SOC 3 TYPE II report



PERIOD UNDER REVIEW

1 OCTOBER 2025 UNTIL 30 SEPTEMBER 2026

Omada

TABLE OF CONTENTS

MANAGEMENT STATEMENT PROVIDED BY OMADA 3

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT 6

I. SCOPE OF THE SOC 3 REPORT 10

I.1.1 SCOPE DEFINITION 10
I.1.2 PROCESSES OUT OF SCOPE 10
I.1.3 CARVE-OUT 11
I.1.4 TRUST SERVICES CRITERIA REQUIREMENTS 11

II. DESCRIPTION OF THE BOUNDARIES OF THE OMADA ORGANIZATION 15

II.2.1 GENERAL 15
II.2.2 CORPORATE OBJECTIVES 16
II.2.3 ORGANIZATION 17
II.2.4 IT SYSTEMS 17
II.2.5 THIRD PARTIES 19

III. OMADA PROCESSES 20

III.3.1 LOGICAL AND PHYSICAL ACCESS CONTROLS 20
III.3.2 SYSTEM OPERATIONS 21
III3.3 CHANGE MANAGEMENT 22
III.3.4 AVAILABILITY 22
III.3.5 CONFIDENTIALITY 23

IV. COMPLEMENTARY USER ENTITY CONTROLS 25

Management Statement provided by Omada

We have prepared the accompanying description around the suitability of the design of controls relevant to Security, Availability and Confidentiality. The description is intended to provide report users entities with information about Omada Identity Cloud that may be useful when assessing the risks arising from interactions with Omada throughout the period of 1 October 2025 until 30 September 2026, particularly information about system controls that Omada has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for Security, Availability and Confidentiality (applicable Trust Service Criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA Trust Services Criteria).

We have prepared the accompanying description based on the criteria of a description in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC Report® (AICPA, Description Criteria) ("description criteria"). We confirm, to the best of our knowledge and belief, that:

(a) The accompanying description in section III: Description of the boundaries of the Omada system fairly presents the Trust Services Criteria of Security, Availability and Confidentiality in relation to Omada Identity Cloud used by user entities throughout the period of 1 October 2025 until 30 September 2026. The criteria used in making this assertion were that the accompanying description:

(i) Presents how the system was designed and implemented, including:

- The types of services provided, including, as appropriate, classes of transactions processed.
- The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary and transferred to the reports prepared for user entities.
- The related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for user entities.
- How the system dealt with significant events and conditions, other than transactions.
- The process used to prepare reports for user entities.
- Relevant control objectives and controls designed to achieve those objectives.
- Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary, to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone.
- Other aspects of our control environment, risk assessment process, information system and communication, control activities and monitoring controls that were relevant to processing and reporting Clients' transactions.

(ii) Includes relevant details of changes to our control systems during the period of 1 October 2025 until 30 September 2026.

(iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common

needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the system that each individual Client may consider important in its own particular environment.

(b) The controls related to the control objectives stated in the Omada Identity Cloud description were suitably designed and operated effectively throughout the period of 1 October 2025 until 30 September 2026. The criteria used in making this assertion were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified;

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period of 1 October 2025 until 30 September 2026.

On behalf of Omada A/S

Luca Bellintani

Chief Information Security Officer

Copenhagen | 9 November 2026

SECTION I



INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT

Omada

Independent service auditor's assurance report

To: the management of Omada A/S

Scope

We have examined Omada A/S (hereinafter: Omada)'s accompanying description titled 'Section III: Description of the Boundaries of the Omada System. Related to the SaaS, Cloud based identity governance and administration platform services were effective throughout the period from 1 October 2025 to 30 September 2026, in providing reasonable assurance that Omada's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (applicable trust services criteria), as set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA Trust Services Criteria).

