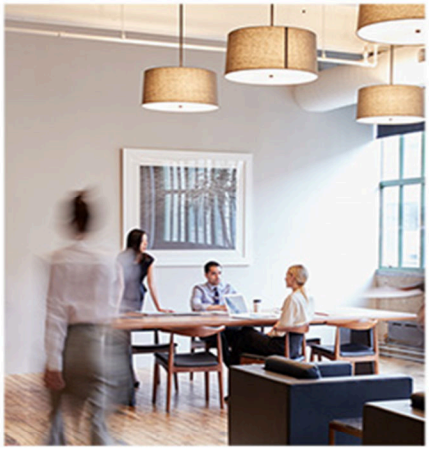
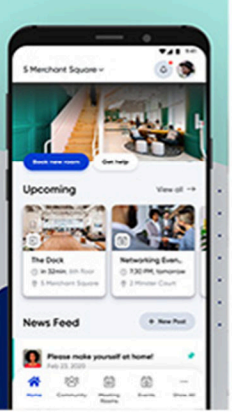
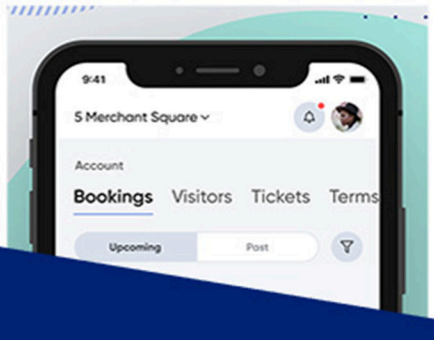
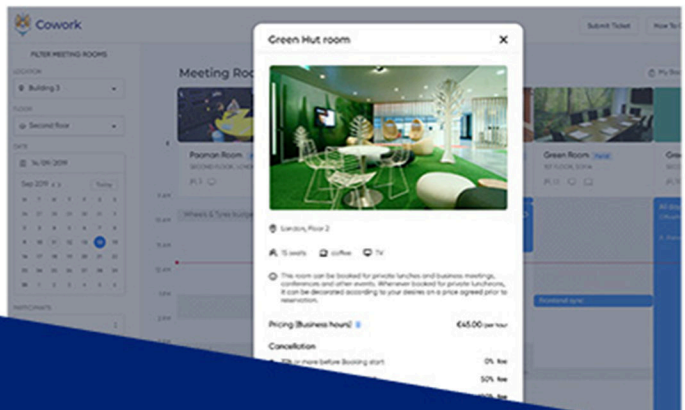
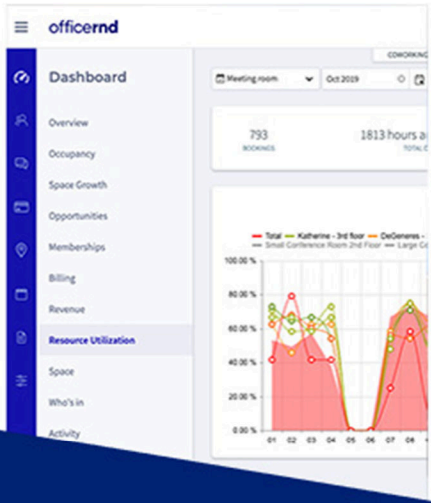


officernd









Security @ OfficeRnD

Version: 1.2

North Shields, UK
69 Church Way, NE290AE

Atlanta, US
3365 Piedmont Road NE, Suite 1400

Melbourne, Australia
Level 3/162 Collins St

Sofia, Bulgaria
33 Alexander Malinov Blvd.

