Security @ OfficeRnD

Introduction

Making flexible working the way of working has always been our main goal. One of the most important aspects of our products and services is ***security*** - our mission depends on it. We're obliged to ensure the safety and security of your data and to provide you with any information you need to understand and evaluate our security practices and policies.

This white paper outlines how we keep our systems secure and what steps we take to build security into our products. Our aim is to help your team take full advantage of all that OfficeRnD offers with the confidence that your organization's security is ensured.

Organizational Security

We base our security policies and practices on the concept of *defense in depth*: securing our organization, and your data, at every layer. Our security program is aligned with ISO 27000, AICPA Trust Service Principles, and NIST standards, and is updated and improved constantly following any new industry best practices. You can review our certifications here.

OfficeRnD’s security program is implemented and managed by our security team, led by our Chief Technology Officer (CTO). We are dedicated to delivering the best possible results when it comes to Secure Engineering and Operations, Detection and Response, Security Architecture, Product Security, and Risk and Compliance.

Customer Data Security

When it comes to security, we put our customers first. To do this, our security team of seasoned professionals works in partnership with peers across the company, takes exhaustive steps to identify and mitigate risks, implements best practices, and constantly develops ways to improve.

Secure by design

Our change management policy defines how every change and new feature is developed and released. It ensures all application changes are authorised before implementation into production. Our Software Development Life Cycle (SDLC) mandates adherence to secure coding guidelines, as well as code screening of changes for potential security issues. We use dedicated analysis tools, vulnerability scanners, and manual review processes to ensure the necessary level of quality.

Encryption

🛫 Data in transit

All data transmitted between OfficeRnD clients and the OfficeRnD services is done using strong encryption protocols. OfficeRnD supports the latest recommended secure cipher suites to encrypt all traffic in transit, including use of TLS 1.2 protocols, AES256 encryption, and SHA256 signatures.

💾 Data at rest

In our production environment we encrypt data at rest using FIPS 140-2 compliant encryption standards. This applies to all types of data at rest within our systems - databases, file stores, database backups, etc. We store encryption keys in a secure place on a segregated network with very limited access. Our security team implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials.

Each customer data is hosted in our shared infrastructure and logically separated from other customers' data. A combination of different storage technologies is used to ensure protection against hardware failures and speed of retrieval. Our services are hosted in data centers maintained by industry-leading service providers (Amazon Web Services). This allows us to rely on state-of-the-art physical protection for the servers and infrastructure that comprise our operating environment.

Network Security and server hardening

We segregate our services into separate networks to better protect sensitive data. Systems used during testing and development activities are deployed in a separate network from systems running production infrastructure. All servers within our production environment are hardened (e.g. disabling unnecessary ports, removing default passwords, etc.) and have a base configuration image applied to ensure consistency across the environment. Network access to our production environment from open, public networks (the Internet) is restricted, with only a small number of production servers accessible from the Internet. We have opened only network protocols which are essential for our product to serve its users. Additionally, for host-based intrusion detection and prevention activities, we log, monitor, and audit all systems and have alerting in place which notify us for a potential intrusion. We have mechanisms preventing distributed denial of service (DDoS) attacks enforced at the network level.

Endpoint Security

We have established strict endpoint security protocols and we make sure they are followed. Each employee workstation is provisioned by the company according to our security standards. We require all workstations to be properly configured, updated and monitored by our endpoint management solutions. Our default setup enforces data encryption at rest on all workstations, users to have strong passwords, and automatic lock when idle. Each workstation has an up-to-date monitoring software which is used to protect against malware, unauthorized software usage, unwanted mobile storage devices etc. If a mobile device is used for business purposes, we mandate it to be enrolled in the appropriate mobile device management system, to ensure it meets our security standards.

Access Control

🛂 Provisioning

In order to minimize the risk of data exposure, we follow the principles of least privilege and role-based permissions when provisioning user access. Employees are only authorized to access data that they reasonably need in order to fulfill their current job responsibilities. Upon dismissal each employee data access is revoked immediately. We review user access at least quarterly.

🛡️ Authentication

To further reduce the risk of unauthorized access to data, we mandate multi-factor authentication for all access to systems with highly classified data, including our production environment, which houses our customer data. Where possible and appropriate, we use private keys for authentication, in addition to the previously mentioned multi-factor authentication on a separate device.

🔐 Password Management

We require employees to use an approved password manager. Password managers generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password-related risks.

Monitoring

We monitor our infrastructure, workstations and mobile devices in order to have a comprehensive view of the security state of our corporate and production assets. All administrative access, use of privileged commands, and system calls on all servers in the production environment are logged and retained for at least 1 year. We analyze logs automatically to the extent practical so that we are able to identify potential risks and alert responsible people. Our production logs are stored in a separate network that is restricted to only the relevant security personnel.

Data retention and disposal

Customer data is removed immediately upon deletion by the end user or upon expiration of data retention. OfficeRnD hard-deletes all information from currently running production systems (excluding information stored in audit logs) and backups are retained for 3 months for disaster recovery purposes. We rely on our hosting providers to ensure destruction of data from disks in a responsible manner before they are decommissioned or repurposed.

Disaster Recovery and Business Continuity

We use services deployed by our hosting provider to distribute production operations across several separate physical locations. These locations are within one geographic region, but protect our services from loss of connectivity, power infrastructure, and other common location-specific failures. Production transactions are replicated among these environments in order to ensure the availability of our services in the case of a location-specific disaster. We maintain a full backup copy of production data in a different location, which is significantly distant from the location of the main operating environment. We save full backups at least once per day and transactions are saved continuously. Our backup procedures are tested at least quarterly to ensure data can be successfully restored.

Security Incidents

We have established policies and procedures for responding to potential security incidents. All security incidents are managed by our Incident Management Team. The process defines each type of event that must be managed via the incident response process and classifies them based on severity. In the event of an incident, affected customers will be informed via email from our customer success team. Incident response procedures are tested and updated at least annually.

Vendor Management

In order to operate efficiently, we rely on additional products and services. When those services impact the security of our production environment, we make sure to maintain our security posture by establishing agreements that require service organizations to adhere to confidentiality commitments we have made to users. We monitor the effective operation of the organization’s safeguards by conducting reviews of all service organizations’ controls before use and review them periodically.

External Validation

📜 Security Compliance Audits

We continuously review and improve the design and operating effectiveness of our security controls. These activities are regularly performed by both third-party credentialed assessors and OfficeRnD’s internal risk and compliance team. Audit results are shared with senior management and all findings are addressed timely.

👮 Customer Driven Audits and Penetration Tests

Our customers are welcomed to perform either security controls assessments or penetration testing on our environment. Please contact your account executive to learn about options for scheduling either of these activities.

Conclusion

It is of vital importance to us to keep our systems and your data safe. All customers expect and deserve their data to be secure and confidential. Making sure everything is protected is a critical responsibility that we have to our customers, and we continue to work hard to maintain that trust. Please contact your account executive if you have any questions or concerns.