Plugilo Security and Reliability

Last Updated: February 2026

1. Our Commitment

Plugilo, Inc. ("Plugilo") is committed to maintaining commercially reasonable technical and organizational measures designed to protect the confidentiality, integrity, and availability of its systems and the data processed therein. This page provides an overview of Plugilo's security and reliability practices and may be referenced by Plugilo's contractual agreements, policies, and other documentation.

2. Scope

The practices described on this page apply to Plugilo's proprietary cloud-hosted solutions, related support services, professional services, and any data processed in connection therewith (collectively, the "Services"). Where Plugilo's contractual agreements with customers, partners, or other parties reference this page, the information provided herein forms part of the applicable contractual framework as specified in the respective agreement.

3. Confidentiality

3.1 Physical Access Controls

Plugilo implements measures to prevent unauthorized physical access to data processing facilities, including:

- Automated access control systems for all facilities housing data processing infrastructure
- Use of security locks and restricted-access zones
- Visitor policies requiring escort by authorized personnel at all times
- Careful vetting and selection of maintenance and cleaning staff
- Policies governing remote work environments, including the requirement to work in dedicated, separated workspaces where feasible and the prohibition of working on confidential matters in publicly accessible locations

3.2 System Access Controls

Plugilo employs the following measures to prevent unauthorized access to its data processing systems:

- User authentication with individual credentials (username and password)
- Two-factor authentication (2FA) for system access
- Deployment of anti-virus and anti-malware solutions
- Network protection through firewalls and intrusion detection systems
- Use of VPN technology for all remote access
- Encryption of data carriers and storage media
- Restriction of external interfaces (e.g., USB ports) where appropriate
- Automatic desktop/session locking after periods of inactivity
- Centralized management of user permissions and role-based access profiles
- Enforced password policies requiring strong, regularly rotated credentials
- Company-wide policies on data protection, secure passwords, data deletion/destruction, and clean desk practices

3.3 Data Access Controls

To ensure that only authorized personnel can access personal and confidential data, Plugilo maintains:

- Role-based access control applying the principle of least privilege
- Logging and auditing of access to applications, including creation, modification, and deletion of data
- Minimization of administrator-level accounts
- Secure storage of all data carriers
- Centralized administration of user rights by designated system administrators
- Policies limiting the printing and physical reproduction of data to what is strictly necessary

3.4 Separation of Processing

Plugilo ensures that data collected for different purposes is processed separately through:

- Physically and logically separated storage on distinct systems or data carriers
- Strict separation of production and test/development environments

4. Integrity

4.1 Transfer Controls

Plugilo ensures that data cannot be read, copied, altered, or removed without authorization during electronic transfer or storage, and that it is possible to verify recipients of data transfers. Measures include:

- Use of VPN tunnels for site-to-site and remote connections
- Encrypted wireless networks (WPA2 or higher with strong credentials)

- Logging of all data access and retrieval activities
- Provision of data exclusively through encrypted channels (e.g., SFTP, HTTPS/TLS)
- Maintenance of records of regular data retrieval and transmission processes
- Use of anonymization or pseudonymization where appropriate when transferring data

4.2 Input Controls

Plugilo maintains the ability to verify who has processed data, at what time, and in what manner through:

- Logging of data entry, modification, and deletion events
- Manual and automated review of audit logs
- Traceability of all data changes to individual user accounts (not group accounts)
- Clear assignment of responsibilities for data deletion processes

5. Availability and Resilience

Plugilo implements measures to protect data against accidental destruction or loss and to ensure continuous availability of the Services:

- **Physical safeguards:** Fire extinguishing equipment, fire and smoke detection systems, and surge protection in server rooms; no sanitary installations located in or above server rooms
- **Power continuity:** Uninterruptible power supply (UPS) systems
- **Data redundancy:** RAID systems and disk mirroring for critical storage
- **Backup and recovery:** Regular backups pursuant to a documented backup and recovery plan, with monitoring of backup processes and regular testing of data restoration procedures (results documented)
- **Disaster recovery:** Documented emergency and disaster recovery plans aligned with recognized standards
- **System architecture:** Separation of operating systems and data layers to limit the impact of incidents

6. Ongoing Review, Assessment, and Evaluation

6.1 Data Protection Management

Plugilo maintains an organizational framework to meet applicable data protection requirements, including:

- Use of a dedicated data protection management platform
- Appointment of a qualified Data Protection Officer

- Employee confidentiality obligations and regular data protection training
- Maintenance of a record of processing activities in accordance with applicable law

6.2 Incident Response Management

Plugilo maintains documented processes for responding to security and data protection incidents, including:

- Defined notification procedures for data breaches directed at supervisory authorities and affected individuals, in accordance with applicable legal requirements
- Involvement of the Data Protection Officer in all security incidents and data breaches
- Deployment of anti-virus software and firewall systems as part of the incident prevention and detection infrastructure

6.3 Privacy by Design and by Default

Plugilo integrates privacy considerations into the design and operation of its systems:

- Employee training on privacy by design and privacy by default principles
- Data minimization: only data that is necessary for the specific processing purpose is collected and processed

6.4 Subprocessor and Vendor Controls

Plugilo ensures that data processed on its behalf by subprocessors is handled in accordance with documented instructions:

- Written data processing instructions to all subprocessors (e.g., through data processing agreements)
- Verification of data destruction upon termination of subprocessor engagements
- Requirement that subprocessors obligate their own employees to data confidentiality
- Careful selection of subprocessors with particular regard to data security capabilities
- Ongoing monitoring and review of subprocessor activities and compliance

7. Cloud Infrastructure and Hosting

Plugilo's Services are hosted on commercially recognized cloud infrastructure providers. Plugilo selects providers that maintain robust security programs and evaluates their technical and organizational safeguards as part of its vendor management process. Where available, Plugilo reviews providers' independent audit reports and certifications as part of this evaluation.

Plugilo itself does not currently hold ISO 27001 or SOC 2 certifications. Plugilo's security program is based on commercially reasonable industry practices and is subject to ongoing internal review and improvement.

8. U.S. Market – Additional Information

8.1 U.S. Data Privacy

Plugilo processes data in accordance with applicable U.S. federal and state privacy laws, including, where applicable, the California Consumer Privacy Act (CCPA/CPRA), the Virginia Consumer Data Protection Act (VCDPA), and other state-level data protection statutes. Plugilo maintains internal procedures to respond to consumer rights requests (e.g., access, deletion, opt-out of sale) where required by applicable law.

8.2 Data Location

Data may be stored and processed in data centers located in the United States. Where data is transferred internationally, Plugilo ensures that appropriate safeguards are in place in accordance with applicable data protection laws.

8.3 U.S. Export Controls and Sanctions Compliance

Plugilo maintains controls designed to comply with applicable U.S. export control and sanctions laws, including the Export Administration Regulations (EAR) and programs administered by the Office of Foreign Assets Control (OFAC). Access to the Services is not permitted from U.S.-embargoed destinations.

8.4 Industry-Specific Requirements

Plugilo's Services are designed as general-purpose commercial software. Customers operating in regulated industries (e.g., healthcare, financial services) are responsible for evaluating whether the Services meet their specific regulatory requirements. Plugilo is available to discuss additional safeguards or contractual commitments on a case-by-case basis.

9. European Market – Additional Information

9.1 GDPR Compliance

Where Plugilo processes personal data subject to the General Data Protection Regulation (EU) 2016/679 ("GDPR"), Plugilo implements technical and organizational measures in accordance with Art. 32 GDPR. Details regarding Plugilo's data processing practices and the availability of a Data Processing Addendum are described in the applicable contractual agreement or may be requested at the contact address below.

9.2 International Data Transfers

Where personal data is transferred from the European Economic Area, Switzerland, or the United Kingdom to countries outside these jurisdictions, Plugilo ensures that appropriate transfer mechanisms are in place, such as Standard Contractual Clauses or other legally recognized safeguards.

10. Continuous Improvement

Plugilo regularly reviews and updates its security and reliability measures to account for evolving threats, changes in technology, and developments in applicable legal and regulatory requirements. Updates to this page will be reflected by the "Last Updated" date above.

11. Questions and Contact

For questions regarding Plugilo's security and reliability practices, please contact:

Plugilo, Inc. Email: legal@plugilo.com

This page is provided for informational purposes and may be referenced by Plugilo's contractual agreements, policies, and other documentation. In the event of any conflict between this page and the terms of an applicable agreement between Plugilo and a customer or partner, the terms of such agreement shall prevail.