Subservice organisations

Omada uses Microsoft Azure to provide cloud security and infrastructure services. The description of the system includes a carve-out of the subservice organisation and therefore includes only the description criteria and related controls of Omada, excluding the control objectives and related controls of Microsoft Azure. The description of the system indicates that certain applicable trust services criteria can only be achieved if controls at the subservice organisation are suitably designed and operating effectively. It also sets out the complementary subservice organisation controls assumed in the design of Omada's controls. Our examination did not extend to the controls of Microsoft Azure, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Complementary user entity controls

The description of the boundaries of the Omada (specifically Section IV. Complementary User Entity Controls) indicates that certain applicable trust services criteria can be achieved only if complementary user entity controls contemplated in the design of Omada's controls are suitably designed and operating effectively, together with related controls at the service organisation. The description of the boundaries of the Omada (specifically Section IV. Complementary User Entity Controls) also sets out the complementary user entity controls assumed in the design of Omada's controls. The Omada's description of the scope, as presented in Attachment A of this report, sets out Omada's controls and the applicable trust services criteria. Our examination did not include these complementary user entity controls, and we have not evaluated the suitability of their design or their operating effectiveness.

Service organisation's responsibilities

Omada is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Omada's service commitments and system requirements were achieved. Omada has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its description, Omada is responsible for selecting, and identifying in its description, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Responsibility of the service auditor

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organisation's service commitments and system requirements were achieved based on the applicable trust services criteria.

We conducted our examination in accordance with Dutch law, including Dutch Standard 3000A 'Assurance-opdrachten anders dan opdrachten tot controle of beoordeling van historische financiële informatie (attest-opdrachten) (assurance engagements other than audits or reviews of historical financial information (attestation engagements))' and in accordance with International Standard on Assurance Engagements 3000, 'Assurance Engagements Other than Audits or Reviews of Historical Financial Information', issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our engagement to obtain reasonable assurance to express our opinion.

We have complied with the independence and other ethical requirements of Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten' (ViO, Code of ethics for professional accountants, a regulation with respect to independence) and the 'Verordening gedrags- en beroepsregels accountants' (VGBA, Dutch Code of Ethics for Professional Accountants). The ViO and VGBA are at least as demanding as the International Code of Ethics for Professional Accountants (including International independence standards) of the International Ethics Standards Board for Accountants (the IESBA Code).

Our firm applies the 'Nadere voorschriften kwaliteitssystemen' (NVKS, Regulations for quality management systems), that is at least as demanding as the International Standard on quality management 1 (ISQM 1), and accordingly maintain a comprehensive system of quality management including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organisation's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Omada's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Omada's service commitments and system requirements based the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organisation's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Omada's system or type of service were effective throughout the period from 1 October 2025 to 30 September 2026, to provide reasonable assurance that Omada's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Utrecht, 9 November 2026

Securance Assurance Ltd.

On behalf of these,

M. Rasul
Registeraccountant

Utrecht, 09 November 2026
eIDAS Qualified Electronic Signature



M. Rasul RA



ATTACHMENT A: OMADA'S DESCRIPTION OF THE SCOPE OF THE SYSTEM

Omada

I. Scope of the SOC 3 report

I.1.1 Scope definition

The scope of this Omada SOC 3 reporting consists of the Omada Identity Cloud, which are defined in Service Level Agreement (SLA) with Clients.

In this SOC 3 reporting the processes are distinguished in ten categories, in accordance with the Trust Services Criteria (TSP Section 100). This SOC 3 report focuses on the Omada non-financial reporting controls as they relate to Security, Availability, and Confidentiality:

CC1: Control Environment

CC2: Communication and Information

CC3: Risk Assessment

CC4: Monitoring Activities

CC5: Control Activities

CC6: Logical and Physical Access Controls

CC7: System Operations

CC8: Change Management

CC9: Risk Mitigation

A1: Availability

C1: Confidentiality

A detailed overview and insight into the abovementioned categories and individual processes is included in Section III and Section IV of this report. This SOC 3 Type 2 report was conducted in accordance with ISAE 3000.

The recently acquired EmpowerID service is excluded from the scope of this SOC 3 examination. The controls and related activities associated with EmpowerID are not covered by this report, as they are subject to a separate external SOC 3 examination.

