Omada A/S

System and Organization Controls SOC 2 Type 2 Report

Report on the Description of Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System and the Suitability of Design and Operating Effectiveness of Controls Relevant to Security and Availability

Throughout the Period October 1, 2020 to March 31, 2021

Contents

Section 1: Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security and Availability

To: Management of Omada A/S

Scope

We have examined Omada A/S's ("Omada") accompanying description of Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System, found in Section 3 titled "Description of Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System" throughout the period October 1, 2020 to March 31, 2021 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2020 to March 31, 2021, to provide reasonable assurance that Omada's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Omada uses subservice organizations to provide certain functions as indicated in the table below. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Omada, to achieve Omada's service commitments and system requirements based on the applicable trust services criteria. The description presents Omada's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Omada's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Subservice Organization	Services Provided to Omada A/S
Microsoft Azure	Microsoft Azure is Omada's cloud hosting provider and serves as the hosting platform for Omada's infrastructure. Microsoft Azure tooling also performs critical functions such as backups, logging, and monitoring.
Microsoft 365	Microsoft 365 provides primary email service and document repository services.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Omada, to achieve Omada's service commitments and system requirements based on the applicable trust services criteria. The description

presents Omada's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Omada's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

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. In Section 2, Omada has provided the accompanying assertion titled "Assertion of the Management of Omada A/S." (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Omada is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves—

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in 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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating 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.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in Section 4, "Information Provided by the Service Auditor" of this report.

Opinion

In our opinion, in all material respects—

a. the description presents Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System that was designed and implemented throughout the period October 1, 2020 to March 31, 2021 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period October 1, 2020 to March 31, 2021 to provide reasonable assurance that Omada's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Omada's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period October 1, 2020 to March 31, 2021 to provide reasonable assurance that Omada's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organizations controls and complementary user entity controls assumed in the design of Omada's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4 is intended solely for the information and use of Omada; user entities of Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System during some or all of the period October 1, 2020 to March 31, 2021, business partners of Omada subject to risks arising from interactions with Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.

- Complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than the specified parties.

Grassi & Co, CPAs, P.C.

GRASSI & CO., CPAs, P.C.

Jericho, New York
June 22, 2021

Section 2: Assertion of the Management of Omada A/S

We have prepared the accompanying description of Omada A/S's ("Omada") Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System titled, "Description of Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System" throughout the period October 1, 2020 to March 31, 2021 ("description") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"). The description is intended to provide report users with information about Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System that may be useful when assessing the risks arising from interactions with Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System, 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 relevant to security and availability ("applicable trust services criteria") set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Omada uses the following subservice organizations:

Subservice Organization	Services Provided to Omada A/S
Microsoft Azure	Microsoft Azure is Omada's cloud hosting provider and serves as the hosting platform for Omada's infrastructure. Microsoft Azure tooling also performs critical functions such as backups, logging, and monitoring.
Microsoft 365	Microsoft 365 provides primary email service and document repository services.

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Omada, to achieve Omada's service commitments and system requirements based on the applicable trust services criteria. The description presents Omada's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Omada's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Omada, to achieve Omada's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

We confirm, to the best of our knowledge and belief, that—

1) The description presents Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System that was designed and implemented throughout the period October 1, 2020 to March 31, 2021 in accordance with the description criteria.

2) The controls stated in the description were suitably designed throughout the period October 1, 2020 to March 31, 2021 to provide reasonable assurance that Omada's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Omada's controls throughout that period.

3) The controls stated in the description operated effectively throughout the period October 1, 2020 to March 31, 2021 to provide reasonable assurance that Omada's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Omada's controls operated effectively throughout that period.

Signature: 

Title: CISO @Omada

Section 3: Description of Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System

