



## INFORMATION SECURITY ADDENDUM

This Information Security Addendum (ISA) is supplemental to and is incorporated by reference into the Agreement between the Emburse and Client. Unless otherwise set forth below, capitalized terms not in this ISA, shall have the meaning set out in the Agreement.

### GOVERNANCE

#### *Information Security Team*

Emburse has a dedicated Information Security Team consisting of Security Engineering, Security Operations, Security Programs, and IT Governance, Risk and Compliance (GRC) professionals. Emburse's Information Security takes an integrated, risk-based approach to security, leveraging automation and tools for continual evaluation of risk and compliance for new developments. Emburse's security and privacy program is certified as ISO 27001 and ISO 27701 compliant. A company-wide security risk assessment is conducted annually with risks associated with the appropriate risk owner for remediation or acceptance. These are maintained within our annual risk assessment. All identified risks are treated as appropriate. Other certifications dependent on service include SOC1 type II, SOC2 type II, PCI-DSS, and Tx-RAMP.

#### *Policies, Plans, and Standards*

Emburse has documented policies to meet the recommendations of the ISO 27001 and ISO 27701 standards. Emburse Information Security Policies are reviewed at least annually or as a significant change occurs to ensure its continuing suitability, adequacy and effectiveness. In conjunction with its data center hosting providers, Emburse covers the critical security and privacy areas: physical security, network infrastructure, security operations and data handling.

- Physical security includes locking down and logging all physical access to our data centers.
- Network infrastructure provides the availability guarantees backed by our SLAs.
- Operational security involves creating business processes and policies that follow security best practices to limit access to confidential information and maintain tight security.
- Data Handling provides guidance on handling customer and employee data.

#### *Emburse Information Security Policies*

- ISPOL01: Information Security
- ISPOL02: Acceptable Use

- ISPOL03: Data Handling
- ISPOL04: Password
- ISPOL05: Messaging & Collaboration
- ISPOL06: Cryptography & Encryption
- ISPOL07: Third Party
- ISPOL08: Network Security
- ISPOL09: Physical Security
- ISPOL10: Data Retention
- ISPOL11: Cyber Resiliency
- ISPOL12: Access Management
- ISPOL13: Asset Management
- ISPOL14: Equipment Disposal
- ISPOL15: Secure Application Development
- ISPOL16: Infrastructure Hardening
- ISPOL17: Change Control

### *Security Plans, Standards, and Guidelines*

- ISPR01: Security Incident Response Plan
- Emburse Business Continuity Plan
- ISDRP01: Information Security Disaster Recovery Plan
- ISTND01: Cryptography and Encryption Standard
- ISGDL01: Security Awareness Guideline
- Password Guideline

## **ACCESS CONTROL**

### *Standards*

Emburse maintains strong access control policies that apply to employee access to all production environments. The control processes include, but are not limited to:

- Strict password complexity requirements
- Use of the Principle of Least Privilege and Segregation of Duties
- Unique user identification and authentication
- Account provisioning and deprovisioning processes
- Secure, encrypted remote access
- Multi-factor authentication

### *Authentication*

Emburse solutions provide integrations with Single Sign On (SSO), it is recommended customers utilize SSO configured with multi-factor authentication. This can be configured in the Emburse Sign-in administrative options and your SSO provider's configuration. This best of breed deployment configuration allows configuring strong authentication to Emburse and allows consistent provisioning, operating and monitoring of Emburse along with other corporate applications.

## DATA HANDLING AND PRIVACY

### *Data Classification*

Emburse has implemented information classification to handle data as securely as possible. Based on its sensitivity, information is classified and labeled into the following three categories:

**Highly Confidential:** Information that is intended for specific individuals, with a high risk of financial loss or damage to the company's reputation if unauthorized disclosure or access occurs.

**Confidential:** Information that is intended for limited distribution, with risk of financial loss or damage to the company's reputation if unauthorized disclosure or access occurs.

**Public:** Information that is publicly available and/or intended for public dissemination.

### *Data Processing*

Please refer to our Data Processing Agreement for how Emburse will process data on behalf of our customers.

