Cloud Security Addendum

Last Updated: March 2022

ERP.Aero's Cloud Security Addendum ("Security Addendum") outlines the technical and procedural measures that ERP.Aero ("ERP" or "the Company") undertakes to secure the Cloud Service. ERP may change this Security Addendum from time to time and such changes will be effective when posted. Capitalized terms used but not defined in this Security Addendum have the meanings as set forth in the ERP Cloud Services Agreement or other written or electronic terms of a cloud service or cloud subscription agreement ("Agreement") entered into by the parties.

1. Customer Data Access and Management

1.1 Customer controls access to the Cloud Service via User IDs and passwords ("User Credentials") or an integration with Customer's Identity Provider (IDP). A User ID is a unique identifier Customer creates to establish an account for the Cloud Service.

1.2 For the purposes of data governance and data confidentiality, Customers should encrypt data prior to sending any data to ERP; in some cases, such encryption will be required, as further detailed in section 15.

1.3 ERP uses Content only as appropriate to provide the Cloud Service to Customer, as specified in the Agreement.

1.4 For Content that consists audit log message ("Message Content"), ERP shall store such Message Content in the Cloud Service production environment set by Customer in the Cloud Service.

1.5 Message Content is replicated by ERP and retained per Customer's specified retention periods set by Customer in the Cloud Service. Customers are expected to consume Message Content regularly and store Message Content in their data stores of choice for storage beyond the retention policy specified.

2. Encryption and Logical Separation

2.1 The Cloud Service stores Content encrypted at rest. This is done leveraging enterprise grade encryption standards employed on the storage backend.

2.2 Communications between Customer's endpoints and the Cloud Service are encrypted in-transit with appropriate encryption standards for data in motion.

2.3 The Cloud Service includes logical separation of data between customers. If purchased, the Cloud Service may be hosted on Customer-specific, dedicated cloud resources. In all cases, ERP has implemented controls designed to prevent one customer from gaining unauthorized access to another customer’s data.

3. ERP Service Infrastructure Access Management

3.1 Access to the systems and infrastructure that support the Cloud Service is restricted to individuals who require such access as part of their job responsibilities.

3.2 Unique User IDs are assigned to such individuals as part of their hiring and onboarding process.

3.3 The server password policy for the Cloud Service adheres to ERP password requirements and is in-line with industry recommendations.

3.4 Access privileges of terminated ERP personnel are disabled promptly. Access privileges of persons transferring to jobs requiring reduced privileges are adjusted accordingly.

3.5 ERP personnel access to the systems and infrastructure that support the Cloud Service is reviewed quarterly.

3.6 Cloud provider firewall or firewall-equivalent controls have deny-all default policies and only enable appropriate network protocols for egress and ingress network traffic.

3.7 Appropriate security measures are utilized for remote administration point of access to the Cloud Service production environment.

4. Risk Management

4.1 ERP maintains a risk management program based on industry guidance.

4.2 ERP conducts risk assessments of various scope throughout the year, including self and third-party assessments and tests, automated scans, and manual reviews.

4.3 Results of assessments, including formal reports as relevant, are reported to the head of the ERP Security Committee (“Security Committee”). The Security Committee meets biannually to review reports, to identify control deficiencies and material changes in the threat environment, and to make recommendations for new or improved controls and threat mitigation strategies to executive management.

4.4 Changes to controls and threat mitigation strategies are evaluated and prioritized for implementation on a risk-adjusted basis.

4.5 Threats are monitored through various means, including threat intelligence services, vendor notifications, and trusted public sources.

5. Vulnerability Management and Penetration Testing

5.1 Vulnerability mitigation is a part of every ERP engineer's responsibilities.

5.2 The latest applicable patches and updates are applied promptly after becoming available and being tested in the Cloud Service's pre-production environments.

5.3 Potential impacts of vulnerabilities are evaluated by ERP engineers.

5.4 Vulnerabilities that trigger alerts and have published exploits are reported to Security leadership, which determines and supervises appropriate remediation action.

5.5 Security Operations monitors or subscribes to trusted sources of vulnerability reports and threat intelligence.

5.6 Penetration tests by independent third parties are conducted at least annually. Detailed results from external penetration tests are not distributed or shared with anyone other than ERP employees with a need to know. Redacted summaries are available with appropriate non-disclosure agreements in place.

6. Remote Access & Wireless Network

6.1 All access to the Cloud Service networks requires authentication through an encrypted connection such as SSH, MFA, using regular-rotated SSH keys, and never passwords.

6.2 ERP corporate offices, including LAN and Wi-Fi networks in those offices, require successful authentication in addition to authentication to public cloud provider accounts for access.

6.3 ERP maintains a policy of not storing Content processed by the Cloud Service on local desktops, laptops, mobile devices, shared drives, removable media, as well as on public facing systems that do not fall under the administrative control or compliance monitoring processes of ERP.