I.1.2 Processes out of scope

Low risk processes

The management of Omada excludes certain categories of processes from the scope of this SOC 3 report. These categories are: processes with a risk profile qualified as 'low' by management of Omada or risks reduced or shared with or by insurance institutions or suppliers. The criteria for the qualification of services or processes as 'low' risk for Clients, are:

Processes relating to activities insignificant for the strategic objectives of Omada.

Processes outside of the Client domain (physical area/ procedures).

Processes without direct or indirect impact on services delivered to Clients.

Processes of which risks are covered and/or controlled otherwise.

I.1.3 Carve-out

Cloud services

All control objectives and related controls provided by the cloud services provider (subservice organizations) Microsoft Azure regarding physical access, environmental security measures, backup/restore, SaaS network protection and monitoring do not form part of this SOC 3 reporting (carve-out method).

I.1.4 Trust Services Criteria requirements

The specific SOC 3 requirements relating to the Trust Services Criteria are outlined below in Table 2. These criteria are established within Omada by following the points of focus and additional criteria as outlined in the COSO 2013 framework and the Trust Services Criteria. The requirements relevant for each criteria of the Trust Services Criteria are outlined below:

Control Environment	CC 1.1	The entity demonstrates a commitment to integrity and ethical values.
	CC 1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
	CC 1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
	CC 1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
	CC 1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Communication and Information	CC 2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
	CC 2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
	CC 2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.
Risk Assessment	CC 3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
	CC 3.2	The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.
	CC 3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
	CC 3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.
Monitoring Activities	CC 4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	CC 4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
Control Activities	CC 5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
	CC 5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.
	CC 5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Logical and Physical Access Controls	CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
	CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data centre facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
	CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
	CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
	CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
	CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
System Operations	CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analysed to determine whether they represent security events.
	CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
	CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
	CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.
Change Management	CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Risk Mitigation	CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
	CC 9.2	The entity assesses and manages risks associated with vendors and business partners.
Availability	A 1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

	A 1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
	A 1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
Confidentiality	C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
	C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

Table. 2. SOC 3 Trust Services Criteria requirements

The SOC 3 requirements (control objectives) are further outlined in section **III.4 Omada Processes** and **III.5 Risk Control Framework** (COSO Framework). The detailed control descriptions resulting from the controls, procedures and monitoring of the relevant Trust Services Criteria are included in section **IV.I Control Matrix**.



ATTACHMENT B: DESCRIPTION OF THE BOUNDARIES OF THE OMADA SYSTEMS

Omada

II. Description of the Boundaries of the Omada organization

II.2.1 General

Omada A/S is a Danish software company with a powerful mission: to help organizations take control of their digital identities in an increasingly complex and regulated world. Founded in 2000 in the heart of Copenhagen, Omada began its journey as an IT security provider, quickly carving out a niche for itself by focusing on enterprise needs.

In the mid-2000s, the company made a pivotal shift, directing its efforts toward identity and access management (IAM). Recognizing the growing importance of secure and structured access to digital systems, Omada began developing cutting-edge solutions tailored to large enterprises—a move that would define its trajectory in the years to come.

By the 2010s, Omada's reputation had crossed borders. The company expanded into international markets, earning accolades for its innovative, risk-based approach to identity governance. Its solutions became especially critical for organizations in highly regulated industries such as finance, healthcare, and manufacturing, where compliance, security, and operational efficiency are non-negotiable.

A major leap forward came in 2018 with the launch of Omada Identity Cloud, a SaaS-based platform designed for scalability, rapid deployment, and seamless integration into complex IT ecosystems. This marked the beginning of a new era—Omada's cloud-first strategy began paying dividends as businesses worldwide sought agile and secure identity governance solutions.

Throughout the 2020s, Omada has continued to grow its footprint across Europe and North America, forging strategic partnerships with global enterprises. The company is now widely recognized as a leader in identity governance and administration (IGA), offering solutions that help organizations manage user access, minimize security risks, and comply with regulations such as GDPR and SOX.

At the end of September 2026 Omada acquired EmpowerID, a pioneer in AI agent governance. The acquisition brings EmpowerID's runtime agent governance capabilities into Omada, strengthening its ability to provide security controls for human, non-human and agent identities.

