IT Security Policy Document: Saged's Company

Document Version: 1.0
Effective Date: June 25, 2025
Review Date: June 25, 2026

1. Introduction and Purpose

This IT Security Policy document outlines the comprehensive security measures and guidelines at Saged's Company to protect its information assets, IT infrastructure, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. The purpose of this policy is to:

- Establish clear expectations for all employees, contractors, and third parties regarding information security.
- Safeguard the confidentiality, integrity, and availability of Saged's Company's data and systems.
- Comply with relevant legal, regulatory, and contractual obligations.
- Minimize risks associated with information technology use and ensure business continuity.
- Foster a security-aware culture throughout the organization.

2. Scope

This policy applies to all employees (full-time, part-time, temporary), contractors, consultants, and any third parties who have access to Saged's Company's information systems, networks, data, and physical IT assets, regardless of their location. It covers all IT resources, including but not limited to:

- Company-owned and managed devices (laptops, desktops, mobile phones, tablets).
- Company networks (wired, wireless, VPN).
- Servers, databases, and cloud services.
- Software applications and data.
- Any personally-owned devices used to access company resources (BYOD).

3. Roles and Responsibilities

Information security is a shared responsibility.

- **Management:** Responsible for providing adequate resources, promoting a security-aware culture, and enforcing this policy.
- **IT Department:** Responsible for implementing, maintaining, and monitoring security controls, conducting security assessments, managing incidents, and

providing security training.
- **All Employees:** Responsible for understanding and adhering to this policy, protecting company information and assets, and promptly reporting any security concerns or incidents.
- **Data Owners:** (e.g., Department Heads) Responsible for classifying data within their departments and ensuring appropriate security measures are applied.

4. Acceptable Use of IT Resources

All users must use Saged's Company's IT resources responsibly and ethically, primarily for business purposes.

- **Prohibited Activities:**
  - Illegal activities, including copyright infringement.
  - Accessing, creating, or distributing offensive, discriminatory, or harassing material.
  - Engaging in activities that could compromise the security, integrity, or performance of company systems (e.g., hacking, introducing malware).
  - Excessive personal use that interferes with job performance or consumes excessive network resources.
  - Unauthorized downloading or installation of software.
- **Monitoring:** All use of company IT resources is subject to monitoring and audit by Saged's Company. Users should have no expectation of privacy when using company systems.

5. Access Control

Access to Saged's Company's information systems and data is granted based on the principle of least privilege – users are given only the access necessary to perform their job functions.

- **User Accounts:**
  - Each user must have a unique account. Sharing accounts is strictly prohibited.
  - Accounts must be disabled or removed promptly upon an employee's termination or role change.
- **Passwords:**
  - Passwords must be strong (a combination of uppercase, lowercase, numbers, and special characters) and a minimum of 12 characters.
  - Passwords must not be reused across multiple systems.
  - Passwords must be changed every 90 days.
  - Passwords must never be written down or shared.
- **Multi-Factor Authentication (MFA):** MFA is mandatory for accessing all critical systems and remote access services.

- **Remote Access:** All remote access to company networks and systems must be via approved VPNs or secure remote desktop solutions.

6. Data Security and Handling

Data at Saged's Company is classified to ensure appropriate protection based on its sensitivity and importance.

- **Data Classification:**
  - **Confidential:** Highly sensitive data (e.g., financial records, customer PII, intellectual property, employee HR records). Requires the highest level of protection.
  - **Internal:** Data for internal business use only (e.g., internal reports, non-sensitive communications).
  - **Public:** Data that can be freely distributed outside the company without risk (e.g., marketing materials, press releases).
- **Data Storage:** Confidential and Internal data must only be stored on approved company servers, cloud storage, or encrypted devices. Personal cloud storage (e.g., personal Dropbox, Google Drive) is prohibited for company data.
- **Data Sharing:** Confidential data should only be shared with authorized individuals on a need-to-know basis and through secure, approved methods (e.g., encrypted email, secure file transfer).
- **Encryption:** All laptops, mobile devices, and removable media containing Confidential or Internal data must be encrypted. Data transmitted over public networks must use encrypted protocols (e.g., HTTPS, SFTP, VPN).
- **Data Retention and Disposal:** Data must be retained according to legal and business requirements. When data is no longer needed, it must be securely disposed of to prevent unauthorized recovery.

7. Network Security

Saged's Company implements network security measures to protect against unauthorized access and cyber threats.

- **Firewalls:** Network perimeters are protected by firewalls. Unauthorized modifications to firewall rules are prohibited.
- **Wireless Networks (Wi-Fi):** Employees are only permitted to connect to the official company Wi-Fi networks (corporate and guest) on company premises. Personal hotspots are not permitted for connecting company devices.
- **Remote Access (VPN):** A Virtual Private Network (VPN) is required for accessing internal network resources from outside the company premises. VPN credentials

must be kept confidential.

