Information Security, Data Protection, and Acceptable Use Policy

The Sripath Group of Companies (Sripath®) is committed to preserving the confidentiality, integrity, and availability of institutional, customer, and proprietary data. This policy establishes requirements for information technology infrastructure, corporate data, and acceptable digital practices across Sripath® operations, including information technology (IT) and security support provided by Sripath-approved Service Provider.

Operational Scope

This policy applies universally across all Sripath® entities. The scope encompasses:

- All personnel, including full-time and part-time employees, contract employees, temporary workers, intern placements, and staff operating under contingent arrangements ("Employee").
- All third-party representatives including independent contractors, consultants, service providers, and affiliated subcontractors operating on behalf of Sripath® ("Contractor").
- All information technology hardware, cloud applications, network resources, databases, mobile devices, and physical facilities owned, leased, managed, or authorized by Sripath®, regardless of physical location, and any Contractor-owned devices used to access Sripath® Systems or data ("Devices").

Governance, Roles, and Accountability

Security and data stewardship are collective obligations enforced at every organizational level:

- **Executive Oversight:** The Sripath® Global Executive Team is responsible for formal approval and strategic alignment of corporate security policies.
- **Management Responsibility:** Individuals in a supervisory role must ensure direct reports and assigned third-party vendors understand and comply with security controls and operational guidelines.
- **Technical Service Providers:** Sripath® remains responsible for business decisions, personnel-change notifications, policy approval, user conduct, data ownership, and final authorization of access, configuration, and security exceptions unless otherwise expressly agreed in writing. Sripath-approved Service Providers may provide infrastructure, security, monitoring, maintenance, and technical support services within the scope authorized by Sripath® and applicable written agreements.
- **Individual Accountability:** Every authorized system user is responsible for safeguarding assigned credentials, protecting company assets, and reporting security anomalies.

System Access and Credentialing

System access within Sripath® follows a least-privilege model. Users are granted access only to the systems, files, and applications required for their assigned duties.

- **Account Integrity:** Shared, generic, or anonymous user credentials are strictly prohibited. Every user must operate under a unique, auditable identity.
- **Authentication Standards:** All access points must be protected by robust authentication protocols. Multi-Factor Authentication (MFA) is required across cloud environments, remote connectivity tools, and email services where supported and appropriate for the system risk profile.
- **Lifecycle Reviews:** Access rights are reviewed periodically. Sripath is responsible for identifying personnel changes and initiating account creation, modification, and termination requests through the designated IT support channel. Sripath-approved Service Providers act on such requests only after receiving appropriate authorization, unless emergency containment is required.

Endpoint Security, Device Management, and Patching

Every authorized system user is responsible for ensuring all endpoints connected to Sripath® infrastructure remain compliant with modern endpoint protection baselines:

- **Malware Defense:** Endpoint Detection and Response or anti-malware software must remain active, monitored, and regularly updated. Users are prohibited from disabling or altering security agents.
- **Vulnerability and Patch Management:** Operating systems, browsers, and core software suites must be configured for automated security updates where feasible. Critical vulnerability patches will be assessed, prioritized, and deployed for covered environments within agreed service levels, subject to Sripath approval, maintenance windows, compatibility constraints, and documented exceptions.
- **Device Handling:** Equipment must be secured when left unattended. Screen lock timeouts must be enforced after short periods of inactivity.

Remote, Hybrid, and Mobile Work Protocols

Personnel performing official duties outside corporate offices, including Contractors, must maintain the same security standards required for on-site operations.

- **Physical Safeguards:** Devices must be stored securely and shielded from unauthorized viewing in public or shared spaces. Devices must never be lent to non-affiliated third parties.
- **Asset Loss Procedures:** Immediate reporting is mandatory if any corporate-connected device is lost, stolen, or compromised.

Acceptable Use of Digital Assets

Access to Sripath® information systems ("Systems") is provided to Employees and Contractors for legitimate corporate operations and client service delivery.