Omada's success lies in its unwavering commitment to innovation. Today, it is at the forefront of AI-driven identity automation and governance, pushing the boundaries of what's possible in identity security. With robust integration capabilities and a focus on efficiency, Omada continues to deliver intelligent, cost-effective solutions to meet the evolving needs of modern businesses.

Omada A/S specializes in Identity Governance and Administration (IGA) solutions designed to help enterprises manage and secure digital identities across various systems and applications. Their flagship products include:

- **Omada Identity**: An on-premises IGA solution offering comprehensive identity lifecycle management, access process automation, compliance reporting, and risk management. It provides organizations with full control over their data and security, featuring high configurability without the need for coding.
- **Omada Identity Cloud**: A cloud-based IGA-as-a-Service platform that delivers real-time visibility and control over the identity landscape. It leverages advanced analytics and automation to streamline identity workflows, enhance security, and ensure compliance.

Both solutions are designed to improve security, achieve compliance, and maximize operational efficiency by providing centralized platforms for managing identities and access across hybrid environments.

Omada's Core values:



II.2.2 Corporate objectives

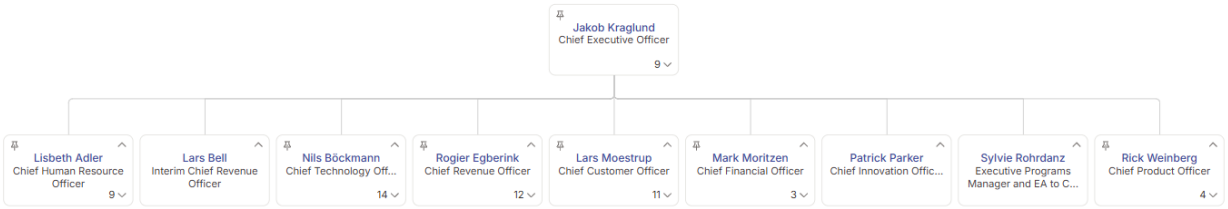
In 2026 and beyond, Omada will focus on delivering a simplified yet powerful approach to modern Identity Governance, designed to address the evolving needs of organizations navigating complex hybrid and multi-cloud environments. Omada's goal is to reduce complexity and lower costs through automated deployments, eliminating time-intensive manual processes, and leveraging Generative AI/ML to streamline implementation and support. This will enable organizations to adopt our solutions more efficiently while achieving the lowest total cost of ownership.

Omada will enhance security and decision-making by integrating advanced AI/ML behavioral insights. These insights will help organizations enforce least privileged access, improve their adaptive identity security posture, and proactively address risks. By leveraging intelligent, real-time data, we aim to empower organizations to make faster, more informed decisions to protect their critical assets.

To simplify compliance and governance processes, Omada will introduce automated compliance reporting, gap analysis with actionable recommendations, and enhanced access visibility across cloud infrastructures. These tools will provide organizations with a clear understanding of their governance posture, enabling them to meet regulatory requirements with confidence and ease.

Finally, Omada will elevate the user experience by introducing personalized AI-driven assistants and automating repetitive tasks to reduce workloads. The company's solutions will empower users with intuitive interfaces and tailored support, enabling them to focus on strategic priorities while maximizing efficiency. This holistic approach reinforces Omada's commitment to delivering innovative, efficient, and secure Identity Governance solutions that drive real value for their Clients.

II.2.3 Organization



II.2.4 IT systems

The following IT support systems are used for the internal organization of Omada:

Infrastructure

The Company utilizes Microsoft Azure to provide the resources to host the Omada Identity Cloud. The Company leverages the experience and resources of Microsoft Azure to quickly and securely scale as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the architecture within Microsoft Azure to ensure security and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure		
Production Tool	**Business Function**	**Hosted Location**
Managed Identities	Authentication	Azure
Recovery Service Vault	Backup	Azure
Content Distribution Network (CDN)	CDN	Azure
Virtual Machines	Compute	Azure
Azure App Services (WebApp / Function App)	Compute	Azure
Kubernetes	Containerization	Azure
Azure Container Registry	Containerization	Azure
SQL Databases	Client data storage	Azure
Public/Private DNS	DNS Addresses	Azure
Load Balancer	Load Balancer	Azure
Log Analytics / App Insights	Logging / Metrics	Azure

