SAKSOFT
your digital transformation partner

Cyber Security 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		02-March-2023
	Title		Sr. IT Manager		
Reviewed By:					
	Name		Srinivasan E		02-March-2023
	Title		VP-Cloud and Infrastructure		
Approved By:					
	Name		Dhiraj Kumar Mangla		03-March-2023
	Titel		Executive Vice President & CCO		

AMENDMENT HISTORY

Sl. No	Amended By	Amended Date	Version No	Description of the Change
1	Senthil Pandi	02-March-2023	1.0	Policy Prepared
2	Senthil Pandi	18-Oct-2023	1.1	Changes in the reference documents
3	Senthil Pandi	14-Oct-2024	1.2	Updated patch manager plus process
4	Senthil Pandi	29-Sep-2025	1.3	Changes in the reference documents

List of Reference Documents

Sl. No	Document Name	Document Version
1	Saksoft Information Security Policy	7.3
2	Social Media Policy	1.0
3	Vulnerability Management Policy	1.5

TABLE OF CONTENT

1. Document Control

DOCUMENT INFORMATION:

Document Name:	Saksoft Cyber Security Policy
Document Version no:	1.3
Version date:	29-September-2025

2. Authorization

Name	Designation
Senthil Pandi	AVP-IT
Nirajkumar Ganeriwal	CFO & COO

3. Purpose

Cyber Security enables confidentiality, integrity, and availability of information by providing protection against malicious and accidental threats. Cyber Security threats take advantage of weaknesses in technology, employees, and processes to harm information. To address the cyber security risk, Saksoft has developed the Cyber Security Policy (CSP). CSP is a structured approach to set out the management strategy to address cyber security concerns and responsibilities of all the personnel to prevent breaches of cyber security and thus protect Saksoft business.

4. Scope

This Cyber Security Policy applies to all Saksoft employees, all employees of the Saksoft Group, contractors, supplier, partners, customers and third party with access to Saksoft's information technology assets.

5. Policy

Saksoft is committed to building a strong cybersecurity program to support, maintain, and secure critical infrastructure and data systems. In order to achieve this, Saksoft will identify, evaluate, and take steps to avoid or mitigate risk to the Saksoft's information assets and prevent unauthorized digital or physical access, damage, theft, compromise, or interference to the Saksoft's information systems and facilities. These steps include implementing and operating controls to manage the Saksoft's information security risks and ensuring that all users of information assets are aware of their responsibilities in protecting those assets while complying with all applicable regulations.

6. Responsibility

Roles and responsibilities must be separated so that a single individual, account, or function cannot intentionally or unintentionally subvert a critical process. Controls must also be put in place so that no single person can access, modify, or use assets without authorization or detection. Achieving and maintaining cybersecurity is a shared responsibility.

Information Technology Manager (IT Manager) will ensure that a written Cybersecurity Policy is implemented, reviewed and updated on a periodic basis.

Under the direction of the IT Manager, the Information Technology Administrator will help implement and enforce the items outlined in this policy.

All users, including employees, elected officials, contractors, must comply with all aspects of this policy. Users are responsible for the acceptable use and security of infrastructure and data.

7. Risk Management

Saksoft maintains an Information Security Risk Management Process and mechanisms to frame, assess, respond, and monitor information security related risks.

All Information Systems, information assets, and business processes that involve non-public information at Saksoft must be assessed for risk to the organization that results from threats to the integrity, availability, and confidentiality of Saksoft Data.

IT Techsupport Team will conduct ongoing assessments of threats and risks related to information assets and business processes, to determine the need of safeguards, countermeasures, and controls. Saksoft senior leadership had adopted an IT risk-averse posture.

Risks identified by a risk assessment must be mitigated or accepted prior to the system being placed into operation.

8. Standards

7.1 Asset Management

An inventory of all approved hardware and software on the Saksoft network and systems will be maintained that documents the following:

- The employee in possession of the hardware or software
- Date of purchase
- Serial number
- Type of device and description
- For licensed software: # of licenses, license renewal date(s), other restrictions, etc.

7.2 Identity Management and Authentication

IT Manager is responsible for ensuring that access to the corporate systems and data is appropriately controlled. All systems in Saksoft such as laptops, desktops and servers are required to be protected with a password or along with other form of authentication.

Saksoft has established the following password configuration requirements for all systems and applications (where applicable):

- Minimum password length: 8 characters.
- Password complexity: Mixture of letters, numbers, upper & lower case and special characters.
- Prohibited reuse for ten (10) iterations.
- Changed periodically (every 30 days).
- Invalid login attempts set to lock after 3.