- **Professional Standards:** Systems must not be utilized to create, transmit, store, or display material that is illegal, defamatory, harassing, or in violation of Sripath® corporate standards.
- **System Integrity:** Personnel must not attempt to bypass System security boundaries, perform unapproved security scans, install unauthorized third-party software, or disable administrative settings.

- **Messaging and Communication:** Corporate email and messaging platforms must be used responsibly. Users must exercise high vigilance against phishing, social engineering tactics, and fraudulent wire or data transfer requests.
- **Identity Verification:** Personnel must verify the identity and authorization of anyone requesting credentials, remote access, payment changes, data transfers, or security exceptions. Requests submitted through designated support channels must follow Sripath-approved identity verification and authorization procedures before account, device, or security changes are performed.

Data Privacy, Retention, and Secure Disposal

Sripath® handles personal and confidential data in alignment with applicable privacy laws, statutory data protection regulations, and client confidentiality agreements that apply to its operations and data processing activities, which may include GDPR (EU), UK GDPR, PIPEDA (Canada), CCPA, and CPRA (California, USA).

- **Data Minimization:** Collection and processing of personal data are limited strictly to legitimate business needs and legal mandates.
- **Lifecycle and Disposal:** Data must be retained only for the duration specified by legal, tax, regulatory, contractual, or operational requirements ("Retention Obligations"). When data reaches the end of its required lifecycle and there are no Retention Obligations to retain data, it must be purged or physically destroyed through secure sanitization methods.
- **End User Access:** Sripath® Employees and Contractors with access to Sripath® Systems or data must comply with applicable confidentiality, data protection, and security obligations under written agreements with Sripath®. Access to personal data, client records, proprietary information, or regulated information must be limited to the authorized purpose, duration, systems, and personnel approved by Sripath®.
- **Monitoring and Privacy Expectations:** Use of Sripath® Systems may be logged, monitored, reviewed, and retained by Sripath® or its authorized service providers for security, operational, legal, and compliance purposes, subject to applicable law and written contractual obligations. Users should have no expectation of privacy when using Sripath® Systems except where required by law.

Management of Generative AI and Machine Learning Tools

Sripath® encourages innovative efficiency while enforcing strict parameters around Artificial Intelligence (AI) platforms:

- **Data Input Restrictions:** Personnel are strictly prohibited from entering proprietary code, client records, personal data, intellectual property, or access credentials into public AI tools or unvetted external services.
- **Verification and Responsibility:** Outputs generated by AI systems must undergo human review for accuracy, bias, and technical validity. Users remain fully responsible for any deliverables or decisions derived from AI-assisted workflows.

Incident Management, Violations, and Reporting

A security incident includes any event that threatens the confidentiality, integrity, functionality, or availability of Sripath® systems such as suspected malware infection, phishing interactions, lost devices, or unauthorized access attempts.

- **Mandatory Reporting:** Security incidents, suspected vulnerabilities, lost or stolen devices, phishing attempts, and unauthorized access concerns must be reported immediately to Sripath management through the company's designated IT support channel.
- **Emergency Containment:** Sripath-approved Service Providers may take temporary containment actions within the authorized scope of services when necessary to reduce imminent security risk and must notify Sripath management as soon as practicable.
- **Non-Retaliation Guarantee:** Sripath® maintains a protective reporting environment. Personnel who report potential security breaches, compliance failures, or vulnerabilities in good faith will be protected from coercion, harassment, or administrative retaliation.
- **Enforcement:** Non-compliance with this policy compromises Sripath® operational security and may result in corrective actions, up to and including account suspension and termination of employment or contract.

Management Oversight of Policy Effectiveness

The Sripath® Data Policy Team, consisting of a minimum of three employees designated by the President, will review reported incidents, audit findings, regulatory changes, operational needs, and service-provider performance considerations at least twice annually. The effectiveness of this policy will be reviewed based on those factors, and revisions will be made when warranted. Revisions to the policy will be communicated promptly throughout the organization.

Approved by: Sripath® Global Executive Team
Reviewed Annually

Issue Date: September 1, 2026