8. Endpoint Security

All devices connected to Saged's Company's network or used to process company data are subject to endpoint security requirements.

- **Anti-Malware:** All company-issued computers and mobile devices must have approved anti-malware software installed and kept up-to-date. Users must not disable or tamper with this software.
- **Operating System & Application Updates:** Operating systems and applications on all company devices must be kept updated with the latest security patches. Automatic updates should be enabled where possible.
- **Mobile Device Security:** Mobile devices (smartphones, tablets) used for company business must be passcode-protected, have remote wipe capabilities enabled, and adhere to all applicable security configurations.
- **Personal Devices (BYOD):** Personally-owned devices used for company business must comply with endpoint security requirements, including anti-malware, password protection, and adherence to company mobile device management (MDM) policies. Saged's Company reserves the right to wipe company data from personal devices in case of loss, theft, or termination of employment.

9. Incident Response

A security incident is any event that could compromise the confidentiality, integrity, or availability of Saged's Company's information assets.

- **Reporting Incidents:** All employees are responsible for immediately reporting any suspected or actual security incidents to the IT Department or their manager. Examples include:
  - Lost or stolen devices.
  - Suspicious emails (phishing attempts).
  - Unauthorized access attempts or successful intrusions.
  - Missing or corrupted data.
  - Malware infections.
- **Incident Handling:** Upon receiving an incident report, the IT Department will:
  - Assess the severity and impact of the incident.
  - Contain the incident to prevent further damage.
  - Eradicate the cause of the incident.
  - Recover affected systems and data.

    - Conduct a post-incident analysis to identify lessons learned and implement preventative measures.
- **No Tampering:** Employees must not attempt to investigate or remediate security incidents on their own, as this could compromise evidence or worsen the situation.

10. Software and Application Security

Saged's Company manages software and application usage to minimize security risks.

- **Approved Software:** Only approved and licensed software may be installed on company devices. Employees must not install unapproved software from unknown sources.
- **Software Updates:** All software must be kept updated to the latest secure versions.
- **Application Development (if applicable):** Software developed internally must follow secure coding practices, undergo security testing, and be regularly audited for vulnerabilities.
- **Cloud Service Usage:** Before using any third-party cloud service for company data or operations, IT approval is required to ensure the service meets Saged's Company's security standards and legal obligations.

11. Physical Security of IT Assets

Physical access to Saged's Company's IT assets is controlled to prevent unauthorized tampering, theft, or damage.

- **Server Rooms/Data Centers:** Access to server rooms and data centers is restricted to authorized personnel only. Access logs are maintained.
- **Workstations:** Employees are responsible for securing their workstations and devices.
    - Always lock your computer screen when leaving your desk, even for a short time.
    - Do not leave sensitive documents unattended.
    - Do not prop open secure doors or allow unauthorized individuals to "tailgate" into secure areas.
- **Equipment Removal:** Company IT equipment (laptops, monitors, etc.) must not be removed from company premises without explicit authorization from management and IT.

12. Compliance

Saged's Company is committed to complying with all applicable laws, regulations, and contractual requirements related to information security and data privacy. This includes, but is not limited to:

- **Data Protection Regulations:** (e.g., GDPR, CCPA, or local country-specific data protection laws) where applicable based on data processing activities.
- **Industry Standards:** Adherence to relevant industry best practices and security frameworks (e.g., ISO 27001, NIST Cybersecurity Framework, if adopted).

Employees are expected to understand and comply with these requirements as they pertain to their roles. Any questions regarding compliance should be directed to the IT Department or Legal Counsel.

13. Policy Violations and Enforcement

Violation of any part of this IT Security Policy may result in disciplinary action, up to and including termination of employment, and potential legal action. The severity of the disciplinary action will depend on the nature and impact of the violation, whether it was intentional or accidental, and the employee's history of compliance.

- **Investigation:** All suspected violations will be investigated thoroughly and fairly by the IT Department and/or HR.
- **Disciplinary Action:** Actions may include:
  - Verbal warning.
  - Written warning.
  - Mandatory security retraining.
  - Suspension of IT privileges.
  - Suspension from employment.
  - Termination of employment.
  - Reporting to law enforcement, if criminal activity is suspected.

14. Policy Review and Updates

This IT Security Policy document will be reviewed annually, or as needed, to ensure its continued relevance, effectiveness, and compliance with evolving threats, technologies, and regulatory requirements. Employees will be notified of any significant updates or revisions. It is the responsibility of each employee to stay informed about the most current version of this policy.

End of Document