Contents

The following document contains all aspects of the Rehearsal security policy. For further details, please contact us directly.

Overview

As a company that takes data security and privacy very seriously, we recognize that Rehearsal's information security and data privacy practices are important to you. While we don't like to expose too much detail around our practices (as it can empower the very people we are protecting ourselves against), we have provided some general information below to give you confidence in how we secure the data entrusted to us. We adhere to this principle: When storing and transmitting data, we must ensure a high level of data protection and data security. That goes for information pertaining to our customers, prospects, business partners and employees. Because data protection is people protection.

For that reason, we view it as our duty to comply with the various legal regulations around the world that govern the collection and processing of personal data. Our top priority is to ensure universally applicable, worldwide standards for handling personal data. For us, protecting the personal rights and privacy of each and every individual is the foundation of trust in our business relationships.

Our corporate data protection, data privacy, and data security policies lay out strict requirements for processing personal data pertaining to customers, prospects, business partners and employees. It meets the requirements of the EU General Data Protection Regulation and ensures compliance with the principles of national and international data protection laws in force all over the world. The policies set a globally applicable data protection and security standard for our company.

Information Security Policy

Rehearsal maintains a written Information Security policy that defines employee's responsibilities and acceptable use of information system resources. The organization receives signed acknowledgement from its employees indicating that they have read, understand, and agree to abide by the rules of behavior, before providing authorized access to Rehearsal information systems and/or the Rehearsal platform and infrastructure. This policy is periodically reviewed and updated as necessary.

Our security policies cover a wide array of security related topics ranging from general standards with which every employee must comply, such as account, data, and physical security, to more specialized security standards covering internal applications and information systems.

Organizational Security

Information security roles and responsibilities are defined within the organization. The security team focuses on information security, global security auditing and compliance, as well as defining the security controls for protection of the Rehearsal infrastructure. The security team receives information system security notifications on a regular basis and distributes security alert and advisory information to the organization on a routine basis after assessing the risk and impact as appropriate.

Application Security

Account passwords are hashed. Our own employees cannot view them. If you lose your password, it can't be retrieved—it must be reset. All login pages (from our website and mobile app) pass data via TLS. Login pages and logins via the Rehearsal API have brute force protection. We engage a third party to perform regular external security penetration tests at least annually. The tests involve high-level server penetration tests, in-depth testing for vulnerabilities inside the application, and social engineering drills.

Asset Management

Rehearsal's data and information system assets are comprised of customer and end-user assets as well as corporate assets. These asset types are managed under our security policies and procedures. Rehearsal authorized personnel who handle these assets are required to comply with the procedures and guidelines defined by Rehearsal's security policies.

Personnel Security

Rehearsal employees are required to conduct themselves in a manner consistent with the company's guidelines, including those regarding confidentiality, business ethics, appropriate usage, and professional standards. All newly hired employees are required to sign confidentiality agreements and to acknowledge the Rehearsal code of conduct policy. The code outlines the company's expectation that every employee will conduct business lawfully, ethically, with integrity, and with respect for each other and the company's users, partners, and competitors. Processes and procedures are in place to address employees who are on-boarded and off-boarded from the company. Employees are provided with security training as part of new hire orientation and on at least an annual basis.

Physical and Environmental Safety

All of our information systems and infrastructure are hosted in Amazon's world-class data centers that are geographically dispersed to provide high availability and redundancy to Rehearsal's and its customers. The standard physical security controls implemented at each data center include electronic card access control systems, fire alarm and suppression systems, interior and exterior cameras, and security guards. Physical access is centrally managed and strictly controlled by data center personnel. All visitors and contractors are required to present identification, are required to log in, and be escorted by authorized staff through the data center. Servers have redundant internal and external power supplies. Data centers have backup power supplies and can draw power from diesel generators and backup batteries. For further information on the AWS data-center controls, please see https://aws.amazon.com/compliance/data-center/controls/.

Independent Audits and Certifications

The AWS data centers have completed a plethora of audits and certifications, including Service Organization Controls (SOC) 2 Type II audits. For further information on the AWS data-center certifications, programs, reports, and attestations, please refer to: http://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

Change Management

Rehearsal maintains a change management process to ensure that all changes made to the production environment are applied in a deliberate manner. Changes to software, operations systems, information systems, network devices, and other system components, and physical and environment changes are monitored and controlled through a formal change control process. Changes are reviewed, approved, tested and monitored post-implementation to ensure that the expected changes are operating as intended.

Change Management ensures that proposed changes that impact production environments are reviewed, tested, authorized, implemented, communicated and released in a controlled manner; and that the status of each proposed change is monitored to completion or retraction.

Auditing and Logging

We maintain audit logs on systems. These logs provide an account of which personnel have accessed which systems. Access to our auditing and logging tool is controlled by limiting access to authorized individuals on a least-privilege basis. Security events are logged, monitored, and addressed by trained security team members.

Organizational responsibilities for responding to events are defined. Security events that record critical system configuration changes and administrators are alerted at the time of change. Retention schedules for the various logs are defined in our security control guidelines.

Antivirus and Malware Protection

Antivirus and malicious code protection are managed and configured to retrieve the updated signatures and definitions available. Malicious code protection policies automatically apply updates to these protection mechanisms. Anti-virus tools are configured to run scans, virus detection, real-time file write activity and signature file updates. All Amazon instances, workstations, and laptops run such protections.

