging in violation of above activity will be subject to severe disciplinary action as given in section 20 of this document.

9. Network Security

9.1. Network

LAN equipment, switches and routers will be kept in secure server rooms which are locked at all times and accessible by authorized personnel only. Saksoft staff and contractors requiring access to server rooms will notify IT TechSupport Team staff in advance so that the necessary approval from Project Director, IT Manger or above can be arranged.

Wireless LAN

Wireless LAN deployed in Saksoft Network only for Laptop users. Wifi connection protected and uses strong encryption and authentication. Wifi password will not be sharing any of the employees apart from prior approval from respective manager.

9.2. Network Cabling

- All network wiring will be fully documented.
- All unused network points will be de-activated when not in use.
- Users must not place or store any item on top of network cabling.
- Redundant cabling schemes will be used where possible.

9.3. Servers

All common (like DC, File Servers etc.) servers will be kept securely in the data center.

Access to the system console and server disk/tape drives will be restricted to authorized IT TechSupport Team staff only.

9.4. Electrical Security

All servers, network equipments and desktops will be fitted with UPS that also condition the power supply.

In the event of a mains power failure, the UPS will have sufficient power to keep the network and servers running until the generator takes over.

All UPS will be tested periodically.

9.5. Inventory Management

IT TechSupport Team will co-ordinate with Admin for Software license while the admin department will keep track of hardware inventory and send a report to the system admin team.

Computer hardware and software audits will be carried out periodically. These audits will be used to track unauthorized copies of software and unauthorized changes to hardware and software configurations.

10. Firewall & Internet Access Control

Firewall Security policy enforcement will emphasize the use of security technology mechanisms to mitigate security risks wherever possible within Saksoft network.

10.1. Perimeter Security Maintenance

Perimeter security for Saksoft Intranet and Extranet will be provided through firewall. The firewall will inspect packets and sessions to determine if they should be transmitted or dropped. In effect, the firewall will act as a single point of network access where traffic can be analyzed and controlled.

Access to the Saksoft internal network will be based on parameters such as (but not limited to):

- Application use.
- User authentication, authorization, and accounting for both incoming traffic from remote users and outgoing traffic to the Internet.
- IP Address and port.

10.2. Firewall Logon Access

Only the IT TechSupport team has rights to logon to firewall. Passwords are constructed based on password policy of Saksoft.

10.3. Firewall Operational Maintenance and Responsibility

The IT TechSupport team will:

- Be responsible for the administration, maintenance and configuration changes in the Firewall that require approval from the IT Manager.
- Be responsible for framing and to making changes in the IS policy and procedures for operational continuity.
- Act as Saksoft technical lead for internal security policy and procedure implementation, have the primary responsibility for ensuring operational continuity for the System administration team security policy.
- Perform firewall rule set changes, addition and deletions as approved by the IT Manager.
- Perform firewall software maintenance and hardware upgrades to the firewall; implement feature set on firewall as approved by the IT Manager.
- Monitor firewall logs, and Intrusion Prevention system on weekly basis.
- Initiate Saksoft's response to any possible security incident.

- Perform security risk management by initiating a cycle of securing, monitoring, and testing security mechanisms and procedures. Review findings will be used to update security policy, procedures, and security mechanisms on a continual basis.

- Firewall changes shall be done by IT TechSupport that requires approval from the IT Manager.

10.4. Firewall Log Configuration and Maintenance

The firewall logs will be stored in Checkpoint Security Management Console. The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartEvent consolidates and shows all security events that are generated by these Software Blades:

- Firewall
- Identity Awareness, and URL Filtering
- IPS
- Application Control
- Anti-Bot, Threat Emulation, and Anti -Virus

IT Tech Support Team can quickly identify very important security events and do the necessary actions to prevent more attacks.

10.5. Firewall Security Services

At a minimum, the firewall will perform the following security services:

- Access control between the internal network and un-trusted networks.

- Block unwanted traffic, as determined by firewall rule sets designed to implement the Saksoft Security Policy while providing security that does not place an undue burden on authorized users.

- Hide system names, network topology, network device types, and internal user ID's from the Internet.

10.6. Firewall Rule Set Management and Change Control Process

The IT Manager must approve all rule set (ACL’s) changes, IOS changes and upgrades. At a minimum, the following information will be included in any firewall change request.

- Requesters Name and Project information.

- Requested Due Date (when change will be applied).

- Change impact statement. Include any supporting documentation necessary to determine why the change is necessary. The change request will be delayed until change requirement has been established and approved.

- Rule Change Notification requirements (who need to be alerted about the change because of potential operational impact).

Change Priority Level

Emergency change needs will be executed immediately because of possible security breach

Change will be applied as scheduled, upon approval from the IT Manager.

Firewall rule sets (ACL's) will work to achieve a "best practices" approach in an effort to balance security risk and operational access requirements. Best practices include:

- All access to the firewall itself is blocked from the Internet.
- Allow outbound Internet access only from the Proxy server.
- ICMP services turned off.

10.7. Network Connection Policy

Only network connections that have been found to have acceptable security controls and procedures will be allowed to connect to the Saksoft network. Every attempt will be made to ensure that all external connections will pass through firewalls that meet the guidelines established by this policy. All connections and accounts related to external network connections shall be validated on an annual basis. When a network connection is no longer needed all accounts and system processes related to the connection should be deleted within one week.

10.8. Trusted Networks Policy - Network Trust Relationships Overview

Approved and authorized network connections are considered trusted networks. Trusted networks share the similar security policy or implement security controls and procedures.

Un-trusted networks do not implement common security controls, or where the level of security is unknown or unpredictable. Network segments external to Saksoft are under the control of different organizational entities, and will be considered as un-trusted networks.