Employees are encouraged to follow further safeguards such as:

- Utilizing Locking file cabinets
- Encrypting sensitive files on computers
- Requiring password protection
- Enabling multi-factor authentication

Where possible, multi-factor authentication will be used when users authenticate to Saksoft systems.

- Users are granted access only to the system data and functionality necessary for their job responsibilities.
- Privileged and administrative access is limited to authorized users who require escalated access for their job responsibilities and where possible will have two accounts: one for administrator functions and a standard account for day-to-day activities.
- All user access requests must be approved by the IT Manager.

- IT Team shall make sure all system access is removed of all users who separate from the company.

7.3 Access Control

Access control procedures, are in place and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

Users will only be given sufficient rights to specific systems that they need access to enable them to perform their job function. Where possible user rights will be kept to a minimum at all times.

File systems will have the maximum security implemented that is possible and where possible, users will be given permission based on access level approved by respective line manager. Files will be flagged as read only to prevent accidental deletion.

Where possible no person will have full rights to any system. IT Techsupport team will control network/ server passwords and system passwords. No single person shall be the only person to have full rights to the Saksoft Systems.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

On an annual basis, a review of user access will be conducted by the departments under the direction of the IT Manager to confirm compliance with the access control policies outlined above.

Removal of users:

When an employee leaves Saksoft, their access to Saksoft systems and data must be disabled at the close of business on the employee's last working day. It is the responsibility of the employees' line manager or HR to advise IT Techsupport of all leavers and the date of leaving and to request the suspension of the access rights. Confirmation that all user assets have been returned, disabled and user rights removed will be documented using the leaver declaration documentation.

This process applies to all Saksoft and its group employees and any contractors or suppliers that have been registered as users of equipment and access to active directories.

Privilege management:

Special privileges are those allowed to IT Techsupport only or to those who are allowed access to any sensitive areas, such as passwords, sensitive personal data, finance drives or any company confidential information. Any non-approved access is a major risk factor to the vulnerability of systems and data.

Privileged access must be authorised by Senior Directors and executives only using the User Access Control Request.

A master list of privileged accesses will be maintained by IT Techsupport.

7.4 Social Media

Saksoft has a separate Team for managing Saksoft's social media platforms. Except for the team, no employee is allowed to post any content on purporting to be on behalf of the Saksoft group companies on the internet.

Rules of use of social media:

- Keep personal and professional life separate.
- Do not post, forward or upload or share a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.
- Any member of the staff who feels that they have been harassed or bullied or are offended by the material posted or uploaded by a colleague onto a social media site must inform the social media team and HR team immediately for investigation and taking further action, if appropriate.
- Never disclose commercially sensitive, anti - competitive, private or commercial information. If unsure whether the information shared lies within any of the above mentioned categories, please consult the social media team.
- Do not post, forward or upload anything belonging to a customer / partner without that their consent.
- When in doubt about a link, please do not share. You can consult with IT Techsupport team to clear your doubts. Before including a link to a third party website, check whether any terms and conditions are involved in linking the website. All links must be done so that it is clear to the user that they have moved to the third party's website.
- Employees should pay special attention to intellectual property and personal data protection before posting. Read before complying with its terms of use/ acceptance guidelines of social media sites.
- Employees should be mindful of the impact of anything they post over social media, as it also reflects on people's perception of the Organization.
- Employees responsible for the content published in the social media tool should be alert that whatever is published will be public for many years and it would be impossible to take it down entirely from the internet e.g. individuals can take screenshots of the content and circulate it.
- Never mention the details or any information pertaining to colleagues, customers or clients without their prior written permission.

- Always consider others privacy and avoid discussing topics that might be inflammatory, controversial, e.g. politics and religion.
- Avoid discussing contact details where they can be accessed and used publicly.
- Posting rumors, internal and confidential information can lead to legal action against the employee.
- Decency and basic etiquettes must be maintained in all modes of communication.

7.5 Awareness and Training

Saksoft employees are required to complete Saksoft assigned security training:

a) Upon hire and within 30 days of receiving login credentials
b) Annually

On an annual basis, the IT Manager will conduct email phishing exercises of its users. The purpose of these tests is to help educate users on common phishing scenarios. It will assess the level of awareness and comprehension of phishing, understanding, and compliance with policy around safe handling of emails containing links and/or attachments, and the ability to recognize a questionable or fraudulent message.