7. Cloud Service Location

7.1 ERP stores Message Content in the available AWS Cloud Service region(s).

8. System Event Logging

8.1 Monitoring tools and services are used to monitor systems including network, server events, availability events, resource utilization, and other security events of interest.

8.2 ERP infrastructure security event logs are collected in a central system and stored using appropriate security measures designed to prevent tampering. Logs are stored for twelve months.

8.3 ERP security events of interest are reviewed for malicious or inappropriate activity.

9. System Administration and Patch Management

9.1 For ERP-managed systems that access Content, ERP creates, implements, and maintains system administration procedures that meet or exceed industry standards, including without limitation, system hardening, system and device patching (operating system and applications), and proper installation of threat detection solution with daily signature updates.

9.2 ERP's security team reviews US-CERT new vulnerabilities announcements weekly and assesses their impact to ERP based on ERP-defined risk criteria, including applicability and severity.

9.3 Applicable US-CERT security updates rated as "high" or "critical" are addressed within thirty days of the patch release.

10. ERP Security Training and ERP Personnel

10.1 ERP maintains a security awareness program for ERP personnel, which provides initial education, ongoing awareness, and individual ERP personnel acknowledgment of intent to comply with ERP's corporate security policies. New hires complete initial training on security, sign a proprietary information agreement, and digitally sign the information security policy that covers key aspects of the ERP information security policy.

10.2 All ERP personnel acknowledge they are responsible for reporting actual or suspected concerns, thefts, breaches, losses, and unauthorized disclosures of or access to Message Content.

10.3 All ERP personnel are required to satisfactorily complete security training annually.

11. Physical Security

11.1 The Cloud Service is hosted in AWS, GCP, and other public clouds. Therefore, all physical security controls are managed by the applicable public cloud provider. Annually, ERP reviews the applicable security and compliance reports of the public cloud providers it uses to ensure appropriate physical security controls, including:

11.1.1 Visitor management including tracking and monitoring physical access;

11.1.2 Physical access point to server locations are managed by electronic access control devices;

11.1.3 Monitor and alarm response procedures;

11.1.4 Use of CCTV cameras at facilities;

11.1.5 Video capturing devices in data centers with ninety days of image retention;

11.1.6 Environmental and power management controls; and

11.1.7 Removal and destruction of physical media including drives.

12. Notification of Security Breach

12.1 ERP will notify Customer in writing within seventy-two (72) hours of confirmed unauthorized access to Message Content (“Security Breach”).

12.2 Such notification will summarize the known details of the Security Breach and the status of ERP’s investigation.

12.3 ERP will take appropriate actions to contain, investigate, and mitigate any such Security Breach.

13. Availability and Disaster Recovery

13.1 ERP maintains a Disaster Recovery Plan (DRP) for the Cloud Service. The DRP is tested annually.

13.2 Disaster recovery strategies may cover recovery of authentication and authorization data comprising account, user information, and data being sent to and stored within the Cloud Service infrastructure. ERP's DRP covers Customer's account and user information. To cover data being sent to and stored within the Cloud Service infrastructure, Customer is responsible for ensuring that it implements a service level that corresponds with Customer's disaster recovery strategy.

Each of the cloud platform providers, such as AWS, Azure, and GCP, offers inbuilt disaster recovery solutions, which Customer is responsible for employing as part of Customer's disaster recovery strategy.

14. ERP Security Compliance, Certifications, and Third-party Attestations

14.1 ERP hires accredited third parties to perform audits and to attest to various compliance standards and certifications annually including:

14.1.1 CSA Star Level 1 Attestation; and

14.1.2 ISO 27001 Certification; and

14.1.3 Payment Card Industry Data Security Standards ("PCI-DSS") – ERP can support PCI data that is message-level encrypted by Customer.

14.2 ERP's Security page (https://www.erp.aero/compliance) provides more information about ERP's compliance certifications and a portal for requesting supporting documentation.

15. Additional Customer Responsibilities

15.1 Customer is responsible for managing and securing User Credential(s) within the Cloud Service and for protecting its own resources used to send Content to the Cloud Service.

15.2 Customer will immediately notify ERP if a User Credential has been compromised or if Customer suspects possible suspicious activities that could negatively impact the security of the Cloud Service or Customer's account.

15.3 Customer may not perform any security penetration tests or security assessment activities without the express, prior written consent of ERP's Chief Information Security Officer.

15.4 ERP has implemented reasonable security measures designed to prevent unauthorized access to and accidental loss of data uploaded to our service as described in this Security Addendum. ERP does not, however, guarantee that its reasonable security measures will prevent all unauthorized third parties from obtaining access to Content.

15.5 Customer shall not transmit cardholder or sensitive authentication data (as those terms are defined in the PCI DSS standards) unless such data is message-level encrypted by Customer.

15.6 Customer is responsible for ensuring a level of data protection commensurate with the sensitivity of the Message Content it uploads to the Cloud Service including, without limitation, an appropriate level of message-level encryption.

15.7 Customer is responsible for managing a backup strategy regarding Message Content.