The following networks are considered trusted networks and permitted controlled access by the firewall.

- VPN link between Chennai Development Center and Noida Development Center.
- Site-to-Site VPN between Chennai and Acuma Solutions, UK
- Site-to-Site VPN between Noida and Acuma solutions UK.

10.9. Non-trusted Networks Policy

All networks not specifically listed as a trusted network are non-trusted networks. Access to the Saksoft network will be denied by the firewall. If complete access control cannot be managed by the firewall, other security technologies will be used in tandem to the Saksoft firewalls to mitigate the security threat. Modem connections with business partners and/or remote sites are also considered un-trusted networks connections. The IT Support Team may terminate unauthorized connections to Saksoft network without notice. An active network port or connection does not imply authorization for connectivity.   IT Tech Support team is responsible for Firewall monitoring.

10.10. **Periodic Review of Firewall Security Policies.**

Firewall security policies will be reviewed bi-annually. When there are major changes to the network requirements this may warrant changes to the firewall security policy.

Changes include events such as the implementation of major enterprise computing environment modifications and any occurrence of a major information security incident.

When new applications are being considered, the IT Manager of the respective development center will evaluate new services before the firewall administrators are formally notified to implement the service. Alternatively, when an application is phased out or up-graded, the firewall Rule set should be formally changed where appropriate.

Firewall installations will be audited on a regular, periodic basis. These periodic reviews can be conducted on paper by reviewing hard-copy configurations provided by appropriate systems administration staff. In other cases, periodic reviews should involve actual audits and vulnerability assessments of the firewall.

File downloading is blocked through proxy configuration rules in order to achieve maximum security.

11. System Admin Security Review Check List

System Admin checklist cover detailed procedure, which covers daily critical tasks and functions, which will ensure that all central servers, services, and network equipments are functioning smoothly.

11.1. Active Directory Domain Controllers

- Check if the primary domain controller and additional domain controller are up.
- In both the domain controllers check for disk space and to ensure that there has been no abnormal increase in disk space.
- Check current replication status between domain controllers in Chennai and Noida.
- Open the systems logs through event viewer and view the system logs. If the system log shows any error or warning, then the corresponding event id check with Microsoft site for explanation for the error message and apply the steps given form the site to clear the error.
- Check for any errors in active directory integrated DNS server through event viewer.
- Check for any unknown hosts connected through network.
- Check whether any unusual process is running.
- Diagnose any compromise of the server through Trojan or virus attack.
- Check system state backup has completed successfully and the logs shows backed up system state data has been verified successfully.
- Check for any unknown login account in the active directory, which might have been created by malicious, scripts executed by Trojans.
- Check RSA SecureID MFA is working to avoid any unauthorized access.

11.2. File Servers and Backup Devices

To check for free disk space in the centralized file storage servers:

- Check with users to clear any unwanted data and very old backed up data.
- Check for any modification in the access-list given to share permission of all shared folders.
- Check with event viewer for any hard disk physical error like bad sectors or unable to write to media error as these errors are common in machines used as file server and storage.
- Check anti-virus signature files are up-to-date.

- Check whether all folders have been properly organized internally and no files are lying on the root space of any hard disk partition.

11.3. Data Backup

- IT Support Team is responsible for providing system support and scheduling/running data backup tasks. Team ensures that adequate backup & system recovery practices, processes and procedures are followed in line with Saksoft Disaster Recovery Procedures.

- All IT backup and recovery procedures are regularly reviewed and made available to trained personnel who are responsible for performing data and IT system backup and recovery.

- All data, operating systems/domain infrastructure state data and supporting system configuration files are systematically backed up - including patches, fixes and updates which may be required in the event of system re-installation and/or configuration.

- Wherever applicable backup media (e.g. tape) is encrypted and appropriately labelled. Any system used to manage backed-up media should enable storage of date/s and codes/markings which enables easy identification of the original source of the data and type of backup used on the media. All encryption keys are kept securely at all times with clear procedures in place to ensure that backup media can be promptly decrypted in the event of a disaster.

- A record is e maintained for all backup information such as department, data location, date, type of backup (e.g. Incremental, Full etc…) including any failures or other issues relating to the backup task.

- Copies of backup media are removed from devices as soon as possible when a backup or restore has been completed.

- Backup media which is retained on-site prior to being removed for storage at a remote location must be stored securely in a locked safe and at a sufficient distance away from the original data to ensure both the original and backup copies are not compromised.

- Access to the on-site backup location and storage safe are restricted to authorized personnel only.

- All backups identified for long term storage are stored at a remote secure location (offsite) with appropriate environmental control and protection to ensure the integrity of all backup media.

- Regular tests are carried out to establish the effectiveness of the backup and restore procedures by restoring data/software from backup copies and analyzing the results. Any issues with the backup testing of data are escalated to the IT Manager.

- IT Tech Support team should maintain a record of job failures, with the re-running of any failed jobs logged in the backup software management console.

- Backup data/media no longer required are clearly marked and recorded for secure disposal.

- Key servers and file stores are backed up either daily or weekly (refer backup schedule) to prevent any data loss that may be due to user deletion, hardware failures, malware encryption attacks or any other event that may result in data loss. These will be backed up locally on the backup server.

- For the media taken out label it with the current day of the week, date and time. This media should be checked with Veeam backup logs whether the data has been written successfully.

- On every week beginning workday the media backed up on Friday / Saturday / Sunday will be handed over to CFO or his designate on a rotation basis for offsite storage and the previous week's media will be obtained from him.