### *Personally Identifiable Information (PII)*

All PII data stored in Emburse applications are retained and used only for the purposes of giving the users the intended service of the system. The information is not reused or sold for other purposes. The information is treated in accordance with authorized data storage plans and off-site storage of the data is managed appropriately as such. Access to PII data is limited to "need to know" employees for authorized purposes only. Storage of PII assets is limited to necessary length of time for purposes of intended workflows. Assets are limited to necessary data elements. Physical access to PII is restricted by the hosting provider's secure data center environment and proper network and hardware/software protections. There is to be no downloading, printing or otherwise storing PII assets on devices other than approved Data Center assets. Disabled user accounts cannot access PII data. An account lockout threshold is enforced that assists with blocking unauthorized access to PII data. Access to PII data is restricted to appropriate users based on Authorization rules and system roles. Emburse Does not collect or store IP addresses, and therefore IP addresses should not be included on the list. Specifically, Emburse's marketing department does not collect IP addresses, and the product does not collect IP addresses nor store IP addresses. The product references only a portion of a user's IP address (the class C subnet) with an irreversible hash, and so Emburse is not able to regenerate the user's IP address.

Emburse services do not collect Sensitive Personal Information (SPI) as defined by GDPR Article 9 or Protected Health Information (PHI) as defined by HIPAA. It is our customers

responsibilities to only provide data that is to be used in our services provided.

Emburse is the data processor and will act in accordance with processing the data based on the agreements and communication from the data controller.

## ENCRYPTION

### *General Standards*

- Employee Laptops - full disk AES-256 encryption
- Customer data - fully encrypted AES-256
- TLS - default is TLS 1.2 or stronger

Emburse enforces our general encryption standards utilizing our cloud service provider encryption tools (AWS, Azure, GCP).

### *Customer Databases*

Emburse uses the multi-tenant model. With Emburse, each tenant is identified by a unique customer identifier within all systems. Each customer is given the same application code but with customer-specific configuration options that adapt the application to their own needs.

Each tenant is served using a single common instance, with configurable metadata specific to them, that is applied at run time to give each customer a unique user experience.

Customers access a load-balanced farm of multiple instances with configurable metadata and data isolation where the data of each customer is kept completely separate from all other customers. Emburse employs the Shared Database Separate Schema methodology (i.e., all client data is stored in a shared database and schema and data are separated by SQL query filters).

Emburse has structured our applications to support the operational requirements of maintainability, scalability and security by using multiple tiers. Tiers are physically partitioned from each other in separate network segments, which isolate them and provide greater security. These tiers are the 1) web layer, 2) application layer and 3) database layer.

Communications between the segments are encrypted and only permitted across limited channels. Emburse performs regular penetration tests to assure the isolation is intact

### *Key Management*

Emburse provides full AES 256-bit encryption at rest. Keys are stored securely and rotated on expiration. Emburse employees who are responsible for managing keys sign Key Custodian agreements that outline the key management responsibilities.

## NETWORK SECURITY

### *Segmentation*

Emburse has structured our applications to support the operational requirements of maintainability, scalability and security by using multiple tiers. Tiers are physically partitioned from each other in separate network segments, which isolate them and provide greater security. These tiers are the 1) web layer, 2) application layer and 3) database layer. Communications between the segments are encrypted and only permitted across limited channels. Emburse performs regular penetration tests to assure the isolation is intact.

### *Firewalls*

Emburse employs stateful firewalls at the edge and host-based firewalls on the interior. Emburse and our hosting environments provide logical and physical security for the service and its related systems, including firewalls, load balancers, routers, network switches and operating systems.

Our cloud service providers (AWS and Azure) offer Emburse with the flexibility to place instances and store data within multiple geographic regions, as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone, meaning availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by region).

In addition to discrete uninterruptible power supply (UPS) and onsite backup generation facilities, availability zones are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

Emburse has architected our cloud environments to take advantage of multiple regions and availability zones. Distributing applications across multiple availability zones provides the ability to remain resilient in the face of failure, including natural disasters and system failures.

### *Data Segregation*

Emburse customer instances are logically separated and attempts to access data outside allowed domain boundaries are prevented and logged. Significant measures are in place to ensure executable uploads, code, or unauthorized actors are not permitted to access unauthorized data - including one customer accessing files of another customer. Emburse's access control policies are based on the principles of "least privilege" and "segregation of duties." Segregation is enforced through role-based access control (RBAC) policies and technical controls. Emburse maintains four environments:

1. Production
2. UAT
3. Internal QA (staging)
4. Development Engineers are not permitted access to any production environments, including UAT.

Engineers are not permitted access to any production environments, including UAT.

## PLATFORM HARDENING

Emburse uses infrastructure as code to have consistent platform hardening in place with industry security standards. Only the necessary functionalities are enabled. Logging and monitoring are in place.

### *Vulnerability Scanning and Penetration Testing*

Emburse runs vulnerability scanning at least monthly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades). Annual penetration testing, by an approved and independent third party.

We perform penetration testing on network infrastructure and applications at least annually and after any significant infrastructure or application upgrade or modification (e.g., operating system upgrade, sub-network added to environment, web server added to environment).

