Omada Security Policy

Last Updated: January 6th, 2025

This Omada Security Policy forms part of the Customer Agreement and applicable Orders between Omada and Customer (the "**Agreement**") and shall be effective on the effective date of the Agreement.

Security Policy

Omada has implemented and shall maintain a commercially reasonable security program in accordance with industry best practices, which shall include technical and organizational measures to ensure an appropriate level of security for Customer Personal Data taking into account the risks presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to Customer Personal Data, and the nature of the Customer Personal Data to be protected having regard to the state of the art and the cost of implementation. Omada's security program shall include the following measures:

DATA PRIVACY CONTROLS

I. OMADA SECURITY CERTIFICATIONS

Omada Identity Cloud services meet the specific requirements of data protection, including Article 28 of the General Data Protection Regulation which are listed as SOC 2, Type 2 and ISO 27001 compliant an others.

At a minimum, Omada has implemented for the Omada Identity Cloud the technical and organizational measures and maintains security practices within the production environments as follows:

II. CONFIDENTIALITY MEASURES

Physical Access Management

a) Employee physical access that is no longer required in the event of personnel termination or role change is promptly revoked. If applicable, temporary badges are returned before exiting the facility.

b) Initial permission definitions and changes to permissions, associated with physical access roles are approved by appropriate Omada personnel.

Physical Access Reviews

Omada performs physical access account reviews every quarter; corrective action is taken where applicable.

Physical Security

a) Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points and/or manned reception desks.

b) All facilities require badge access and have 24x7 security guards. Some facilities use additional measures to prevent unauthorized individuals from tailgating authorized individuals into the facility.

c) Intrusion detection and video surveillance are installed at all facilities. Omada may review video logs when issues or concerns arise to determine access.

d) Omada power and telecommunication lines are protected from interference, interception and damage.

e) Granting physical access to an Omada data center requires management approval and documented specification of:

(1) account type: (visitor, vendor, or regular)

(2) intended business purpose

(3) visitor identification method, if applicable

(4) temporary badge issued, if applicable

(5) access start date and end date

(6) access duration

f) Visitors to a facility are required to be always escorted and are not allowed in caged areas.

g) Visitor Access Logs are retained for up to 12 months following Omada's documentation retention policy.

Logical access

a) Logical access provisioning to information systems requires approval from appropriate personnel.

b) Logical access that is no longer required in the event of termination is documented, communicated to management, and revoked.

c) Omada performs account and access reviews quarterly, and corrective action is taken where applicable.

Authentication

a) Omada creates unique identifiers for user accounts and prevents the reuse of identifiers. Account Login parameters follow these rules:

(1) Accounts are not shared;

(2) Inactive sessions are password protected after 15 minutes; and

(3) All systems classified as confidential and restricted require multifactor authentication. Multifactor authentication must be used for access to environments that host production systems or systems and applications containing restricted or confidential data.

b) Omada users are enrolled with the Omada Identity Cloud platform. Omada Identity Cloud platform is a platform that uses multifactor authentication plus device and security posture during authentication. For more information on the Omada Identity Cloud platform, see the Omada white paper available here: https://omadaidentity.com/resources/product-brief/

(1) Omada Identity Cloud access proxy is encrypted with Transport Layer Security (TLS).

(2) Users enrolled in the Omada Identity Cloud platform are only required to change their passwords upon compromise indicator.

(3) Access to the system needs to be requested every day, as it is revoked every day, at midnight. Authentication is based on 2FA.

c) In case of circumstances where an Omada user is not enrolled with the Omada Identity Cloud platform, user and device authentication to information systems is protected by passwords that meet Omada's password complexity requirements.

Strong password configurations adhere to the following rules:

a) Omada enforces the use of complex Windows passwords.
b) All Omada business critical systems are protected by the two-factor authentication.
c) Unless Omada Identity Cloud is cloud-enabled, remote connections to the corporate network are accessed via VPN through managed gateways.