7.6 Data Security

7.6.1 Data Classification

Users must adhere to the Records Retention Policy regarding the storage and destruction of data. Data residing on Saksoft's systems must be continually evaluated and classified into the following categories:

Users' Personal Use: Includes individual user's personal data, emails, documents, etc. This policy does not apply to a user's personal information.

Marketing or Informational Material: Includes already-released marketing material, commonly known information, data freely available to the public, etc. and this policy does not apply.

Operational: Includes data for basic organizational operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.

Confidential: Any information deemed confidential. The following list provides guidelines on what type of information is typically considered confidential. Confidential data may include:

- Employee Information
- Client / vendor Information
- Protected Health Information
- Network diagrams and security configurations
- Privileged communications regarding legal matters

- Passwords/passphrases
- Bank account information and routing numbers
- Payroll information
- Credit card information
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information).

7.6.2 Data Storage

The following guidelines apply to storage of the different types of organizational data.

- **Operational:** Operational data should be stored on a server that gets the most frequent backups.

- **Confidential**: Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored with password protected.

7.6.3 Data Encryption

Data in Rest

Full disk encryption encrypts all data on a system, including files, folders and the operating system. This is most appropriate when the physical security of the system is not assured. Examples include traveling laptops or desktops that are not in a physically secured area. Saksoft authorized to use BitLocker for full drive encryption.

Data Transmission

The following guidelines apply to the transmission of the different types of organizational data.

- **Confidential**: Confidential data shall not be 1) Transmitted outside the Saksoft's network without the use of strong encryption 2) Left on voicemail systems, either inside or outside the organization's network. 3) Transmitted via email, outside of the organization's network.

Data while transmitted, includes any data sent across the Saksoft's network or any data sent to or from a Saksoft provided system. Types of transmitted data that shall be encrypted include:

- VPN tunnels
- Remote access sessions
- Web applications
- Email and email attachments
- Remote desktop access
- Communications with applications.

7.6.4 Data Destruction

Employees must follow Saksoft's records retention policy and procedures before destroying any data.

Confidential: Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply to data located on Saksoft provided systems, devices, media, etc.:

- Storage media (CD's, DVD's): Physical destruction is required, some shredders may be able to perform this function.

- Hard drives/systems/mobile storage media: At a minimum, DoD three (3) pass data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, Saksoft shall use the most secure commercially available methods for data wiping. Alternatively, Saksoft may physically destroy the storage media.

9. Information Protection Progress and Procedures

8.1 Secure Software Development

Where applicable, all software development activities performed by Saksoft shall employ secure coding practices including those outlined below.

A minimum of 2 software environments for the development of software systems should be available – development and testing environment. Software developers or programmers are required to develop in the development environment and promote objects into the testing environments. The development environment is used for assurance testing by the end-user and the developer.

8.2 Contingency Planning

The Saksoft's business contingency capability is based upon cloud and local backups of all critical business data. This critical data is defined as "the data that is critical to successful organization operation". Full data backups will be performed on a daily basis. Confirmation that backups were performed successfully will be conducted daily. Testing of cloud backups and restoration capability will be performed on a monthly basis.

During a contingency event, all IT decisions and activities will be coordinated through and under the direction of the Information Technology Manager.

The following are some examples of possible business contingency scenario procedures:

- In the event that one or more of Saksoft's systems or applications are deemed corrupted or inaccessible, the Information Technology Manager will work with the respective vendor(s) to restore data from the most recent cloud and local backup and, if necessary, acquire replacement hardware.

- In the event that the on-premises Saksoft's systems are no longer accessible, the Information Technology Manager will work with the respective vendor(s) to acquire any necessary replacement hardware and software, implement these at one of the Saksoft's other sites, and restore data from the most recent cloud, off-site, or local backup.

8.3 Network Infrastructure

The Saksoft will protect its electronic communications network from the Internet by utilizing a firewall. For maximum protection, the network devices shall meet the following configuration standards:

- Vendor recommended, and industry standard configurations will be used.
- Changes to firewall and router configuration will be approved by Information Technology Manager.
- Both router and firewall passwords shall be secured and difficult to guess.
- The default policy for the firewall for handling inbound traffic shall be to block all packets and connections unless the traffic type and connections have been specifically permitted.
- Inbound traffic containing ICMP (Internet Control Message Protocol) traffic shall not be passed in from the Internet, or from any un-trusted external network.
- Simple Network Management Protocol (SNMP) Community Strings shall be made (changed from the default “public”) “private”.