Network segmentation is conducted twice per year for PCI environments.

Penetration Test Results Executive Summary are available on request subject to NDA.

In addition, Emburse has a private Bug Bounty program. Emburse and the security of the platform are tested on a continuous basis.

### *Web Application Firewall*

Emburse has deployed and manages an Web Application Firewall (WAF), in addition to the network-based firewalls. This additional security control prevents many known attack patterns.

### *Endpoint Protection: Malware and Antivirus*

Emburse has deployed endpoints protections through the use of the anti-malware and Intrusion Detection (IDS) software across all Emburse systems. Malware detection runs continuously and comprehensive scans are done on a regular basis. Emburse has implemented CrowdStrike for workstation and windows server protection and has contracted

incident response for anomalous activity. Networks and emails are monitored for illicit file movement and movement of confidential data. Anti-virus and anti-malware are installed on all workstations and servers.

## **PATCHING AND VULNERABILITY MANAGEMENT**

### *Patching*

We follow an agile development model with system updates deployed every two weeks. These biweekly updates install without downtime and with minimal impact to end users. These updates include patches and bug fixes, as well as new product functionality and system performance tuning.

Critical vulnerabilities are patched in 14 days. High vulnerabilities are patched within 30 days. Medium vulnerabilities are patched within 90 days.

### *Vulnerabilities*

Emburse uses scanners to monitor the production environment for vulnerabilities and misconfigurations. Vulnerability scans are performed regularly. Newly discovered security vulnerabilities are assessed, mitigated and remediated based on impact. The Security and Operations team meets weekly to review new Common Vulnerabilities and Exposures (CVE) across all systems in the environment.

Emburse participates in a Bug Bounty program. Findings disclosed by security researchers are assessed, mitigated and remediated based on impact.

Emburse Information Security Team members regularly monitor threat feeds, vulnerability platforms or databases, and other security information sources for up-to-date information on emerging threats, vulnerabilities, and exploits.

## **CHANGE AND RISK MANAGEMENT**

### *Change Management Policy and Process*

Emburse change management processes apply to changes made to the platform and infrastructure. The process requires, but is not limited to:

- Developers are identified and authorized
- Source code changes are reviewed and approved
- Source code changes pass testsRoll-back procedures exist
- Segregation of duties in deployment
- Logically separated development, staging, and production environments

- All changes are logged
- Emergency changes require approval

### *Security Reviews*

Emburse conducts regular security stakeholder review meetings on a regular basis to discuss and track potential or active risks related to the business.

### *Third Party Risk: Vendor and Partner Management*

Emburse performs a risk analysis on third-party service providers. Emburse senior management recognizes that secure, dependable relationships with third parties are necessary to support the company's products and services. These policies and procedures apply to third parties regardless of the country in which they are based or from where the services are provided.

Senior management further recognizes that third-party relationships present potential risks that must be properly managed, beginning with a sound due diligence process at the outset and continuing with annual or more frequent reviews of all third-party relationships. The extent of risk varies with each third-party relationship; among the most common third party-related risks are lack of third-party oversight by senior management, which could result in the company experiencing operational risks, privacy risks and reputation risks.

Senior management recognizes that it is ultimately responsible for identifying and controlling the risks arising from such relationships, to the same extent as if they were handled within the company. The security review and threat modeling can include, but is not limited to:

- Reviews of data flow or technical diagrams
- Risk assessments related to data handling and measures taken to protect data
- Other third-party integrations
- Compliance reporting
- Access controls and requirements
- Penetration testing results
- Hosting models
- Sandbox testing or security testing performed by Emburse's Information Security Team

### *Sub-Processors*

Emburse uses sub-processors to support our business, please refer to the DPA (section 3) and Sub-Processor Letter for more information.

### *Security Awareness & Privacy Training*

All Emburse employees are required to complete Security Awareness training on hire and every year thereafter. The training includes data privacy and governance, data protection, confidentiality, social engineering, password policies, and overall security responsibilities



inside and outside of Emburse. As part of the Security Awareness a privacy training, employees must acknowledge completion and accept their part of maintaining the overall security and privacy of Emburse.

Developers are trained annually, so as to maintain knowledge of the OWASP Top 10 for secure code development. Finally, Emburse conducts regular phishing tests. Those who click on a simulated phishing email are to take remedial training.

## **RESILIENCY: INCIDENT RESPONSE, BCP, AND DR**

### *Incident Response*

Emburse's Incident Response Policy encompasses four principal phases: 1) preparation, 2) detection and analysis, 3) containment, eradication and recovery and 4) post-incident activity. When an incident is suspected, the appropriate resources are dedicated to validation and remediation. Depending on who reported the issue and how it is handled, the responsibility for remediation will lie with either the Emburse support or operations teams.