- First day of the week we would restore the backup media from any randomly chosen tape to check for the integrity of the backed-up data. Once integrity of the data has been verified log the activity for successful completion of the task.

11.4. Patch Management

IT Tech Support team will ensure regular security patching and vulnerability fixes on all the relevant IT infrastructure.

ManageEngine Patch Manager Plus, is a comprehensive patch management solution that automates everything from scanning endpoints for missing patches, downloading these patches from vendor websites, and deploying these patches to generating reports of every step in this process. Accelerate the process of patching, and improve operational efficiency with Patch Manager Plus.

IT Tech support team will check the latest patches on Patch Manager Plus, analyze its applicability and deploy the same in a test server/desktop. After successful testing the same will get applied on respective servers.

Server software update will be manually installed at least monthly. However, any vulnerability patches, we will be installed immediately after testing is completed.

Workstations will be configured to install software updates every fortnight automatically.

Any exception will be documented.

11.5. Endpoint Protection

All Desktops, Laptops and Servers running Windows Operating System will be updated with the latest updates of Cortex XDR to protect from cyber-attack.

Host Insights, an add-on module for Cortex XDR. Host Insights combines Vulnerability Management, Host Inventory, and a powerful Search and Destroy feature to help you identify and contain threats. Host Insights offers a holistic approach to endpoint visibility and attack containment, helping reduce exposure to threats so you can avoid future breaches.

Cortex XDR centralized cloud monitoring console is managing by Security Operation Centers (SoC).

- 24x7 monitoring as events/incidents happen
- Review of all detections in Cortex XDR and Deep Visibility on metadata
- Important notifications will be sent to IT Security Team for follow-up
- Emergency communications will be notified to IT security team and Senior Management team.

11.6. Network

- Check all Ethernet switches in the server room are up.

- Ping the LAN interface IP address from any systems to check for LAN interface status.

- Browse any website to check whether Internet link is up.

- In the router check access-lists counters for traffic statistics.

- Check the MRTG graph traffic details for the previous day, and also check whether the traffic for the previous day is within our daily average traffic statistics, if the traffic shows abnormal increase, then check with intra-day statistics of the MRTG graph to find if there is increase in traffic during any particular time frame, if the graph shows constant increase in traffic from any particular time frame, then check for outage through router IP accounting tool.

- Check for syslog messages sent by router to syslog server and review the log thoroughly to cross verify if there is any particular host attempted to breach our network security.

- Ping Noida router to confirm Noida VPN link is up.

11.7. Separation of duties

The basic principle of separation of duties is that no individual person, role, or group, should be able to execute all parts of a transaction or process. In practice, separation of duties is a loss-control measure designed to reduce the risk of accidental or intentional damage to the integrity, confidentiality, and availability of a transaction or process.

- Software developers, contractors, and third-party vendors cannot access production systems, database management systems, or system-level technologies.
- End users cannot access or modify production data, except through an appropriate administrative application.
- Install only approved software and code on production systems.
- Only IT Techsupport can access system logs and system audits, which is monitored on a regular basis.
- Only IT Techsupport can access firewalls and network security systems, which is monitored on a regular basis.
- Only approved operators can make data backup tapes, with regular monitoring to ensure that appropriate compliance procedures were followed.
- Only IT Techsupport can create, update, or delete user accounts, which are independently monitored on a regular basis for excessive, unauthorized, or unused privileges.
- Monitor source code repositories for excessive use.
- Create two user accounts for System Administrators - one for routine activities such as email and one for activities requiring privileged user access and permissions.
- Use two-factor authentication for privileged users, to ensure the person is who he claims to be.
- Use network access controls to prevent VLANs from accessing production systems.
- Use role-based access to logging and audit records, to ensure that administrators can only see records for their networks or systems.
- Generic administrator accounts are disabled.

12. Incident Management and Response Process

It provides a mechanism to carry out the Incident Management Process in a structured and consistent manner in accordance with ITIL guidelines and Industrial Standard Practice. The goal of the IT Infra Security Incident Response Plan is to detect and react to IT Infra security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

Saksoft in conjunction with its Compliance, Information Security, Corporate Security and any other relevant security functions, shall document all security related incidents.

The Security Incident Response Process shall cover the following incidents:

- Misuse of systems ID's and passwords.
- Virus attacks & infections on network PC's.
- Malware, exploits and ransomware
- Evidence of tampering with data.
- Attempts at identity theft.
- Social engineering (e.g. calling IT Support Team and impersonating another individual to gain access or information).
- Misuse of privileged systems access by technology or support staff or outright cases of fraud.
- Misuse of unauthorized use of Saksoft resources. (Surfing of undesirable content, exchange of abusive contents on email etc.).
- Other incidents that could undermine confidence and trust.
- Attempts to bring personal devices in office premise (like-laptops, memory device, etc.).

Please refer Saksoft Incident Management Policy document for detailed procedures and processes.

12.1. Escalation Procedures

For post follow-up and escalation of security incident response, the internal escalation matrix is as follows.