System Backups

Rehearsal has backup standards and guidelines and associated procedures for performing backup and restoration of data in a scheduled and timely manner. Controls are established to help safeguard backed up data (onsite and off-site). Periodic tests are conducted to test whether data can be safely recovered from backup devices.

Network Security

Our infrastructure servers reside behind high-availability firewalls and are monitored for the detection and prevention of various network security threats. Firewalls are utilized to help restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need.

Rehearsal maintains separate development, testing, staging, and production environments. Our firewalls provide adequate network segmentation through the establishment of security zones that control the flow of network traffic. These traffic flows are defined by strict firewall security policies. Automated tools are deployed within the network to support near-real-time analysis of events to support of detection of system-level attacks.

Data Protection

Rehearsal continually works to develop products that support the latest recommended secure cipher suites and protocols to encrypt traffic while in transit. We monitor the changing cryptographic landscape closely and work to upgrade our products to respond to new cryptographic weaknesses as they are discovered and implement best practices as they evolve. Data at rest is also encrypted with strong types of generally-accepted, non-proprietary encryption algorithms.

We apply a common set of personal data management principles to customer data that we may process, handle, and store. We maintain policies and procedures which limit the collection and use of personal data to the minimum necessary for our business purposes and as otherwise may be limited by applicable law. We protect personal data using appropriate physical, technical, and organizational security measures. Any non-public information Rehearsal may process, handle or store is encrypted at rest. We give additional attention and care to sensitive personal data and respect local laws and customs, where applicable.

Customer data is logically segregated within the Rehearsal multi-tenant architecture. Customer data is never used for application testing.

Rehearsal only processes personal information in a way that is compatible with and relevant for the purpose for which it was collected or authorized in accordance with our privacy policy. We take all reasonable steps to protect information we receive from our users from loss, misuse or unauthorized access, disclosure, alteration and/or destruction.

Vulnerability Management

Security assessments are done to identify vulnerabilities and to determine the effectiveness of the patch management program. Each vulnerability is reviewed to determine if it is applicable, ranked based on risk, and assigned to the appropriate team for remediation.

Patch Management

Rehearsal strives to apply the latest security patches and updates to operating systems, applications, and network infrastructure to mitigate exposure to vulnerabilities. Patch management processes are in place to implement security patch updates as they are released by vendors. Patches are tested prior to being deployed into production.

Secure Network Connections

HTTPS encryption is configured for customer web application access. This helps to ensure that user data in transit is safe, secure, and available only to intended recipients. The level of encryption is negotiated to either SSL or TLS encryption and is dependent on what the web browser can support.

Access Controls

Role based access controls are implemented for access to information systems. Processes and procedures are in place to address employees who are voluntarily or involuntarily terminated. Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis. Access control lists define the behavior of any user within our information systems, and security policies limit them to authorized behaviors.

We support multiple single sign-on implementations, allowing you to streamline authentication processes and tie directly into your existing identity management solutions.

User provisioning is controlled solely by the customer.

Access rights and privileges necessary to perform an employee's job function is granted in accordance with:

- Need to Know
- Need to Use
- Least Privilege
- Segregation of Duties
- Contractual obligations regarding limitation of access to data or services
- Regulatory requirements

Authentication and Authorization

We require that authorized users be provisioned with unique account IDs. Our password policy covers all applicable information systems, applications, and databases. Our password policies enforce the use of complex passwords, which are deployed to protect against unauthorized use of passwords.

Rehearsal employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines.

Software Development Lifecycle

We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products. Our products are deployed on an iterative, rapid release development lifecycle. Security and security testing are implemented throughout the entire software development methodology. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of all development activities.

Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments. The Rehearsal architecture teams review our development methodology regularly to incorporate evolving security awareness, industry practices and to measure its effectiveness.

Rehearsal's development team employs secure coding techniques focused around the OWASP Top Ten Vulnerabilities.

Incident Management

Rehearsal has a formalized incident response plan (Incident Response Plan) and associated procedures in case of an information security incident. The Incident Response Plan defines the responsibilities of key personnel and identifies processes and procedures for notification. Incident response personnel are trained, and execution of the incident response plan is tested periodically.

An incident response team is responsible for providing an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Breach Response and Notification

Although Rehearsal takes all necessary actions to protect data, we cannot guarantee absolute security as no method of transmission over the Internet and or electronic storage is perfectly secure. However, if Rehearsal learns of a security breach, we will notify affected users so that they can take appropriate protective steps.

Breach notification procedures comply with in-country laws and regulations, as well as any standards relevant to Rehearsal.

Rehearsal are committed to keeping customers fully informed of any matters relevant to the security of their data.

Business Continuity and Disaster Recovery

To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, we implement a disaster recovery program at all our data center locations. This program includes multiple components to minimize the risk of any single point of failure. For business critical applications, application data is replicated to multiple systems within the data center and, in some cases, replicated to secondary or backup data centers that are geographically dispersed to provide adequate redundancy and

high availability. High-speed connections between our data centers help to support swift failover.

Disclaimer

The information in this document is not legal advice for you or your company to use in complying with data security laws or data privacy laws, such as EU data privacy laws like the GDPR. The content in this document is meant only for educational purposes and to provide you with background information to help you better understand Rehearsal's efforts to comply with various regulations and standards. If you have any questions or concerns that we can help you with compliance or any other privacy-related concerns, don't hesitate to contact us directly.