



Information Security and Privacy Exhibit

Last updated: February 16, 2026

This Information Security and Privacy Exhibit is subject to the terms and conditions of the Portal26 SaaS Subscription Agreement (the "Agreement"). Capitalized terms not defined in this exhibit will have the meanings specified in the Agreement or the Order. We reserve the right to change the terms and conditions of this exhibit from time to time.

This Exhibit reflects Portal26's Information Security and Privacy policies and controls designed to protect Customer Data from accidental or unlawful destruction or accidental loss, alteration, unauthorized access, use, or disclosure, and against all other unlawful forms of processing as stipulated in this Exhibit. Portal26 may update and/or amend the underlying Information Security and Privacy policies, technology and procedures from time to time, but will not materially diminish the level of data protection provided.

1. Programs and Policies

Portal26 maintains an information security and privacy program, including administrative, technical, and physical measures for the governance and security of Portal26's relevant systems for the cloud hosting of Customer Data. Portal26's information and security program includes policies and controls for the privacy, security, availability, confidentiality, integrity, access and use of Customer Data in the Subscription Services being provided to Customer. Portal26 reviews and/or updates its policies at least annually.

2. Access Control

- a. Portal26 maintains an internal access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- b. Logical Security. Portal26 will:
 - i. employ a formal procedure for granting and revoking access and access rights to the Subscription Services;
 - ii. follow a separation of duties standard, a formal approval process and audit trail for all access requests;
 - iii. use password controls which include a minimum length, multi-factor authentication, alpha/numeric characters, and expirations; and
 - iv. control access to operating systems through a secure log-on procedure.
- c. Network Access: Portal26 will deploy the following network access controls for the Subscription Services:
 - i. industry standard authentication for network users;
 - ii. perimeter controls (including firewalls) designed to protect the Services from unauthorized logical access; and
 - iii. authentication methods to control access by remote users and multi-factor authentication and network intrusion detection for the remote access.
- d. Access communications or sessions are encrypted using no less than industry standard encryption. Remote access from non-Customer devices to Customer Data or Systems to use secure protocols.
- e. Portal26 will provide users only with the minimum access rights and privileges to the Subscription Services needed to perform a particular function or transaction.

3. Business Continuity Verification

Throughout the term of this Agreement, Portal26 will:

- a. Maintain business continuity and disaster recovery plans covering the Subscription Services.
- b. Document in written form, the business continuity and disaster recovery plans and will include details regarding the Subscription Services, the complexity of the environment and probability of occurrence.
- c. Review and, if necessary, update the business continuity and disaster recovery plans at least annually.
- d. Upon Customer's written request but not more than once in any twelve month period, provide Customer with the table of contents and a summary for the business continuity and disaster recovery plans.
- e. Perform business continuity exercises at least annually covering the Subscription Services.

4. Change Management

- a. Portal26 has change management practices in place and documented to ensure controlled and approved changes for systems relevant to the Subscription Services.
- b. Portal26 provides a clear and specified process for change management, as well as communication regarding any changes made to systems maintaining Customer Data.
- c. Portal26 has documented and follows a process for testing changes and updates to functionality and security before rollout to environments containing Customer Data.

5. Data Security

- a. Portal26 stores encryption keys used to protect Customer Data in a secure environment.
- b. Portal26 will logically segregate Customer Data from other customers' information.
- c. Portal26 will encrypt Customer Data at rest and in transit to Portal26 systems in situations in which the transmission is under Portal26's control.
- d. Portal26 will use industry standard secure encryption protocols in those situations in which it controls the transmission of Customer Data.
- e. Portal26 uses secure methods to gain access to information (to include but not limited to: login sessions, remote administration and troubleshooting) and electronically transferring Customer Data files within its control.
- f. Portal26 encrypts backups using an industry recognized secure encryption protocol.

6. Network and Application Security

- a. Portal26 will remediate all critical, high and medium penetration test issues in a timeframe commensurate with Industry Best Practices. "Industry Best Practice" means the exercise of methods and practices which would reasonably and ordinarily be expected to be used by a skilled and experienced Portal26 that provides the same or similar services.
- b. Portal26 will ensure that corrective or mitigating action is taken for all critical and high application and network vulnerabilities detected in a time frame commensurate with Industry Best Practices.
- c. For any relevant Internet facing Subscription Applications, Portal26 will implement web application and web services security controls commensurate with Industry Best Practices.
- d. Portal26 will routinely evaluate all relevant systems for necessity of anti-malware protection, and where applicable, will implement, and keep up-to-date, malware prevention software as needed.
- e. Portal26 will maintain a program to evaluate security patches and implement patches within commercially reasonable time limits.
- f. Portal26 annually performs penetration testing using independent third parties to proactively identify and remediate security flaws.

