Last Updated: April 24, 2026

TECHNICAL & ORGANIZATIONAL MEASURES

Zasio has implemented and will maintain the following Technical and Organizational measures to support its provision of Zasio Services under the Agreement. These measures are designed to ensure an appropriate level of security, considering the nature, scope, context, and purpose of the processing, and risks to individual rights and freedoms.

Because information security threats continuously evolve, Zasio will regularly improve its technical and organizational measures to address emerging risks. Any updates will maintain the same purpose and will not materially reduce the level of security provided in connection with Zasio Services.

These measures, together with Zasio's security commitments in the applicable Agreement to which this document is linked, represent Zasio's sole responsibility regarding the protection of Customer Data.

Capitalized terms not defined in this Exhibit have the meanings given in the Agreement.

1. **Security Program.** Zasio maintains a comprehensive written Information Security Management System (ISMS) to systematically protect both its own information and that of its customers. All security and privacy policies are (i) documented, (ii) approved by executive management, (iii) communicated to all personnel, and (iv) reviewed and updated at least annually.

2. **SOC 2, Type 2 Audit Report**. Zasio implements and maintains administrative, technical, and physical safeguards consistent with its most recent SOC 2, Type 2 report (or equivalent) issued by a qualified third-party auditor. A current copy of this report is available via Zasio's trust portal.

3. **Physical Security.** Zasio's facility is secured with electronic locks and monitored by web-enabled video surveillance. Visitor access is logged and requires escort by Zasio personnel. Outside of business hours, access is electronically restricted. Additional security controls protect sensitive areas, including accounting, server and network infrastructure, and executive offices.

4. **Logical Safeguards.** Zasio uses Windows Server 2016 & 2019 Active Directory to manage logical access to internal network resources. All personnel are assigned unique IDs and must use strong passwords, enforced through network policies. A company-managed commercial password vault is required for storing credentials. Password reuse is prohibited, and passwords for confidential systems must meet Microsoft's complexity standards unless infeasible. Clean desk and clear screen practices are enforced through HR policies.

   Remote access to Zasio's network is permitted only through IKEv2 VPN and solely on company-provided, authorized devices. Access is granted on an as-needed basis. All remote connections require encryption and two-factor authentication. VPN credentials are managed through Active Directory.

5. **Data Security.** Zasio's ISMS includes: (i) an annual risk assessment presented to executive management; (ii) annual tabletop exercise to test Zasio's Information Security Incident Response Plan; (iii) an internal audit program overseen by committee; and (iv) committee-led management of the overall information security program.

6. **Information Security Team**. Zasio's information security team includes representation from multiple business units, including in-house legal and certified professionals (e.g., CISM and data privacy certifications). The team maintains security controls, collaborates with executive leadership, and supports compliance with security-related policies and procedures.

7. **Data Center Security**. Zasio systems that process Customer Data are protected by the physical and logical safeguards in these Technical and Organizational Measures. SaaS applications, including hosted customer databases, are hosted by Microsoft Azure™. Microsoft's security and compliance measures are detailed at: https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all.

8. **Risk Management and Assessments**. Zasio maintains a written risk management policy that defines the methodology for identifying, assessing, and managing information security, strategic, and operational risks.

9. **Access Control Policy**. Zasio enforces a written access control policy that limits access to information, systems, and facilities to authorized personnel with a legitimate need to know.

10. **Vendor Management.** Zasio operates a vendor management program aligned with industry standards to ensure third-party suppliers meet contractual, security, and availability requirements. Vendor agreements include confidentiality and privacy obligations that support Zasio's compliance with its own security and privacy commitments.

11. **Secure Software Development Lifecycle**. Zasio follows a documented software development lifecycle policy that incorporates industry-standard security practices and privacy by design principles. The policy includes the OWASP Top 10 as a baseline and requires scanning all new releases and updates for open-source vulnerabilities, which are promptly remediated.