http://www.officernd.com
info@officernd.com

officernd

1. INTRODUCTION. 1

2. GOVERNANCE AND ORGANIZATIONAL SECURITY. 1

Integrity and ethical values 1

Risk assessment, governance, and treatment 1

Internal control framework 2

2. HUMAN CAPITAL SECURITY. 3

Pre-employment verification 3

Security and awareness training and acknowledgment 3

Continuous training 4

3. CUSTOMER DATA SECURITY. 4

Secure by design 4

Data encryption in transit 4

Data encryption at rest 5

Physical security 5

Network Security 5

Endpoint Security 6

4. ACCESS CONTROL. 6

Access management 6

Authentication 6

Password Management 7

5. MONITORING. 7

Availability, capacity, and security 7

Vulnerability scanning and penetration testing 8

5. DATA RETENTION AND DISPOSAL. 8

6. BUSINESS CONTINUITY AND DISASTER RECOVERY. 8

7. INCIDENT MANAGEMENT. 9

8. VENDOR MANAGEMENT. 9

9. EXTERNAL VALIDATION. 9

Security Compliance Audits 9

Customer Driven Audits and Penetration Tests 10

10. CONCLUSION. 10

officernd

1. INTRODUCTION.

For us at OfficeRnD making flexible working the way of working has always been our main goal. **Security, availability, confidentiality, and privacy** have always been important aspects of our products and services. 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.

2. GOVERNANCE AND ORGANIZATIONAL SECURITY.

As a software developer and technology provider, OfficeRnD takes security, confidentiality, and privacy seriously. The OfficeRnD security strategy is well defined and implemented company-wide.

Integrity and ethical values

Our core values are the driving force of OfficeRnD success. They have been dictating our approach from the very start, and we need all our employees to share these values. In this constantly changing world, we are committed to observing the strictest ethical business practices in all that we do, with all our partners, and in each of the countries we operate. If you want to learn more about our core values you can take a look at our Code of Conduct.

Risk assessment, governance, and treatment

At OfficeRnD we have specified objectives with sufficient clarity to identify and assess risks relating to our objectives. All assets (infrastructure, information, people, software, data, etc.) are identified, assigned ownership, and maintained in an asset register. A company-wide risk assessment that evaluates risks related to confidentiality, privacy, availability, integrity, fraud, security, and vendors is conducted annually.

officernd

Internal control framework

We base our internal controls framework on the concept of defense in depth: securing our organization, and your data, at every layer. Our security program is aligned with ISO 27000, American Institute of Certified Public Accountants (AICPA) Trust Service Criteria (TSC), and National Institute of Standards and Technology (NIST) standards and is reviewed, updated, and continuously improved following any new industry best practices.

In our Information Security Management System (ISMS) we have the following policies and procedures in place:

- Vendor management and risk assessment.
- Risk assessment and treatment.
- Hiring, onboarding and termination.
- Performance evaluation.
- Incident management.
- Vulnerability management.
- Data classification, labeling, protection, retention, and disposal.
- Acceptable use.
- Business continuity and disaster recovery.
- Change management.
- Identity and access management.
- Cryptography and key management.
- Backups and backup restoration.

View the certificate

Request the report

Read Privacy Policy

Download questionnaire

We are ISO 27001 certified and has obtained a SOC 2 Type 2 report for compliance with the AICPA TSC for Security, Availability, Confidentiality and Privacy.

We are compliant with the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Personal Information Protection and Electronic Documents Act (PIPEDA) and all other applicable privacy legislation in the locations we operate in.

OfficeRnD is also Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) Level 1 registered service provider.

Our security program is implemented and managed by our security and compliance 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, Governance and Compliance.

2. HUMAN CAPITAL SECURITY.

Our employees are an essential part of upholding our commitment to security. We are doing pre-employment background screening in compliance with local laws. New employees got though onboarding and ongoing trainings that include the following:

Pre-employment verification

Our hiring process for candidates includes background screening and reference checks. These checks also include verification of education and previous employment history.

Where local labor law or statutory regulations permit, OfficeRnD may also conduct criminal checks, depending upon the specific jurisdiction and position.

All OfficeRnD employees are also required to sign a non-disclosure agreement prior to employment.

Security and awareness training and acknowledgment

All OfficeRnD employees are required to successfully complete information security, data protection and awareness training and acknowledge the Information Security Management System (ISMS) policies and procedures, the Employee Handbook, and the Code of Conduct upon employment and annually thereafter.

Phishing campaigns are conducted on a quarterly basis.

officernd

Continuous training

Our security and compliance team provides continuous communication about emerging threats and advises employees on security trends. All employees have access to continuous development funds.