Azure Service Bus	Messaging	Azure
Event Hub / Event Hub Namespace	Messaging	Azure
Private Link	Network	Azure
Public IP Address	Networking	Azure
Virtual Private Network	Networking	Azure
Application Gateway (WAF)	Reverse Proxy	Azure
Key Vault	Secret Storage	Azure
Storage Accounts	Storage	Azure

Software

Software consists of the programs and software that support the Omada Identity Cloud. The list of software and ancillary software used to build, support, secure, maintain, and monitor the Omada Identity Cloud include the following applications, as shown in the table below:

Software	
Production Application	**Business Function**
Azure Defender	IDS / IPS / Anti Malware
Azure DevOps	Code Repository, Configuration Management
Fresh Service	Ticketing System
WithSecure Elements	Antimalware
DependencyAgent	VM Dependency Monitoring (processes and network connections)
Sisense Fusion Embed	Analytics Platform

In addition to the supporting systems for the internal organization Omada has various (customized) operational systems in use for Client solutions. These support in performing the services as agreed with the Client. This often is specific software and services and shall not be further detailed in this report.

All IT systems are managed by the IT departments. All systems and data are backed-up daily and kept safe. In case of emergency, there is a fallback location prepared and available (data centre).

II.2.5 Third parties

Omada use third-party Sub-processors to provide infrastructure for the Omada Identity Cloud service, and to aid in things like providing Client support and other ancillary services used by the organization, e.g., interacting with partners, prospects, and Clients. These Sub-Processors have access to personal information (PII) only to assist Omada in the processing of data which has been authorized.

Omada does not sell or otherwise share Clients personal information with any other entities.

Prior to engaging any third party, Omada performs due diligence to evaluate their privacy, security, and confidentiality practices, and executes an agreement implementing its applicable obligations.

Sub-processor	Purpose	Scope	Personal Data	Processing location
Microsoft Ireland Operations, Ltd.	Public cloud network, storage, and compute (Microsoft Azure)	Omada Identity Cloud environments in the Europe delivery zone	All data of the IGA platform as setup by Client	European Union
Microsoft Corporation	Public cloud network, storage, and compute (Microsoft Azure)	Omada Identity Cloud environments in the North American delivery zone	All data of the IGA platform only if the Client requests this in writing or activates US as an Azure region in the cloud environment	United States
Twilio SendGrid	E-mail delivery	Omada Identity Cloud environments configured for Omada to deliver system generated mails (an option in the self-service management portal)	Name and email address of selected Client admin accounts if provided by Client. The Client may use non-personal email addresses to avoid processing of personal data	European Union and United States

III. Omada Processes

The following processes are part of the scope of this SOC 3 report:

- Logical and Physical Access Controls
- System Operations
- Change Management
- Availability
- Confidentiality

III.3.1 Logical and Physical Access Controls

Omada has implemented a logical access management framework designed to safeguard the confidentiality, integrity, and availability of its systems and data. This framework is grounded in policies, automated controls, and role-based procedures that ensure access is granted appropriately and revoked in a timely manner.

Access to system resources is managed through a structured role-based authorization model. Each employee is assigned access rights based on their specific function within the organization. Authorizations are reviewed and approved by both the Management Team and the respective line managers. These rights are documented in a centrally maintained authorization table, which can only be modified following explicit instruction from the appropriate authority.

Access to sensitive data and system components is restricted to individuals whose job responsibilities require it. The asset owners oversee access and conduct reviews on an ad hoc basis, depending on the criticality of the asset. Non-personal accounts are limited to a small group of authorized users, and all access to IT systems is tied to uniquely identifiable personal accounts.

Security controls have been implemented across all company-managed devices, including the use of password managers, hard-disk encryption, and encryption of both data at rest and in transit. Multi-factor authentication is required for all system access, and stringent password policies are enforced. These policies include minimum complexity requirements, password history restrictions, expiration rules, and account lockout mechanisms after multiple failed login attempts.