12. **Vulnerability Assessments**. Zasio's information systems infrastructure undergoes annual penetration testing. In addition, SaaS services undergo monthly web application scans. Pen testing and web scanning are performed by qualified third parties.

13. **Change Management**. Zasio maintains a formal change management program to plan, test, communicate, and implement changes affecting its SaaS services, systems, networks, and applications.

14. **Network Security**. Zasio uses industry-standard technologies and controls to secure its network, including firewalls, intrusion prevention, monitoring, network segmentation, and VPN and wireless security. Network architecture and controls are reviewed annually. A dedicated firewall/proxy appliance with enhanced security features enforces Zasio's network boundary policies. This includes: (i) traffic pattern monitoring to detect sensitive data; (ii) port blocking and automatic port scan prevention; (iii) advanced traffic analysis with cloud-based threat response; and (iv) DNS-level filtering to block malicious connections and protect users and systems.

15. **Malware Protection**: Zasio employs an industry-standard malware protection strategy designed to prevent and remediate virus outbreaks, attempts to gain unauthorized access, and other malware-related threats across its networks and connected services.

16. **Data Transfers**: Zasio's data management policy governs the protection of Customer Data entering its network. Non-sensitive data is transferred via SFTP. Sensitive data transfers follow restricted handling procedures to ensure secure transmission.

17. **Restricting Information Access**. Zasio applies the principle of least privilege to manage personnel access to information and systems. All personnel are contractually obligated to protect personal and confidential data.

18. **Background Checks and HR Practices**. Zasio conducts pre-employment background checks for all employees and may repeat them as needed. Access to software and servers is granted on an as-needed basis. Zasio follows industry-standard onboarding and offboarding procedures to ensure new hires are trained in their roles and security responsibilities, and that system access is promptly revoked upon departure. All employees are subject to Zasio's business ethics and code of conduct.

19. **Business Continuity and Disaster Recovery.** Zasio maintains a formal BC/DR plan to help ensure service resilience during extended outages. The plan is tested annually, including backups and procedures.

20. **Data Backup and Recovery**. Zasio follows a documented backup and recovery plan to help ensure regular backups and to define recovery time and recovery point objectives for unplanned outages.

    - **Hosting Facility Backups**. Each database and dedicated server undergoes daily point-in-time (hot) backups retained for two weeks and monthly backups retained for three months. Backup and recovery systems are tested regularly in accordance with industry standards.

    - **Internal Backups**. Major systems, including Active Directory, email servers, document repositories, production databases, and critical application servers are backed up weekly, with media rotated offsite to a secure location. Incremental backups of active document repositories occur every two hours.

    Both internal and hosted backup systems are tested at least annually.

21. **Information Security Incident Response Planning**. Zasio maintains a formal incident response plan that is activated in the event of any Information Security Incident or related event. Any breach is documented with a description, time period, consequences, reporter identity, and the recovery procedure.

22. **Data Segregation**. Zasio maintains separate hosted databases for each customer, with access permissions restricted to the associated customer. Internal production and test databases are also segregated to prevent unauthorized access to Personal Data.

23. **Encryption of Customer Data**. Zasio uses industry standard strong encryption to protect Customer Data both in transit and at rest. All mobile computing devices used to transmit or store Customer Data must be encrypted.

24. **Security Training**. Zasio provides security awareness training to all personnel upon hire and at least annually, with quarterly updates to reinforce key practices.

25. **Asset Management**. Zasio follows a formal IT asset management policy that includes real-time tracking of all IT assets and secure, industry-standard disposal procedures at the end of each asset's lifecycle.

26. **Customer Data Deletion**. Zasio maintains formal policies and procedures to help ensure timely deletion of Customer Data in accordance with contractual and legal obligations.

27. **Log Data**. Zasio operates a Security Information and Event management (SIEM) and anomaly detection program for SaaS services. Log data is retained for up to 1 year for purposes of conducting forensic analysis of security anomalies and incidents.