10. Protective Technology

9.1 Email Filtering

Saksoft has applied the filters for email inbound and outbound traffic on email gateway. This filtering will help reduce spam, viruses, or other messages that may be deemed either contrary to this policy or a potential risk to the Saksoft's IT security.

Additionally, anti-malware program has implemented to identify and quarantine emails that are deemed suspicious.

9.2 Internet Filtering

The IT Department shall block access to internet websites and protocols that are deemed inappropriate or pose a security risk. Some examples of blocked categories are adult/sexually explicit material, advertisements, hacking, violence and hate content.

9.3 Network Vulnerability Assessments

On a biannual basis the Security Testing Team will perform both internal and external network vulnerability assessments. The purpose of these assessments is to establish a comprehensive view of the organization’s network as it appears internally and externally. These evaluations will be conducted under the direction of Information Technology Manager to identify weaknesses with the network configuration that could allow unauthorized and/or unsuspected access to the organization’s data and systems.

In addition, annual penetration testing will be run to identify weaknesses or vulnerabilities that will need to be addressed.

11. Anomalies and Events

The following logging activities are conducted by IT System Administrator under the direction of Information Technology Manager:

- Domain Controllers - Active Directory event logs settings configured to log the following security events: account creation, escalation of privileges, login failures, and excessive repeated login attempts.

- Application Servers - Logs from application servers (e.g., web, email, database servers) settings configured to log the following events: errors, faults, login failures, and excessive repeated login attempts.

- Network Devices - Logs from network devices (e.g., firewalls, network switches, routers) settings configured to log the following events: errors, faults, login failures, and excessive repeated login attempts.

12. Security Continuous Monitoring

12.1 Anti-Malware Tools

Saksoft has deployed Palo Alto Cortex XDR as Endpoint security on all the servers, desktops and laptops. 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.

12.2 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.

13. Response Planning

Saksoft's annual security awareness training shall include direction and guidance for the types of security incidents users could encounter, what actions to take when an incident is suspected, and who is responsible for responding to an incident. A security incident, as it relates to Saksoft's information assets, can be defined as either an Electronic or Physical Incident.
Information Technology Manager is responsible for coordinating all activities during a significant incident, including notification and communication activities and the chain of escalation and deciding if/when outside agencies, need to be contacted.

13.1 Electronic Incidents

This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes to a virus outbreak or a suspected Trojan or malware infection. When an electronic incident is suspected, the steps below should be taken in order.

- Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.
- Report the incident to the IT System Administrator or Information Technology Manager.
- Contact the third-party service provider (and/or computer forensic specialist) as needed.
- Disable the compromised account(s) as appropriate.
- Backup all data and logs on the machine, or copy/image the machine to another system.
- Determine exactly what happened and the scope of the incident.
- Determine how the attacker gained access and disable it.
- Rebuild the system, including a complete operating system reinstall.
- Restore any needed data from the last known good backup and put the system back online.
- Take actions, as possible, to ensure that the vulnerability will not reappear.
- Conduct a post-incident evaluation. What can be learned? What could be done differently?

13.2 Physical Incidents

A physical IT security incident involves the loss or theft of a laptop, mobile device, Smartphone, portable storage device, or other digital apparatus that may contain Saksoft's information. All instances of a suspected physical security incident should be reported immediately to the IT System Administrator or Information Technology Manager.

12.3 Notification

If an electronic or physical security incident is suspected of having resulted in the loss of, or unauthorized access to employee information or third-party/customer data, notify the Saksoft Attorney's office for direction on procedures for notification of the public or affected entities as well as necessary government agencies.

14. Recovery & Restoration

Recovery processes and procedures shall be executed and maintained to ensure timely restoration of systems and/or assets affected by cybersecurity events.

Information Technology Manager is responsible for managing and directing activities during an incident, including the recovery steps.
Recovery planning and processes are improved by incorporating lessons learned into future activities.

Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet service providers, owners of the affected systems, victims, and vendors.

External communications should only be handled by designated individuals at the direction of the Saksoft Administrator. Recovery activities are communicated to internal stakeholders, executives, and management teams.

15. Policy Governance

The following table identifies who within Saksoft is Accountable, Responsible, or Informed with regards to this policy. The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.
- Accountable – the person who has ultimate accountability and authority for the policy.
- Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Executive Vice President
Accountable	IT Head
Informed	All employees, Contractors and Partners