The Security Incident Response Team (SIRT) Lead acts as the coordinator in response to all major security-related incidents or weaknesses. A major security incident or weakness is considered to be an impact to confidentiality (e.g., exfiltration of encryption keys), integrity (e.g., unanticipated data leakage or exfiltration), or availability (e.g., severe degradation of performance). The Incident Response Team Lead is responsible for assigning staff to work on specific tasks of the incident handling process and coordinating the overall incident response.

All personnel involved in incident response and remediation are responsible for providing any needed information to members of the Incident Response Team. Any directives given by a member of the Security Incident Response Team may supersede the specifics of this policy.

### *BCP/DR*

Emburse conducts a business risk analysis annually to evaluate and determine critical business processes and systems for all business functions. This includes an inventory of critical systems, measuring the overall potential operational impact of critical system disruption and assigning an appropriate RTO and RPO metric based on that criticality. All backups are encrypted.

The detection of a disruption or disaster that could affect Emburse operations or application services is the responsibility of the Security Incident Response Team (SIRT). The specific responsibilities of the SIRT and associated groups are outlined in our ISO-certified Business Continuity Plan.

The SIRT is automatically updated through monitoring services that provide notifications through email and phone. When a disruption or disaster occurs, the on-call SIRT member immediately makes an assessment of affected services. If necessary, they initiate the Disaster Recovery Plan and notify the other members of the Disaster Recovery Team (DRT).

### *Tabletop*

Emburse conducts an annual tabletop exercise with a cross-functional group of employees from all departments of the organization. This annual event is structured to test the readiness of the team for response to a production event. The exercises require participants to test, record, and simulate response activities in the event that the tabletop was an actual emergency. An after action review and lessons learned are conducted to ensure continuous improvement.

### *Resiliency Policy*

Emburse Resilience Policy governs and enforces processes including, but not limited to:

- Backup scheduling and monitoring
- System restoration
- Encryption in transit and at rest
- Engineering responsibilities

Emburse customer content and data are highly available and backed up daily. Any data at rest and in transit is encrypted. Logging is enabled to track backup status. Emburse backs up to a segmented, independent cloud account and is kept unavailable (offline) to the rest of production systems and engineers.

### *Monitoring and Alerting*

Emburse performs 24x7x365 monitoring of the Emburse infrastructure and environments. Automated monitoring and alerting for performance (e.g. uptime, CPU, memory, disks) and security is in place and monitored.

Monitoring for misuse is performed across all production infrastructure to detect and alert suspicious activity or changes to critical infrastructure.

### *RTO/RPO*

Emburse strives to keep services up and running; however all SaaS companies suffer occasional disruptions and outages. Recovery time objectives (RTO) and recovery point objectives (RPO) are tied to specific processes, not general availability of the entire platform. These metrics are evaluated annually during Emburse business risk analysis. Emburse maintains near-real time backups, therefore, the general RPO is measured in minutes.

## COMPLIANCE

### *Emburse*

Emburse and its subsidiaries are compliant with multiple security and compliance frameworks including SOC1, SOC 2, ISO 27001, and PCI-DSS. (Note: specific compliance attestations differ per Emburse services)

SOC 1, Many of Emburse's subsidiaries have been audited by a third-party and have achieved certified SOC 1 compliance. The report is available under NDA for customers or prospective customers to review. SOC 2, Many of Emburse's subsidiaries have been audited by a third-party and have achieved certified SOC 2 compliance. The report is available under NDA for customers or prospective customers to review.

ISO 27001, Many of Emburse's subsidiaries have been audited by a third-party and has achieved certified ISO 27001 security compliance. The certificate of registration is available under NDA for customers or prospective customers to review.

ISO 27701, Many of Emburse's subsidiaries have been audited by a third-party and has achieved certified ISO 27701 privacy compliance. The certificate of registration is available under NDA for customers or prospective customers to review.

PCI-DSS, Many of Emburse's subsidiaries have been audited by a third-party and have achieved PCI-DSS compliance. The certificate of registration is available under NDA for customers or prospective customers to review.

GDPR and Schrems II Ruling, Emburse's Privacy Policy and GDPR Data Privacy information can be found here: <https://www.emburse.com/privacy-policy>

Data Privacy Framework, Emburse is compliant with the US-EU-UK-Swiss Data Privacy Framework.

### *Amazon Web Services*

AWS compliance can be found here: <https://www.atlas.aws/>

### *Microsoft Azure*

Azure compliance can be found here: <https://learn.microsoft.com/en-us/azure/compliance/>