Role-Based Access Control

a) Initial permission definitions and changes to permissions associated with logical access roles are approved by the appropriate personnel.

b) Access that allows modification to source code is restricted to authorized personnel.

c) Role-based and context-based access to data are modelled on the concept of least privilege.

Network Operations

a) Omada maintains a dedicated Support Center which is staffed 24/7 with at least 2 dedicated personnel.

b) Network traffic to and from untrusted networks passes through a policy enforcement point; firewall rules are established following identified security requirements and business justifications.

c) Omada uses Web Application Firewalls, network zones isolation and strict protocol controls as layers of security. Antivirus is running on all employee desktops and laptops and all email traffic is scanned for malware. Additionally, real-time antivirus scanning is enabled.

d) Production environments are logically segregated from non-production environments.

Key Management

Omada uses encrypted, centrally managed cryptographic key stores. Access to the cryptographic key stores is limited to authorized personnel, it is logged and reviewed as defined by the process.

Preservation and Review of Security Logs

a) Omada keeps logs used in connection with its security procedures for the protection of Personal Data related to the applicable product operations in a secure location. Omada retains logs within the Security Event Monitoring and logs aggregation service, for a minimum period of one year.

b) Security event logs are reviewed per the event context and severity, some of which require daily review.

III. Employee Management

Background Checks and Non - Disclosure Agreements

a) For business-critical functions, Omada obtains pre - hire background check reports for employment purposes. The specific nature and scope of the report that Omada typically seeks may include (as permitted or required by applicable law):

(1) Educational background;

(2) Work history;

(3) Court records (including criminal conviction records); and

(4) References obtained from professional and personal associates.

b) Omada hires employees based on a documented job description.

c) Employees are required to sign a Non-Disclosure Agreement upon employment. Omada employees including contractors are required to sign an agreement that they will protect confidential information.

Training and Awareness

a) Omada personnel (including contract workers) complete security awareness training, which includes annual updates about relevant policies, standards, and new or modified attack vectors and how to report security events to the appropriate response team. Records of annual training completion are documented and retained for tracking purposes. Any Omada vendors with network access are required to complete their own equivalent security awareness training.

b) Annually, Omada full-time and temporary employees and interns complete a code of business conduct training. Anyone who is found to violate the Code of Business Conduct or other Omada policies may be subject to disciplinary action including termination of employment or contract.

IV. Information Systems and Technology Management

Production Configuration Management

a) Omada ensures security hardening and baseline configuration standards have been established according to industry standards defined by the Microsoft Security Baseline (Security baselines guide - Windows Security | Microsoft Learn) and are reviewed and updated periodically.

b) Omada uses mechanisms to detect deviations from baseline configurations in production environments.

c) Installation of software or programs in the production environment requires approval by the appropriate personnel.

Change Management

a) Change scope, change type, and roles and responsibilities are pre-established and documented in a change control workflow. Notification and approval requirements are also pre-established based on the risk associated with change scope and type. Change management uses an automated ticketing system.

b) Based on risk, before introducing changes into the production environment, approval from appropriate personnel is required based on the following:

(1) Change description is documented;

(2) Impact of change;

(3) Test results are documented; and

(4) Back-out procedures are defined.

c) Changes to the production environment are implemented by authorized personnel only.

Data Transfer

a) Omada deploys dedicated network connections from its corporate offices to Omada data center facilities to enable secure management of the servers.

b) All management communications to the servers occur over encrypted tunnels and sessions. Some examples are Secure Shell (SSH), Transport Layer Security (TLS); Internet Protocol Security (IPSec) and Virtual Private Network (VPN) channels. Remote access for VPN always requires multifactor authentication.

c) Administrative data is encrypted in transit across the internet via TLS 1.2 or greater over HTTPS between the Customer and the user interface.

d) All customer data is encrypted with Transparent Data Encryption (TDE) using AES256.

e) All environments and components are pseudonymized.

f) Right to be forgotten. Omada Identity Cloud setup with its true data isolation allows deletion of all data from the customer environment when requested.