First Level Contact – Respective Project Leader

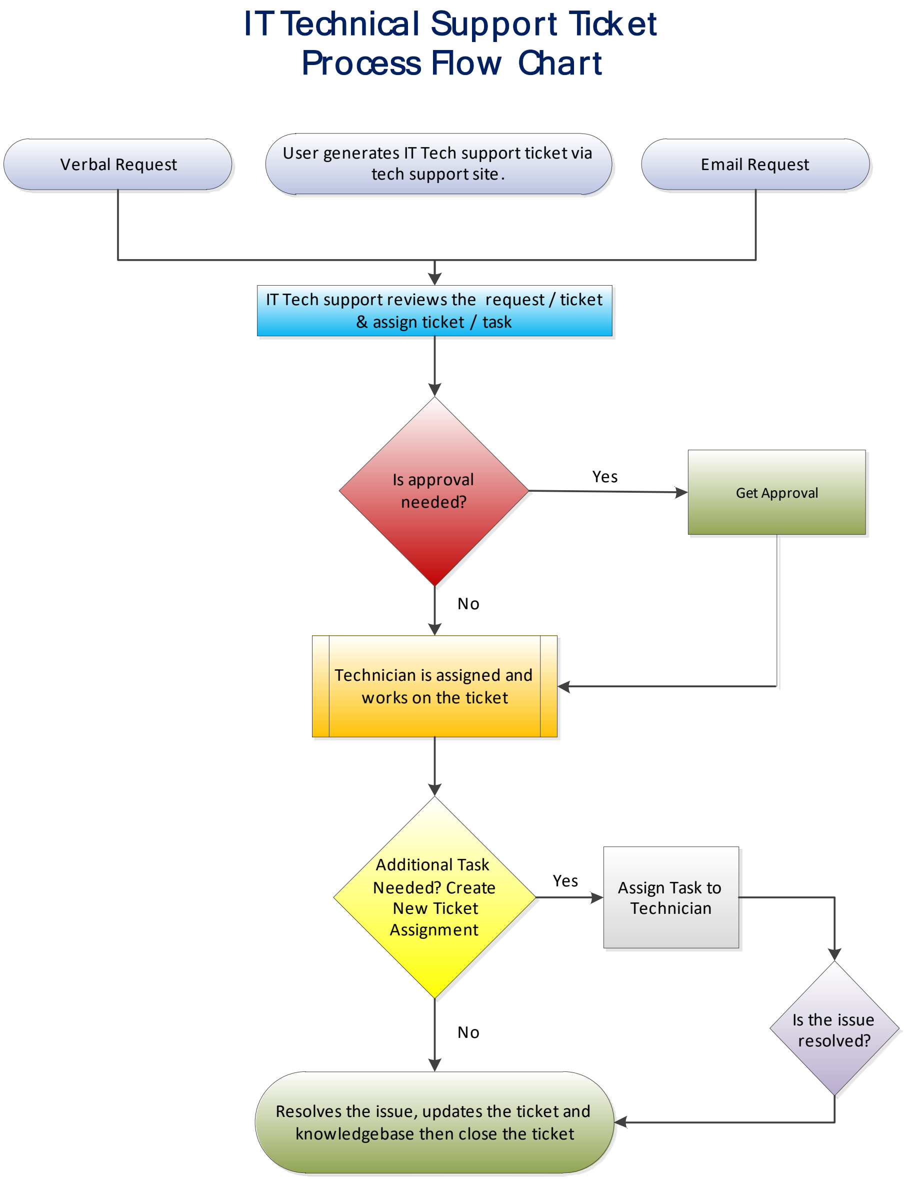
Second Level Contact – Project Manager

Third Level Contact – IT Manager / Delivery Manager

Fourth Level Contract – CEO / Executive Vice President (If the member is not satisfied with the follow-up action and incident handling, as well as to provide any additional information about the incident).

The external escalation procedures shall be in line with process guidelines as prescribed by Saksoft Business Partners.

12.2. Support Ticket low process


IT Technical Support Ticket
Process Flow Chart
Verbal Request
User generates IT Tech support ticket via tech support site.
Email Request
IT Tech support reviews the request / ticket & assign ticket / task
Is approval needed?
Yes
Get Approval
No
Technician is assigned and works on the ticket
Additional Task Needed? Create New Ticket Assignment
Yes
Assign Task to Technician
Is the issue resolved?
No
Resolves the issue, updates the ticket and knowledgebase then close the ticket

13. Document/Information Classification

Workers are expected to familiarize themselves with the Saksoft data/information classification system and to conduct their business activities in accordance with it.

Information created, stored or processed by Saksoft shall be classified by Workers (if they created the information), or Data Owners (for information systems or customer data) according to the following classification scheme:

- Public
- Internal
- Confidential
- Restricted

All Workers must consider information to be governed by the principle of "need-to-know." Unless a Worker has reason to access information in the performance of his or her defined job duties, access is denied.

Workers shall not disclose non-Public information to anyone who is not authorized to have it.

This includes disclosure through oral and written means, whether electronic or otherwise.

Any questions as to whether information is Public, Internal, Confidential or Restricted, should be presented to the classifying Worker, or the applicable Data Owner, for determination. In the event that the Worker or applicable Data Owner cannot be readily identified, direct all such questions to the Information Security team.

13.1. Public Information

Public information is information that is freely available to the general public, or whose release will not cause any harm to Saksoft.

Examples of Public information include marketing literature, annual reports, disclosures submitted by Saksoft Limited with the Stock Exchanges where the shares are listed and other information which are to be placed in the website of the Company which is open to general public and other materials specifically created by the marketing department for public release.

There are no special handling or disposal requirements for Public information and no special markings are required.

13.2. Internal Information

Internal is the default classification of data at Saksoft and includes all of Saksoft's internal business correspondence, records, and data created in the normal course of business which is not otherwise classified as Confidential or Restricted. This includes all business email as well as all correspondences with clients. All non-marked material, which is not

Restricted or Confidential Information, must be treated as Internal (i.e., not released to outside parties or maintained on a need-to-know basis) until it is confirmed as Public information.
There are no special markings required for printed or electronic internal information. Printed Internal information must be destroyed using the secure document disposal facilities provided at Saksoft business locations, or it can be shredded.