7. Vulnerability and Web Application Scanning Requirements

- a. Web Application Scanning: Portal26 will implement recurring network and web application vulnerability scans.
- b. Application Security Testing: Portal26 will perform secure code analysis to assess implemented security controls in Portal26 subscription services and identify potential security vulnerabilities in both internal and external networks or applications. Assessed vulnerabilities include, but are not limited to OWASP TOP 10, SANS Top 25, unauthenticated or unauthorized access to functionality (privilege escalation), cross Customer Data access and access to the underlying services through the application, server infrastructure, or network ports.
- c. Customer shall not perform any external third-party penetration testing of Portal26's environment without prior approval of, and coordination with, Portal26.

8. Logging and Monitoring

- a. Portal26 will perform logging of relevant applications, systems, and databases. Relevant logs will be monitored and reviewed by trained personnel. Logs will be archived for three (3) years. Examples of log types include, but are not limited to:
 - i. Application/System/Database Logs (such as authentication attempts to the application, changes to application configuration, and creation, modification, or deletion of application access)
 - ii. Operational Logs (such as Services failing, hardware issues/failures, out-of-bounds errors)
 - iii. Security Event Logs (logging may include failed authentication attempts, enabling/disabling services, privilege escalation, creating/modifying/deleting accounts).

9. Independent Verification (Security Certifications, Audits or Attestations)

- a. Portal26 has implemented the appropriate administrative, physical and technical safeguards to protect Customer Data and meet standards and State or Federal Laws or Regulations applicable to Portal26.
- b. As they become available, Portal26 will provide independent verification of its safeguards. Attestations such as a SOC 2 Type II report, or evidence of equivalent security controls will be provided annually upon request.

10. Security Incidents

If Portal26 becomes aware of any Security Incident, Portal26 will:

- (a) investigate the Security Incident; (b) notify Customer without undue delay and in any event within seventy-two (72) hours of becoming aware of the Security Incident, and provide Customer with detailed information about the Security Incident to the extent known at the time of notification, with updates as the investigation progresses; and (c) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. Customer agrees that Portal26's obligation to report or respond to a Security Incident under this Section is not and will not be construed as an acknowledgement by Portal26 of any fault or liability with respect to the Security Incident.

11. Physical Security Measures for Facilities and Data Centers

- a. Portal26 hosts systems comprising the solution with a public cloud provider, and relies on such cloud provider's physical security controls as it relates to the hosting environment.

12. Security Audits

Customer may audit Portal26's compliance with this Exhibit and relevant to the Subscription Services at Customer's sole expense no more than once per year, unless more frequent audits are required by laws applicable to Customer. Customer shall submit an audit plan at least 60 days in advance of the proposed audit, and Portal26 will work cooperatively with Customer to agree on a final audit plan. If the requested audit scope directly corresponds to an ISO 27001, SOC 2 Type II or similar audit report performed by a qualified third-party auditor within the prior twelve months, Customer shall accept those findings in lieu of a security questionnaire response by or audit of Portal26, unless additional scope in an audit or questionnaire is required by Customer to comply with legal or regulatory requirements, at which time a security questionnaire shall first be required prior to additional audit. Should Customer still require additional scope, not covered by a qualified third-party audit or security questionnaire, an audit under this Section may be conducted during regular business hours and may not unreasonably interfere with Portal26's business activities. Audits of Portal26's public cloud provider are limited to available documents. Customer may only use an audit report for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of the Agreement and each audit report shall remain the property of Portal26 and shall be treated as the Confidential Information of the parties under the terms of the Agreement. Portal26 shall have no obligation to remediate any findings from such audits except to the extent such findings demonstrate a material breach of Portal26's obligations under this Agreement.

13. Secure Coding Practices

Portal26 uses Secure Coding Practices and leverages industry standard practices such as the OWASP Software Assurance Maturity Model or equivalent. Portal26:

- a. Uses Secure Coding Practices in all relevant phases of the application development lifecycle.
- b. Includes security considerations in code reviews.

14. Software Security

- a. Portal26 implements protective measures (using current industry standard anti-malware detection tools) to safeguard software against viruses, worms, Trojan horses or other malware on systems relevant to the Services provided.
- b. Portal26's hosted and supplied applications, hardware, or operating systems, are regularly patched in accordance with Portal26's vulnerability management guidelines.

15. Information Security Awareness and Compliance Training

- a. Portal26 provides Information Security Awareness and/or Compliance training program for all employees accessing Customer Data.
- b. Employee training is provided at least annually.

16. Data Privacy

- a. Cross Border and Onward Data Transfer: Portal26 will treat all Customer Data in a manner consistent with the requirements of the Agreement.
- b. Portal26 will not disclose personal data to law enforcement unless required by law. If compelled to disclose personal data to law enforcement, Portal26 will use commercially reasonable efforts to notify Customer in advance of a disclosure unless legally prohibited, and will limit the disclosure to only that personal data specifically required by the legal demand.
- c. Upon Customer's written request, Portal26 shall reasonably support Customer in dealing with requests from individual data subjects and/or a supervisory authority with respect to the processing of personal data controlled by Customer.