Automated monitoring mechanisms are in place to track the expiry of SSL certificates, with alerts sent to relevant personnel when action is required. Inbound and outbound network traffic is restricted to what is necessary for business operations, and root account activity within cloud environments is actively monitored and reviewed for appropriateness. Remote access to production environments is only permitted through encrypted connections, and the environment is segmented to ensure that internal traffic is controlled according to business and security needs.

Access lifecycle management is governed by formal onboarding and offboarding procedures. These include checklists for provisioning and revoking access rights, which are reviewed and approved by designated functions. Access requests outside of the standard onboarding process are subject to additional approval and, if necessary, updates to the role-based authorization table. Upon termination of employment or client relationships, access is revoked in line with service level agreements, and any associated environments are deleted following a structured, ticketed process.

To protect assets beyond the office premises, mobile device management (MDM) is deployed on all company-issued and approved bring-your-own devices. This enables location tracking, remote locking and wiping, threat detection, and control over software installations.

Omada also maintains documented policies for data erasure and hardware disposal. These policies are reviewed regularly, and data is securely destroyed through methods such as digital wiping and physical destruction. All disposal activities are logged accordingly.

To detect and respond to security threats, Omada has implemented a multi-layered monitoring strategy. This includes a threat detection system to monitor web traffic, a web application firewall to protect public-facing applications, and an intrusion detection and prevention system configured to alert personnel to potential threats.

All company-managed devices are configured for automated operating system updates to ensure timely application of security patches. In addition, anti-malware software is installed and configured to perform real-time scans and behavioural analysis. These solutions are automatically updated and are capable of detecting, blocking, or containing known types of malware.

To control software usage, Omada applies an allow-by-exception or deny-by-exception policy. A list of approved software is maintained and made available to all employees. Requests for new software are submitted through a ticketing system, reviewed by a designated function, and processed in accordance with security policies.

III.3.2 System Operations

Omada has implemented system operations processes that ensure the resilience, integrity, and security of its production environment. These processes are supported by a structured vulnerability management program, robust logging and monitoring practices, and a incident response framework.

Vulnerability Management

To proactively identify and address weaknesses, Omada conducts regular vulnerability scans of its production environments in alignment with company policy and compliance obligations. These scans are conducted both broadly across the environment and specifically on external-facing systems. The organization places particular emphasis on identifying critical and high-risk vulnerabilities, which are tracked through to remediation in accordance with defined prioritization and risk-based procedures.

Complementing internal scans, Omada engages an independent third party to conduct periodic penetration testing of its production environment. These tests are also performed following any significant infrastructure or application changes. Findings are reviewed by management and remediation efforts are documented and monitored to resolution.

All vulnerability management activities are guided by a formal policy that defines expectations across the organization. This includes the monitoring and cataloguing of vulnerabilities, assigning appropriate risk levels, and prioritizing remediation efforts to reduce exposure and ensure timely response.

System Logging and Monitoring

Omada maintains a centralized logging system that captures system activity and generates alerts based on pre-defined criteria. Access to these logs is restricted to authorized personnel to maintain integrity and confidentiality.

Audit logging is configured to trace individual user activity and includes relevant metadata such as user identifiers, event types, timestamps, outcomes, and the origin of events. This enables thorough forensic analysis in the event of anomalies or incidents. Furthermore, all system components are configured to automatically log failed access attempts and other indicators of potentially unauthorized activity, ensuring comprehensive coverage of the environment.

Incident Management

Omada has established detailed incident management procedures that encompass the identification, classification, and resolution of security events. These procedures are reviewed on an annual basis and updated as needed to remain aligned with emerging threats and business changes.

The company's incident response plan outlines clear roles and responsibilities, and includes standardized processes for incident analysis, documentation, communication, and resolution. Security events are assessed to determine if they qualify as incidents. Verified incidents are assigned priority levels, tracked throughout their lifecycle, and resolved in accordance with internal policies and procedures.