13.3. **Confidential Information**

Confidential information includes all of Saksoft's business, financial and technical information including, without limitation, customer, product, pricing and product development plans, network and system diagrams or other non-restricted information, records or data created in the normal course of business which if made public would cause harm to Saksoft.

Categories of Confidential Information

Employee Data

Name, DOB, Gender, Marital Status, Health Records, Bank Account Details, Previous Employment Details, Background Verification Details, Academic and Professional Qualifications, Awards, Rewards

Client /Vendor Data

Data, Reports, Intellectual Property Rights, and Confidential Information of the Client / Vendor stored accessed by the employees of Saksoft in the course of his employment.

Confidential information also includes information not otherwise classified as Restricted and which is obtained by Saksoft or to which Saksoft otherwise had access to, under obligations of confidentiality to a third party, whether under a confidentiality agreement, non-disclosure agreement, or other agreement.

If information is Confidential, it must be marked "Saksoft Confidential" before being distributed or exposed to a non-Saksoft party, regardless of distribution method (e.g., written form, email, via facsimile, etc.) and then only under a Saksoft approved non-disclosure or similar agreement. Confidential information concerning Saksoft networks or systems must be approved for release by the Information Security / Compliance team or the appropriate business unit prior to distribution to non-Saksoft 3rd parties. Confidential information must be destroyed using the secure document disposal facilities provided at Saksoft business locations, or, if on paper, DVD or CD media it can be cross-shredded. Confidential information contained or stored in other media must be disposed of in accordance with the instructions of the Information Security Team.

13.4. Restricted / Unpublished Price Sensitive Information

All information/ data classified as Unpublished Price Sensitive Data as defined under Code of Practices and procedures for fair disclosure of unpublished price sensitive information of Saksoft Limited. Examples are Financial Results, Dividend, Mergers/ Demergers, Change in Capital Structure, Change in the Key Managerial Personnel of the Company, etc.

Restricted information includes all information subject to restriction in access, storage or processing by law, or regulation, or by customer contract and any Saksoft owned information that could cause significant harm, to Saksoft, if inappropriately disclosed, accessed or modified. This information includes, but is not limited to, all non-public personally identifiable information (for example, names, addresses, social security numbers (or equivalent in each country), consumer credit information, full credit card number and protected health information), data that we receive, create, store or process for consumers and our customers, as well as Saksoft information such as intellectual property, board minutes, business plans, sensitive employee information, etc.

Access to Restricted Information is controlled by the designated Data Owner for the information. For customer data, the Data Owner is, by default, the senior manager responsible for the business unit receiving, creating, processing, or storing the data. For Restricted Saksoft Information, the Data Owner is the senior business unit manager/executive responsible for creating or using the information. The Data Owner is responsible for ensuring that access to the information is restricted to those who have a legitimate business need for the access and that the access, storage and processing is in keeping with customer contractual, legal (e.g., regulatory) and/or business restrictions.

Restricted information should be encrypted in storage, or otherwise maintained in accordance with Information Security policies where encryption is not practicable, and shall be encrypted during transmission to/from the Saksoft network, including when shipped manually or being sent by email. Depending on contractual or legal requirements, encryption may be mandatory. Non-electronic, Restricted Information being transported must be shipped using Information Security Team approved shipping method.

Restricted Information must not be distributed to, nor can access be provided to, anyone who does not have a specific business reason to receive or access it – Data owners (or their delegates) must approve all access to Restricted Information. Restricted information must be stored on Saksoft servers in Saksoft Data Centers and accessed remotely as needed. Storage on any other device requires: (a) approval from the Data Owner, Business Unit Manager and Information Security Team ; and (b) the use of encryption using Information Security team approved method.

Printed Restricted information must be destroyed using the Saksoft approved secure document disposal facilities provided at Saksoft business locations or by other Information Security team approved means of shredding, erasing or otherwise making the information unreadable or undecipherable. Restricted information stored electronically must be securely disposed of when no longer needed in accordance with information disposal standards.

All customer data (records, tapes, data transmissions, etc.) that Saksoft stores, processes or manages shall be considered Restricted unless otherwise designated by the customer or Information Security. Customer communications and correspondence shall be considered Confidential unless otherwise defined by contract or law. If a system contains data in more than one of the classifications, it shall be treated according to the classification needed for the most sensitive data on the system (for example, Confidential information mixed with Restricted information shall be treated as if all such information was Restricted).

13.5. Information labeling scheme

All Confidential, Sensitive / Business critical information that is backed up on tape devices will be labeled with a naming convention as applicable. This will enhance the inventory control system and also have better control over accidental file deletion / modification/ misuse.

14. Social Engineering Awareness

Social engineering, the process of deceiving people into giving away access or confidential information, is a formidable threat to most secured networks. The threat is considered very real. Saksoft corporate training plan includes guidelines for employees to understand and resist social engineering incidents. Saksoft employs multi-level defensive strategy for hardening employees to social engineering threats.

Pre-employment screening

All employees are trained to be aware of the basic signs present in a social engineering attack.

As part of training employees are trained to utilize resistance-training techniques to be adequately prepared to resist any persuasion techniques of a social engineer.

Understanding the psychological triggers behind social engineering incidents

Regular reminders through the internal communication process are undertaken to ensure that awareness is given to any new methodologies by which Social Engineering events are bound to happen and the associate risk involved.

Employees are trained to be aware of what kind of information a social engineer can use. Employees should know how to identify confidential information and should understand their responsibility to protect it.

