# Trackmedium Information Security Program Standards

These Information Security Program Standards describe the information security program adopted by Trackmedium to help secure Subscriber Data against unauthorized processing and accidental or unlawful loss, access, or disclosure (the "**Information Security Program**"). These Information Security Program Standards are in addition to, and not in lieu of, any additional security requirements specified in the Agreement or otherwise agreed in writing between Trackmedium and Subscriber. These Information Security Program Standards are incorporated into the Agreement (as defined in the Trackmedium Master Subscription Agreement (the "MSA")) by reference and apply to Subscriber's use of the Products. These Information Security Program Standards apply separately to each Subscriber account using the Products.

Capitalized terms used but not defined in these Information Security Program Standards have the meanings set forth in the Agreement.

**Effective Date of this version**: February 25, 2026.

1. **Policies**. Trackmedium will maintain and enforce information security policies and procedures designed to safeguard the confidentiality, integrity, and availability of Subscriber Data. Trackmedium's policies are aligned with relevant industry standards and the ISO/IEC 27001 framework. These policies cover managerial, operational, and technical security controls appropriate to the Services and the risks to Subscriber Data. Trackmedium will periodically review and update its policies to address evolving security risks and findings identified through such reviews.

2. **Strong authentication and role-based, non-unilateral access restrictions**. By default, Trackmedium personnel do not have access to Subscriber Data. Trackmedium personnel must be a member of relevant access control lists to gain access to sensitive data. In addition, personnel must read and acknowledge Trackmedium's data access policies regularly. To access Subscriber Data, Trackmedium personnel must use individual accounts and authenticate using a trusted device and multi-factor authentication via Security Keys, which also minimizes the risk of credentials being phished. From this trusted device, they can access tooling that evaluates the justification provided (i.e., Support Ticket, etc.), the user's role and context to determine if they can obtain access to the Subscriber Data.

3. **Data Storage.** Subscriber Data is hosted on Google Cloud. Google Cloud regularly undergoes independent third-party audits and makes SOC 2 Type II reports (SSAE 18) available to customers for in-scope services via Google's Compliance Reports Manager. Data centers implement physical and environmental security controls designed to protect customer data, including controlled facility access and monitoring.

4. **Role-Based Logical Access Control**. Trackmedium maintains role-based access controls (RBAC) and authentication controls designed to limit access to systems and Subscriber Data to authorized personnel only. Access is granted based on job role and least privilege. Trackmedium requires unique user accounts for personnel and prohibits shared credentials. Administrative access requires multi-factor authentication. Access to production systems and Subscriber Data is reviewed periodically and revoked promptly when no longer required.

5. **Network Security**. Trackmedium uses network security controls such as firewalls, network segmentation, and monitoring technologies designed to help protect systems that store or process Subscriber Data. External access to production services is restricted and monitored. Web application traffic is protected using a web application firewall (WAF) or functionally equivalent controls where applicable.

Proprietary to Trackmedium, LLC

6. **Secure Data Transfer.** Trackmedium requires that Subscriber Data transmitted to or from Trackmedium systems use approved secure transfer processes, such as HTTPS/TLS and secure file transfer protocol (SFTP), as applicable. Data transmitted using these processes is authenticated and encrypted during transmission.

7. **Encryption**. Trackmedium uses encryption in transit for Subscriber Data transmitted to or from Trackmedium systems using industry-standard TLS. Subscriber Data stored within Trackmedium hosting environments is encrypted at rest using industry-standard encryption capabilities provided by our hosting providers and managed services, where applicable.

8. **Security Training.** Trackmedium requires security awareness training for personnel with access to Subscriber Data.

9. **Vulnerability Assessments.** As part of its continuous monitoring program to evaluate the effectiveness of its security controls, Trackmedium conducts regular vulnerability assessments of both its network and web applications. These assessments encompass an evaluation of adherence to the Open Web Application Security Project (OWASP) Top Ten Web Vulnerabilities (www.owasp.org). Trackmedium may engage independent third-party assessors as part of its ongoing security program.

10. **Security & Network Monitoring.** Trackmedium has integrated various technologies, including firewalls, intrusion detection systems, and vulnerability management tools, into its infrastructure to monitor and detect network security events. Trackmedium monitors security logs and events for indicators of unauthorized access and anomalous activity, and investigates alerts in accordance with its incident response procedures.

11. **Endpoint Protection**: The Products offered by Trackmedium are designed to minimize the risk of introducing viruses to the Subscriber's Systems. However, it's important to note that while Trackmedium employs endpoint protection on its servers and corporate end user devices, its virus scanning capabilities may not extend to attachments or other data provided by the Subscriber, which may contain viruses or malware.

12. **Incident Response.** Trackmedium maintains an incident response process designed to identify, respond to, and mitigate security incidents. Trackmedium will notify customers of a confirmed security incident affecting Subscriber Data in accordance with the Agreement and applicable law.

13. **Web Application Security Controls and Procedures**: Trackmedium's Products employ the following procedures and controls:
    13.1. Secure Web Communications. Use of HTTPS for securing web server to web browser communications using Transport Layer Security (TLS) encryption and certificates issued by a trusted certificate authority.

    13.2. User Authentication. To ensure security, a valid and unique user ID and password combination is required for access, and while in transmission, they are encrypted to safeguard against unauthorized access.

    13.3. Password Reset and Account Recovery. Password resets are performed through a controlled workflow, either through self-service reset mechanisms or administrator-assisted resets, as applicable. Temporary credentials are time-bound and must be changed upon first login. Password reset activity is logged.

13.4. Security Controls:

13.4.1. Unique user IDs are assigned to ensure that activities can be traced back to the responsible individual.

13.4.2. Password complexity requirements mandate the use of both letters and numbers.

13.4.3. Controls are put in place to automatically terminate a user session after a period of inactivity to reduce the risk of unauthorized access.

13.4.4. User lock-out controls are implemented to prevent unauthorized access after a specific number of consecutive failed login attempts.

13.5. Security Procedures, Policies and Logging:

13.5.1. **Logging and Audit Trails**. Trackmedium maintains audit logs designed to record security-relevant events, including authentication events, authorization or role changes, administrative actions, and access to sensitive data functions. Logs are time-stamped, protected from unauthorized modification, and access to logs is restricted to authorized personnel. Logs are retained for a minimum of 90 days and are stored in a secure location to prevent tampering. Logs are reviewed as part of security monitoring and incident investigation activities.

13.5.2. **Time Synchronization**. Systems generating audit logs are configured to use synchronized time sources, where supported, to enable accurate event correlation.

14. **Information Security Program Changes**. Trackmedium regularly updates and enhances its Information Security Program, and may make changes to security controls, procedures, policies, and features to address evolving threats, changes in technology, changes in law, and operational needs. Trackmedium will not materially reduce the overall level of protection for Subscriber Data provided by the Information Security Program. Trackmedium may retire, replace, or modify specific controls and will maintain controls that are reasonably designed to provide a comparable level of protection overall. Trackmedium may update these Information Security Program Standards by posting a revised version at https://www.trackmedium.com/legal. Any such update will be effective as of the date of posting. Subscriber is responsible for reviewing the then-current version.

Proprietary to Trackmedium, LLC