# System and Organization Controls (SOC) 3 Report Omada A/S's Identity Cloud Relevant to Security, Availability, and Confidentiality For the Period April 1, 2023, to March 31, 2024

# TABLE OF CONTENTS

# INDEPENDENT SERVICE AUDITOR’S REPORT

## INDEPENDENT SERVICE AUDITOR’S REPORT ON A SOC 3 EXAMINATION

To: Omada A/S

### Scope

We have examined Omada A/S’s (‘Omada) accompanying assertion titled “ Omada A/S’s Management Assertion” (assertion) that the controls within Omada’s Identity Cloud (system) were effective throughout the period April 1, 2023, to March 31, 2024, to provide 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) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022) in* AICPA, *Trust Services Criteria*.

### Service Organization’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 assertion, Omada is responsible for selecting, and identifying in its assertion, 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.

### Service Auditor’s Responsibilities

Our responsibility is to express an opinion, based on our examination, on management’s assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization’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 service criteria.

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Omada's service commitments and system requirements based on 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 organization'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 Platform were effective throughout the period April 1, 2023, to March 31, 2024, 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.

Insight Assurance LLC

Tampa, Florida
July 3, 2024

# OMADA A/S' MANAGEMENT ASSERTION

**OMADA A/S’ MANAGEMENT ASSERTION**

We are responsible for designing, implementing, operating, and maintaining effective controls within Omada A/S’s (‘Omada’) Identity Cloud throughout the period April 1, 2023, to March 31, 2024, to provide 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) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022),* in AICPA *Trust Services Criteria*. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2023, to March 31, 2024, to provide reasonable assurance that Omada’s service commitments and system requirements were achieved based on the applicable trust services criteria. Omada’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2023, to March 31, 2024, to provide reasonable assurance that Omada’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Omada A/S
July 3, 2024

# ATTACHMENT A DESCRIPTION OF THE BOUNDARIES OF THE OMADA IDENTITY CLOUD

## ATTACHMENT A

## OMADA A/S’S DESCRIPTION OF THE BOUNDARIES OF ITS OMADA IDENTITY CLOUD

### SERVICES PROVIDED

Omada is a Software-as-a-Service (SaaS) company. Omada offers the Omada Identity Cloud, a cloud-based Identity Governance and Administration (IGA) solution which helps organizations enable and secure digital identities for all users, applications, and data, while also allowing organizations to provide automated access technology assets and manage potential security and compliance risks at the same time.

### INFRASTRUCTURE

The Company utilizes Azure to provide the resources to host the Omada Identity Cloud. The Company leverages the experience and resources of 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 Azure to ensure security and resiliency requirements are met.

| 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 | Customer 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 | |
|---|---|
| **System/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 |

## PEOPLE

The Company develops, manages, and secures the Omada Identity Cloud via separate departments. The responsibilities of these departments are defined in the following functional areas:

**Executive Management (CEO/CTO):** Responsible for overseeing company-wide activities, establishing, and accomplishing goals, and managing objectives.

**Technical Development (Developers):** Responsible for the development, testing, deployment, and maintenance of new code for Omada Identity Cloud.

**Operations:** Responsible for business operations.

## DATA

Data is categorized into the following major types of data used by The Company:

| Data | | |
|---|---|---|
| **Category** | **Description** | **Examples** |
| Customer data | All data of the IGA platform as setup by customer. | Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the Omada Identity Cloud production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet. |

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements. Customer data is captured and retained, to be utilized by Omada in delivering its managed IT Services and Cybersecurity Solutions Services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Omada has policies and procedures in place for proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

### PROCEDURES

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by the change control board.

# ATTACHMENT B
# PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

## ATTACHMENT B

## PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Omada designs its processes and procedures related to the Content Cloud software to meet its objectives for its services. Those objectives are based on the service commitments that Omada makes to customers, the laws and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Omada has established for the services. The content services of Omada are subject to the Security, Availability, and Confidentiality criteria of the trust services categories for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*TSP section 100*).

Security, availability, and confidentiality commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offered provided online.

### Security Commitments

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Content Cloud software and the Omada service are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Segregated operating environments for each customer. Individual environments are created and maintained with each customer's data and access restrictions.
- Multiple types of security tools are integrated into the platform architecture.

### Availability Commitments

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities.
- Operational procedures supporting the achievement of availability commitments to user entities.

### Confidentiality Commitments

Confidential commitments to customers are documented and communicated in service level agreements and other customer agreements, as well as in the description of the service offered provided online. Confidentiality commitments are standardized and include, but are not limited to, the following:

- All customer content processed and managed by Omada is treated as confidential information. Procedures are in place to identify and categorize this content when it is received or created and to assign the appropriate retention period and storage policy.
- Procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information.
- Procedures are in place to identify and destroy confidential information requiring destruction when the end of the retention period is reached based on contract requirements.