The following table lists some common intrusion tactics and strategies adopted by Saksoft for prevention:

Area of Risk	Hacker Tactic	Combat Strategy
Phone (Help Desk)	Impersonation and persuasion	Employees / help desk are trained to never give out passwords or other confidential info by phone
Building entrance	Unauthorized physical access	Swipe card access, combination lock control, employee training and security officers present
Office	Shoulder surfing	Employees are trained not to type in passwords if anyone else present (or if you must, do it quickly and secretly!)
Office	Wandering through halls looking for open offices	Require all guests to be escorted

Server room	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab confidential data	Server rooms are kept locked at all times and keep updated inventory on equipment
Intranet-Internet	Creation & insertion of mock software on intranet or internet to snarf passwords	Continual awareness of system and network changes, training on password use
General-Psychological	Impersonation & persuasion	Make employees aware of such tactics through continued awareness and training programs

15. Training And User Guidelines

The following usage guidelines and mandatory training are provided to all employees so as to ensure that Saksoft security policy is well-adopted and compliance maintained.

15.1. General

- Ensure that you are aware of all available security mechanisms at Saksoft.
- Ensure that Cortex XDR is running and protecting the endpoint.
- NEVER share the entire C: or D: drive. If you have to share files, share only a folder, and only for a limited time. When you share a folder, make sure to click on “Permissions” to explicitly limit who can access your files. Try to grant only the “Read” permissions.
- Do not use the C: drive as your work area. Backup your work regularly. System administrators will help you in identifying backup and storage locations.
- The use of ‘Chat’ software is prohibited unless permitted for specific case/ project/ duration.
- Playing computer games is not permitted.
- If there is a need to download software for evaluation/testing purposes, inform to IT Support Team of your requirement.
- Unless your shared files are needed in your absence, shut down your system at the end of the day. Where this is a routine, seek IT TechSupport help to create a share in common fileservers, which are kept running 24*7.

15.2. Password Protection Standards

- Don't reveal a password over the phone to anyone.
- Don't reveal a password in an email message
- 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 co-workers while on vacation.

15.3. Email

Email is for employee business use only and is to be used in a responsible and efficient manner by Saksoft employees only.

NEVER open an email or an email attachment if it looks suspicious. Emails to be wary of will contain attachments with multiple filename extensions. If you are in doubt, ask for help from IT Support Team.

Email, which could be considered as “Chain Letter” or “Spam”, is not to be forwarded or distributed through Saksoft Corporate Email. If there is something of note to be shared with others at Saksoft, forward the relevant article to the HRD and they will do the needful.

Any email that contains material which could be deemed inappropriate or indecent, defamatory, racist or discriminatory is expressly forbidden to be sent through Saksoft Corporate Email.

Third Party provider email address should never show up in official emails / communications. Use of any email service other than official email service is not permitted except in emergencies.

Usages of standard disclaimer in email communication to outside entities support the process of exchange of information. A disclaimer note is sent out for all outgoing messages from the Saksoft E-mail Server.

<u>E-mail must not be used to for:</u>

- Any form of personal e-commerce e.g. buying anything, or conducting banking or investment activities.
- Activities that incur additional costs to Saksoft or interfere with your work performance.
- Profit-making activities that benefit you.
- Unlawful activities including sending or receiving copyrighted materials in violation of copyright laws or license agreements.
- Sending or receiving messages that are obscene or lewd in any way.
- Sending or receiving messages that are abusive in any way (racial, religious, etc.).
- Sending or receiving messages that contain information regarding criminal activities (drugs etc.).
- Sending or receiving messages that are inflammatory in way.
- Sending or receiving sexually explicit or offensive messages or graphics, jokes, ethnic slurs, racial epithets or any other statement (written or audible) or image (still or moving) that might be construed as harassment, disparagement or libel.

Remember that when you use e-mail to an external address you are a representative of Saksoft at all times and must portray a professional image.

15.4. Web

Do not use Internet at work to visit inappropriate web content.

Do not use your Saksoft email address when registering for services at websites. Your email address will end up a destination for unnecessary and potentially harmful spam. This also adds to our overhead and maintenance costs.

Checkpoint UTM feature is used as a web-filtering tool to restrict/monitor Internet usage in Saksoft. This tool is used to enhance the policy enforcement to ensure compliance. It is used as a centralized real time event monitoring via reporting and forensics service.

Only Project Leaders and above are provided with full time Internet access facilities based on respective approval. All other members shall have only limited period of Internet access. Additional hours of Internet access are enabled based upon request and subsequent approval from reporting manager.

Only Senior management and above will have access to private based Internet e-mails while it is blocked for the rest of the employees. Access to private e-mails can be provided upon request through IT Tech Support system and approval from respective project manager.

Only senior management and above will have access to Internet based instant messenger access while it is blocked for the rest of the employees. Access to Internet based instant messenger can be provided upon request through IT Tech support system and approval respective department head.

When trying to save a harmless file, you may be prompted by some websites to run an installation program. Check with your IT Support team first if this is all right.

16. Review Policy

Changes include events such as the implementation of major enterprise computing environment modifications and any occurrence of a major information security incident.

An evaluation of the existing security policy will be done by the IT Manager during the implementation of new System / Network Infrastructure or when there is a change in this policy document.

Exceptions to this document require approval from IT Manager

The IT Support team is responsible for regular review of the policy in the light of changing circumstances. The review will occur annually or when there are significant changes to the Systems / Network Infrastructure that may warrant changes to Saksoft Information Security Policy.

Saksoft’s internal auditor has a brief to ensure that the policy is appropriate for the protection of Saksoft IT Infrastructure.