g) Account closure and deletion of data. Upon the end of the subscription (whether through expiry or termination), the Customer no longer has rights to access or use the Services, including the associated Omada software. Within 30 days after the effective date of termination or expiration of this Agreement, Omada will make the Customer Data available to the Customer for export or download as provided in the Documentation. After the 30 days, Omada has no obligation to maintain or provide any Customer Data and, as provided in the Documentation, must delete, or destroy all copies of Customer Data in its systems or otherwise in its possession or control, unless legally prohibited. Notwithstanding the foregoing, in the event of termination of this Agreement and/or the applicable Order, Omada may make the Customer Data available to the Customer for a longer period by mutual agreement and at fees negotiated by the parties. The Customer may, in addition, request Omada to assist in the extraction of Customer Data. Such assistance requires a separate statement of work (SoW) and must be compensated on a time and material basis applying Omada's then-current price rates for such services.

Security Governance

a) Corporate Documents. Omada's key business functions and information security capabilities are supported by documented procedures that are communicated to authorized personnel.

b) Information Security Management. Omada has an established governance framework that supports relevant aspects of information security with policies and standards.

c) Security Leadership & Roles. Roles and responsibilities for the governance of Information Security within Omada are formally documented and communicated by Management.

Cloud Services Systems Monitoring

a) Critical Information System Logs.

(1) Omada utilizes a centralized Security Event Monitoring solution to aggregate and correlate log events.

(2) To protect against unauthorized access and modification, Omada captures network logs, operating system logs, application logs and security events.

(3) Application user activity is logged by the application.

b) Security Monitoring and Evaluation

(1) Omada defines security monitoring alert criteria, how alert criteria will be flagged and identifies authorized personnel for flagged system alerts.

(2) Omada defines availability monitoring alert criteria, how alert criteria will be flagged and identifies authorized personnel for flagged system alerts. Customers can monitor a product's availability at: https://status.omada.cloud

c) System Design Documentation.

(1) Documentation of system boundaries and key aspects of their functionality are published to authorized Omada personnel.

(2) Omada publishes public-facing whitepapers that describe the purpose, design, and boundaries of the system and system components which are available here: Cloud Identity Management Solution | Omada Enterprise SaaS (omadaidentity.com)

Service & Product Lifecycle

a) Source code is checked for vulnerabilities before being released into production. For high-risk services and products, manual security testing, and, where appropriate, manual and automated code review, is performed for significant changes to ensure detection and prevention of common security issues.

b) All software releases are subject to the Service Life Cycle, which requires acceptance via Concept Accept and Project Plan Commit phases before implementation.

Vulnerability Management

a) Information Systems and Technology.

1. For customer‐facing products as defined in Omada's Current List of Certifications, Standards, and Regulations listed at The Trusted Partner for Modern IGA | Omada Trust Center (omadaidentity.com), at least annually, Omada engages with specialized third parties to perform application penetration testing, assign risk ratings to discovered vulnerabilities, and track vulnerabilities through resolution. At least annually, Omada will perform network penetration testing for all critical services defined in the above list. Network testing may be performed by Omada's internal security teams.

2. The objective of penetration testing is to find security vulnerabilities following industry standards and best practices (such as those listed in the Open Web Application Security Project current ten most common web application security risks).

3. Upon receipt of the deliverable provided by a third party, Omada documents these vulnerabilities, evaluate them following its internal processes as well as recommendations by the third party, and then creates a mitigation strategy or remediation plan.

4. A remediation report which provides an overview of the testing methodologies, findings and remediations can be requested from an Omada sales representative.

b) If applicable, Omada has managed enterprise antivirus deployments and ensures the following:

1. Signature definitions are updated daily;

2. Full scans are performed weekly and real-time scans are enabled; and

3. Alerts are reviewed and resolved by the appropriate personnel.

c) Vulnerability Scans. External and internal vulnerability scans are performed on a continuous basis.

d) Vulnerability Reviews. Omada reviews reasonable customer vulnerability-related inquiries for advisement only.

e) Patch Management. Omada installs security-relevant patches, including software or firmware updates following Omada's patch management standard.