For each identified incident, a post-incident review is conducted. This includes root cause analysis, evidence documentation, and a retrospective assessment to capture lessons learned. Insights from these reviews are used to refine the incident response plan and improve future response capabilities.

Omada also ensures compliance with contractual and regulatory requirements by providing timely notifications of breaches or incidents to affected stakeholders and relevant authorities. The effectiveness of the incident response plan is validated through annual testing exercises, including simulated events. Outcomes of these tests inform potential revisions to the documented response procedures.

All incidents are logged and managed by the appropriate teams, and communication with internal and external parties is handled in accordance with the company's policies, ensuring transparency and accountability throughout the incident lifecycle.

III3.3 Change Management

Omada has implemented a structured change management process to ensure that changes to systems, applications, and environments are executed in a controlled, secure, and auditable manner. This process supports system stability and the mitigation of risks associated with unauthorized or erroneous changes.

All changes are initiated and managed through a formalized workflow supported by a service management application. The application includes automated controls that ensure all change-related events are recorded in a comprehensive audit trail. This promotes accountability and traceability throughout the change lifecycle.

Version control is a critical component of Omada's change management process. A secure version control system is used to manage source code, track changes, document updates, and facilitate release labelling. Access to this system is strictly limited to authorized personnel, ensuring the integrity and confidentiality of development assets.

During refinement meetings, designated functions and the development team assess backlog items for relevance and adequacy. Acceptance criteria are clearly defined before items are processed in the service management system. The product team reviews dependencies and required resources, and determines which stories will be included in the upcoming development sprint, typically executed on a bi-weekly cadence.

Changes to the codebase are subject to mandatory peer review and approval before deployment. This review must be conducted by someone other than the original developer, ensuring segregation of duties. Automated enforcement mechanisms—such as branch protection rules in the version control system—support compliance with this requirement.

All changes are tested in environments that are strictly segregated from the production environment. These environments are protected by access controls, and sensitive production data is never used for testing or development purposes. Instead, anonymized or synthetic test data is utilized to preserve confidentiality. Evidence of testing, including criteria and results, is documented and retained to provide assurance over the effectiveness of pre-deployment validations.

Final approval for deployment to production is granted only by authorized personnel, and deployment privileges are limited in line with segregation of duties principles. This ensures that only individuals with the appropriate authority and knowledge are able to implement changes in the live environment.

To maintain the security posture of its applications, Omada integrates static application security testing (SAST) into its CI/CD pipeline. This allows for early detection of vulnerabilities in the source code. When vulnerabilities are identified, appropriate remediation actions are taken prior to the release, based on the risk and nature of the findings. Additionally, Omada maintains a software update management process that ensures critical patches and application updates are applied to all approved software in a timely manner. This minimizes the risk of exploitation due to outdated components and supports the overall stability and security of Omada's technology environment.

III.3.4 Availability

Omada has established a framework to ensure the ongoing availability and resilience of its systems and services. The company's approach to availability management is built on a combination of proactive capacity planning, resilient infrastructure design, automated monitoring, and comprehensive backup and disaster recovery procedures.

Capacity and Performance Management

To effectively manage system performance and meet user demand, Omada continuously monitors processing capacity and resource utilization. This real-time visibility enables the organization to identify potential constraints early and scale resources proactively to avoid service disruptions.

Omada leverages modern cloud capabilities, including load balancing and auto-scaling. Incoming application traffic is automatically distributed across multiple instances and availability zones using a load balancer. Auto-scaling configurations ensure that additional cloud resources are dynamically provisioned when pre-defined thresholds are reached, allowing the platform to seamlessly handle fluctuations in workload.

Production systems and cloud-based resources are under continuous monitoring, supported by automated alerts triggered based on predefined conditions. When events are detected, they are triaged according to established protocols to determine severity and impact. Where appropriate, events are escalated and managed through the incident response process, ensuring timely resolution.

Backup and Recovery

To safeguard critical data and systems, Omada has implemented a comprehensive backup strategy governed by a documented backup policy. This policy outlines requirements for the frequency, retention, and scope of backup operations for information, software, and systems.