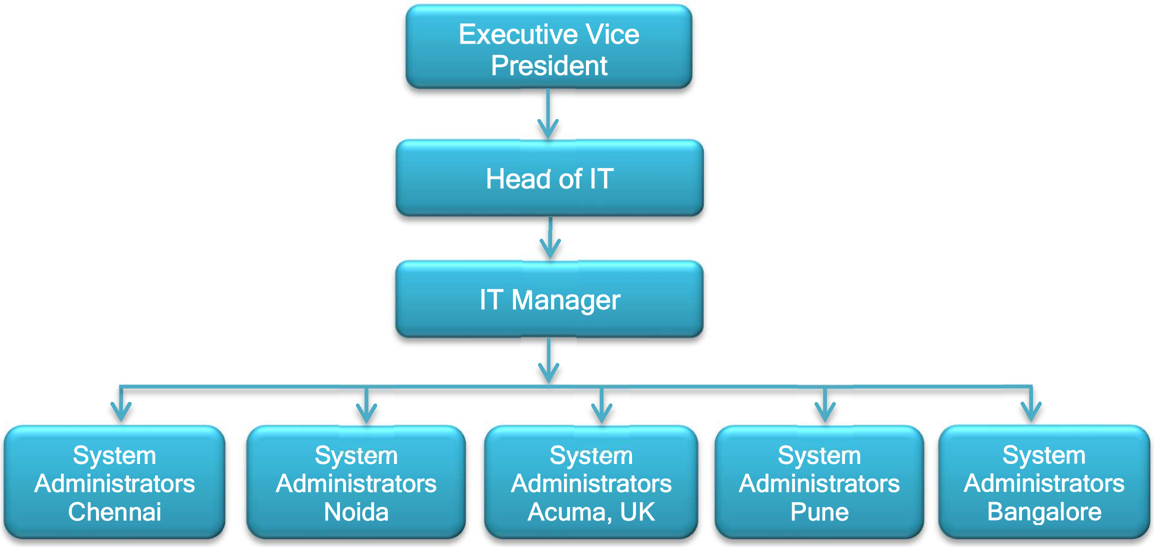
17. Change Management Policy

Saksoft’s Change Management Policy is based on the need for deploying changes to the IT Infra environment and avoiding business disruption while meeting compliance, regulatory, and audit requirements. Formalized Change Management brings discipline and quality control to IT. Attention to governance and formal policies and procedures will ensure Saksoft’s change deployment success.

The purpose of this policy is to establish a global standard methodology for deploying changes into the IT Infra environment. This policy will ensure the implementation of Change Management and control strategies to mitigate associated risks.

Please refer Saksoft Change Management Policy for detailed processes and procedures.

18. SYSTEM ADMIN ORGANIZATION CHART


Executive Vice President
Head of IT
IT Manager
System Administrators Chennai
System Administrators Noida
System Administrators Acuma, UK
System Administrators Pune
System Administrators Bangalore

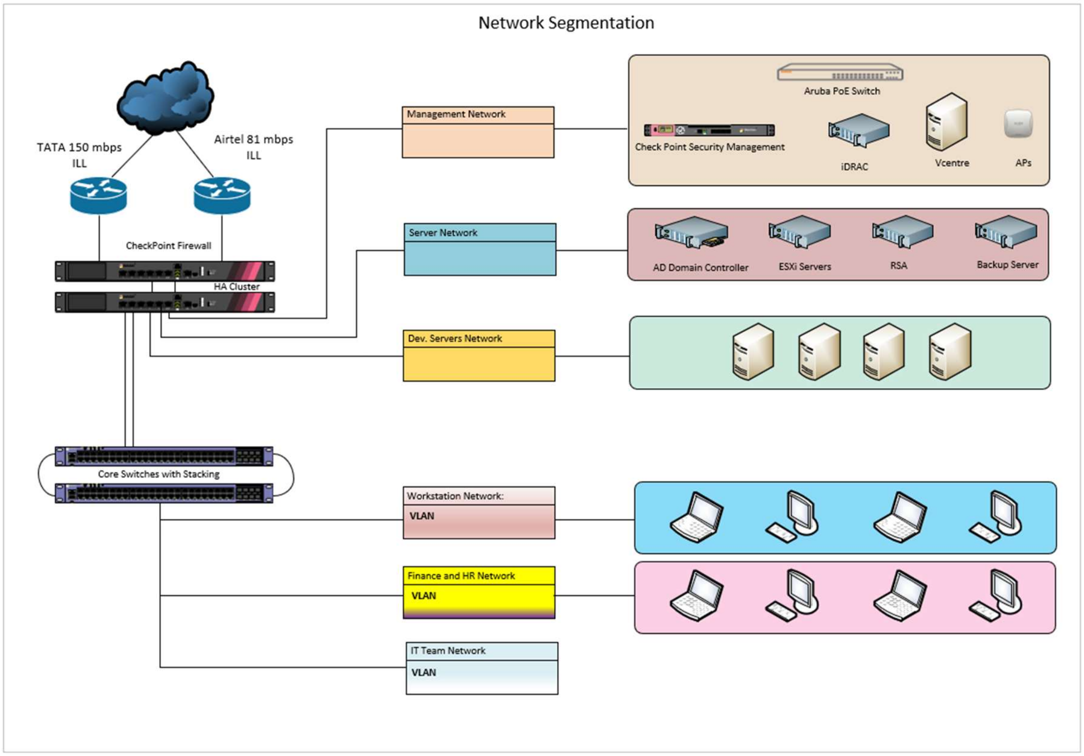
→	Executive Vice President	:	Dhiraj Mangala
→	Head of IT	:	Senthil Pandi
→	Chennai Team (CDC)	:	Manikandan, Kalaivanan and Joyhinn
→	Noida Team (NDC)	:	
	Saksoft	:	Mukesh Kumar and Karan Singh
	360Logica Team	:	Gurdeep, Azeem and Vishal Kumar
→	Acuma Team	:	Makarand
→	Pune Team (PDC)	:	Kishor Dhumal
→	Bangalore Team (BDC)	:	Boopathi, Kiran, Srikanth, Sivakumar and Naveen