V. Measures for prompt recoverability & access to Data

Incident Response

Omada has implemented a comprehensive incident response program that includes at least the measures below and as described at the The Trusted Partner for Modern IGA | Omada Trust Center (omadaidentity.com)

a). Omada defines the types of incidents that need to be managed, tracked, and reported. Such management includes the following:

1. Procedures for the identification and management of incidents.
2. Procedures for the resolution of confirmed incidents.
3. Key incident response systems.
4. Incident coordination and communication strategy.
5. Contact method for internal parties to report potential incidents.
6. Support team contact information.
7. Notification to relevant Omada management in the event of a security breach.
8. Provisions for updating and communicating the plan.
9. Provisions for the training of the support team.
10. Preservation of incident information; and,
11. Management review and approval (either annually or when major changes to internal organization occur).

b) Omada responds to confirmed incidents and resolution is tracked with appropriate management channels. If applicable, Omada coordinates the incident response with business contingency activities.

c) Omada provides a contact method for external parties to report incidents here: https://omadaidentity.com/company/contact-us/

Disaster Recovery and Business Continuity Plans

a) Omada maintains disaster recovery and business continuity plans and processes to allow for the continuation of the services and to provide an effective and accurate recovery. Such plans are tested on an annual basis.

b) Within the Disaster Recovery process, the following objectives have been defined:

1. Recovery Point Objective (RPO) – a time measurement from the loss event to the most recent preceding backup – 15 minutes

2. Recovery Time Objective (RTO) – the duration of time between loss and recovery. The objective also accounts for the steps internal technical departments have to take to restore the application and it's data – 240 minutes.

c) Within the Disaster Recovery topic we may differentiate two layers – the data layer and infrastructure layer. The data layer consists of databases that are stored within the Azure environment and can be recovered directly by the customer via the Customer Portal

d) All used resource types are operated redundantly in the data centers of an Azure Region (Azure zone-redundant). Back-ups are mirrored in a second Azure region. If the customer subscribes to Omada's geo-redundancy package, the application's data are mirrored in a third Azure region as well.

e) The different data backup types and the time said backups are being stored for the production environment are as follows:

Backup Type	Time
Pont-in-time-recovery (PiTR)	0 Days – 7 Dats
Full Weekly	1 Week – 52 Weeks (total of 52 backups)
Full Monthly	1 Month – 12 Months (total 12 backups)
Full Yearly	1 Year – 5 Years (total 5 backups)

VI. Processes for regular testing, assessing, and evaluating the effectiveness of security measures

Risk Management

a) Omada management performs an annual risk assessment in alignment with the ISO/IEC 27001:2013 - Information Security Management Systems and ISO 31000:2009 - Risk Management Principles and Guidelines. Results from risk assessment activities are reviewed to prioritize mitigation of identified risks.

b) Management assesses the design and operating effectiveness of internal controls against the established controls framework. Corrective actions related to identified deficiencies are tracked to resolution.

c) Omada establishes internal audit requirements and executes audits on information systems and processes at planned intervals.

d) Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.

Third-Party Management

a) Periodically, management reviews controls within third-party assurance reports to ensure that they meet organizational requirements. If control gaps are identified in the assurance reports, management addresses the impact that disclosed gaps have on the organization.

b) Any Third-Party contract changes applied to Omada services, are a subject of the Risk Assessment process.

Technical Progress

Omada´s Technical and Organizational Measures are subject to technical progress and further development. Accordingly, Omada reserves the right to modify the Technical and Organizational Measures provided that the functionality and security of the Omada Identity Cloud are not degraded.

Notification to Omada

a) To notify Omada of a security issue, please send an email to: security@omadaidentity.com

b) For the data privacy matters, please send an email to: dataprotection@omadadentity.com