3. 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, evaluate 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. Our processes encompass all types of changes -, infrastructure, network, system, and application code. It ensures all changes are reviewed and authorized 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.

Data encryption 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 enforcing of Transport Layer Security (TLS) 1.2 protocol as minimum with Advanced Encryption Standard (AES) 256 encryption.

officernd

Data encryption at rest

In our production environment we encrypt data at rest using AES 256 encryption. 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.

Physical security

Each customer's 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 applications are hosted in data centers maintained by industry-leading service provider Amazon Web Services (AWS). This allows us to rely on state-of-the-art physical protection for the servers and infrastructure that comprise our operating environment. OfficeRnD leverage AWS compliance and certifications like ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC 2 Type 2, HIPAA, and many others.

All our vendors and service providers are managed according to our robust vendor management program.

Network Security

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, we monitor, audit, and log all systems and have alerting in place which notify us for a potential threat. 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 that is used to protect against malware. 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.

4. ACCESS CONTROL.

Access management

To minimize the risk of data exposure, we follow the principles of least privilege and role-based permissions when provisioning user access. Employees can only access data that they reasonably need to fulfill their current job responsibilities. Upon termination, each employee's access is revoked on the last day of employment. All access modifications are documented and approved by the respective asset owners. We review user access at least quarterly.

Authentication

To access systems, employees are required to authenticate using their Google Workspace credentials through Single Sign On (SSO). Our policy enforces the use of multi-factor authentication (MFA) for users. Users are also required to separately sign-on to any systems or applications that do not support SSO functionality. Whenever supported by the service providers, the use of MFA is enabled and

enforced. Passwords must conform to defined configuration standards which are enforced through security policy configuration. Passwords are rotated on a 90-day basis.

Access to the staging and production environments is possible only through separate VPNs. Users authenticate by individually assigned certificates and need to be additionally whitelisted to be provided access.

Password Management

We require employees to use an approved password manager with multi-factor authentication. Password managers generate, store, and enter unique and complex passwords for all system accounts.

5. MONITORING.

Availability, capacity, and security

Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. Our Web Application Firewall (WAF), Intrusion Detection System (IDS) and File Integrity Monitoring (FIM) and availability and capacity monitoring software are configured to alert IT personnel when thresholds have been exceeded. We monitor our cloud infrastructure, workstations, and mobile devices to have a comprehensive view of the security state of our 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 can 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.

officernd

Vulnerability scanning and penetration testing

Web application vulnerability scanning is performed on a bi-monthly basis, continuous vulnerability scanning is performed on the AWS environment in accordance with OfficeRnD policy.
Penetration testing is performed on annual basis.
Any identified vulnerabilities are remediated according to our internal policies and procedures and their assigned Common Vulnerability Scoring System (CVSS) score.

5. DATA RETENTION AND DISPOSAL.

Customer data is removed immediately upon deletion by the end user or upon expiration of data retention period. OfficeRnD hard-deletes all information from currently running production systems (excluding information stored in audit logs) and backups are retained for 5 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.

6. BUSINESS CONTINUITY AND DISASTER RECOVERY.

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 are doing hourly and daily backups. Our backup procedures are tested at least daily to ensure data can be successfully restored by conducting backup restoration tests.

Our formal Business Continuity and Disaster Recovery plans are tested at least annually.

7. INCIDENT MANAGEMENT.

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. Security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. In the event of an incident, affected customers will be informed via our status page. Incident response procedures are tested and updated at least annually.

8. VENDOR MANAGEMENT.

To operate efficiently, we rely on additional third-party 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 the security, confidentiality, and privacy commitments we have made to users.

We monitor the effective operation of the organization's safeguards by conducting comprehensive reviews of all service organizations' controls related to security, confidentiality, and privacy before engaging a service provider. All service providers undergo an annual reassessment.

9. 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 accredited 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.

10. CONCLUSION.

It is of vital importance to us at OfficeRnD 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 or our Security and Compliance team if you have any questions or concerns.