Information Security Roles and Responsibilities:

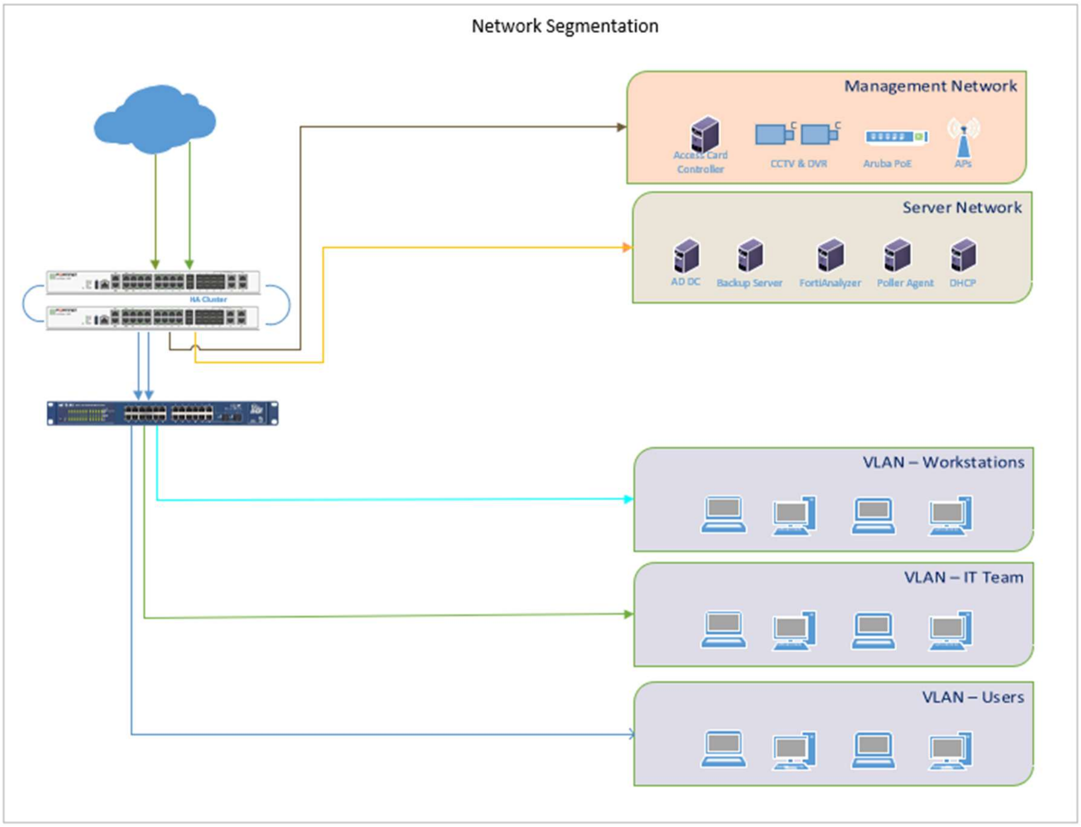
- Develop, implement, and maintain a comprehensive Information Security Program.
- Ensure the security and confidentiality of classified information.
- Protect against anticipated threats or hazards to the security or integrity of such information.
- Perform regular risk assessments to address reasonably foreseeable internal and external risks to the security, confidentiality, integrity, and availability of Classified Information.
- Employee training and management,
- Information systems including network and software design, as well as, information processing, storage, transmission and disposal,
- Detecting, preventing and responding to attacks, intrusions, or other system failures.
- Design and implement information safeguards to control risks identified through the above risk assessments, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures. Also, review and approve any changes to systems, procedures or Processes that could affect the effectiveness of these safeguards.
- The type of data being used or accessed (non-sensitive to sensitive)
- technical network changes • facility or processing locations • processes that would change security risks
- Develop and manage Information Security policies, guidelines, standards and procedures, including this document, as part of the Information Security Program. Policies, guidelines and standards must be regularly reviewed, but no less than annually.
- Provide security information and advice to all areas of the corporation, and responding, as appropriate, to security information requests and audits from customers and other third parties.
- Investigate information security events and violations of this policy.
- Ensure that all Workers receive security awareness training in information security appropriate to their position when initially on boarded, and at least annually thereafter, have completed online training in general security awareness topics.
- Monitor internal and external sources of threat and vulnerability information to identify and track risks to organization's reputation and business operations.
- Monitor organization's networks for threat activity, taking appropriate remediation or mitigation measures, and alerting appropriate parties to take action as needed.
- Stay informed about the latest developments in the information security field, including new products and services, through on-line news services, technical magazines, professional associations, industry conferences, training seminars, and other information sources.

19. Network Diagram

19.1. Chennai Development Center



19.2. Noida Development Center



20. Confidentiality Agreements

Saksoft will continue to adopt comprehensive policies and procedures to ensure the secure handling of personal information within all information environments.

Computer system users shall sign an appropriate NDA (Non Disclosure Agreement) and IPR (Intellectual Property Rights). This shall be part of the joining formalities of all employees. In addition to this Saksoft employees sign a separate security agreement if the customer/client insists from staff with access to sensitive data or systems.

21. Disciplinary Action

Disciplinary action is applicable to employees / to contract staffs who have violated organisational security policies or procedures, or used Saksoft facilities or equipment for unethical/ abusive purposes. It may lead to termination of employment also. Top management will decide on the action to be taken.