Backups of production data are performed at least daily and are configured in line with defined retention periods. Critical systems are backed up consistently to ensure data recoverability in the event of a disruption. Automated notifications are generated in the event of a backup failure. These alerts are routed to designated personnel, who investigate and resolve issues in accordance with internal procedures.

Omada further reinforces resilience by deploying and replicating business-critical resources across multiple availability zones or regions. This geographical distribution supports high availability and ensures operational continuity even in the event of localized failures.

Disaster Recovery and Testing

The organization maintains a documented disaster recovery plan that outlines procedures for restoring systems and services following a major disruption. The plan identifies critical systems and includes the roles and responsibilities necessary to ensure an effective response. Disaster recovery tests are conducted at least annually to validate the effectiveness of recovery strategies. Results and lessons learned from these exercises are documented, and the plan is updated accordingly to reflect evolving requirements and best practices.

In addition to testing recovery processes, Omada also performs periodic tests to verify the integrity and recoverability of backup data. This ensures that data can be successfully restored when needed and supports confidence in the company's data protection capabilities.

Client data is given specific consideration within Omada's backup policies. Requirements for the backup and recovery of Client data are clearly documented to ensure alignment with contractual obligations and industry standards.

III.3.5 Confidentiality

Omada has established policies and procedures to ensure that confidential information is appropriately identified, handled, and disposed of in line with the organization's confidentiality objectives and applicable legal or contractual requirements.

Confidential information is identified and maintained according to internal data classification and handling policies. These policies define what constitutes confidential information and provide guidance on how such data should be protected throughout its lifecycle—whether at rest, in use, or in transit. Employees are trained to recognize and manage confidential information according to their roles and responsibilities, thereby reinforcing a culture of data sensitivity and integrity.

To safeguard information at the end of its lifecycle, Omada has implemented a formal data removal procedure. The secure disposal of physical storage media and devices containing confidential data is handled

by a certified third-party service provider. This process includes the issuance of certificates of destruction, which record key details such as the serial numbers of disposed components. These certificates serve as verifiable evidence that the data was permanently destroyed in a secure and compliant manner.

IV. Complementary user entity controls

The Omada Identity Cloud is designed with the assumption that certain complementary user entity controls are operating effectively at the user entities. This paragraph describes the complementary user entity controls that are necessary to achieve the control objectives stated in the description of Omada Identity Cloud and also identifies the control objectives to which the complementary user entity controls relate. Omada is responsible for the Omada Identity Cloud for its customers.

The user control considerations are aspects of the control system for which the user organization is responsible. These include the following:

- Employees and contractors using Omada's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services;
- Functional management, including authorizing own staff, for the relevant applications (CC6.2 and CC6.3);
- Informing Omada on relevant administrative decisions, policy changes and changes in circumstances relating to the services of Omada;
- Physical and logical security to computers is in place (CC6.1 and CC6.2);
- User management (granting, revoking and changing authorizations) is in place. Changes in authorizations (granting, revoking or changing authorizations) are communicated to Omada (CC6.2 and CC6.3);
- Personnel are trained to use the system in a correct way (CC1.4);
- Internal procedures and instructions regarding use of the system are in place (CC1.3 and CC2.2);
- Incidents are being reported as quickly as possible and by using the correct process and communication paths (CC2.3);
- Changes in the used software are adopted and implemented within the agreed time frame (CC8.1);

The nature of the services of Omada implies that within this context, regarding the user control considerations the client must:

- If applicable, provide adequate physical and logical access to their own software/hardware which is related to services provided by Omada;
- Manage user/password controls of the user applications.

To ensure that personal information can only be entered in the Omada Platform to the extend necessary to achieve the goal, only required information can be entered.

SECURANCE

Office The Netherlands

Reactorweg 47

3542 AD Utrecht
The Netherlands

+31 (0)30 280 08 88

info@securance.com

www.securance.com

Office United Kingdom

63-66 Hatton Garden

EC1N 8LE London

United Kingdom

+44 (0)20 351 446 56

info@securance.com

www.securance.com