Overview of the Company

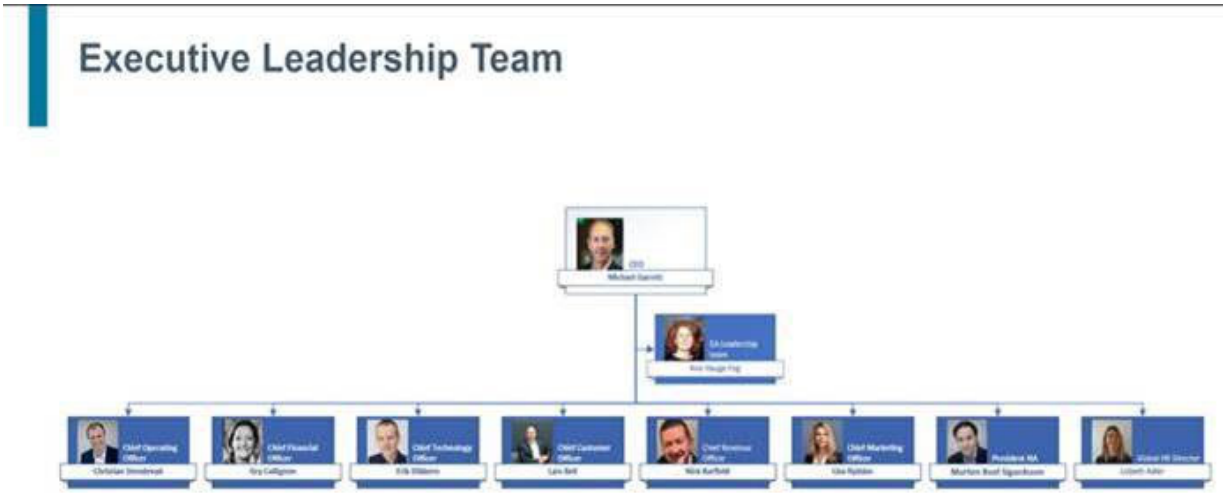
Omada A/S ("Omada") is an identity governance platform. Omada provides Omada Identity Cloud, an enterprise SaaS solution. Omada also provides Omada Identity, an on-premise solution for identity and access management with portability for future cloud adoption. Policy and role reporting, along with audit support for identity and access management, are further supported.

Omada was formed in 2000.

Management Philosophy

Omada's organizational structure provides a framework for planning, executing and controlling business operations. The organizational structure assigns roles and responsibilities to provide for adequate staffing, efficiency of operations and the segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel via an organizational chart that is updated automatically each time an employee is hired. In addition, Omada has established a board of directors that is independent from management; the board meets on a periodic basis to provide oversight over internal controls. Omada follows a structured onboarding process to assist new employees as they become familiar with processes, systems, policies and procedures. Omada places emphasis on ethics and communication within the organization.

The organization's responsibilities are delineated along departments and reporting and supervisory roles, as follows



Commitment to Compliance and Ethics

Management communicates and oversees the implementation of the Code of Business Ethics and Conduct to new and current employees via a written Code of Conduct. Employees receive the Code of Conduct upon hire and annually thereafter and sign the Employee Acknowledgement form to confirm that they have received, read, and understand the contents.

The Code of Conduct states the core values of the company: Ambition, Teamwork, Constant Care, and Creating Value. The Code of Conduct also describes core practices at Omada such as business conduct, anti-corruption, anti-bribery, anti-harassment anti-discrimination, a commitment to diversity and inclusion, and a commitment to sustainable practices. The Code of Conduct further describes a Whistle Blower policy in which reporting methods and investigatory procedures are discussed in detail.

Omada commits to the highest level of integrity in dealing with its customers, vendors, and workforce. This commitment to integrity is promulgated with established policies that cover a variety of business and integrity objectives. Omada protects all sensitive and confidential data in accordance with federal and state laws.

As part of the compliance effort, Omada maintains a complete inventory list of all third parties, identifying the risks associated with each third party; the inventory is reviewed on an annual basis for completeness and accuracy. Such third parties are contractually required to maintain relevant elements of information security policy requirements, and to report cyber security incidents to Omada, in a timely manner.

Description of the Control Environment

Omada has implemented controls to protect its data using people, processes, and technology.

Personnel

Omada has implemented controls to ensure that the workforce members access the least amount of information possible in order to perform their job duties and are trained on their personal responsibility to protect information. Omada requires that every new employee undergo a background screening that includes a criminal background check performed by an independent agency prior to hire in accordance with the Omada Employee Screening Procedure. After an employee is onboarded, the employee is only granted access to systems and privileges required for them to perform their job functions in accordance with the principle of least privilege.

Process Controls

Omada has developed and implemented methodologies to support the protection of sensitive information. These processes include change management, incident response, onboarding and offboarding personnel, and risk assessment.

Technology Controls

Omada uses a variety of technical controls to protect its information. Through Microsoft Azure Cloud, Omada encrypts data at rest and in transit using a minimum of American Encryption Standard (AES) 256 and Transport Layer Security (TLS) 1.2. Omada also enforces role-based access control (RBAC), uses logging and monitoring to detect and alert the staff to potential security issues, and deploys firewalls and anti-virus to secure endpoints.

Risk Management

Omada's Risk Management Committee is comprised of senior leadership. The committee was established to coordinate the risk assessment and management efforts. The committee ensures that:

a) risks arising from both internal and external sources are identified and evaluated,
b) controls are properly designed and implemented to address all areas as appropriate, and
c) controls operate effectively to achieve the entity's risk management objectives.

The Risk Management Committee meets on a quarterly basis and meeting minutes from the meetings are maintained.

Areas evaluated include systems development, computer operations, program changes, and access to programs and data.

Risk Assessment Process

Policies and procedures outlining the objectives and procedures for risk assessment are documented, made available to employees, and reviewed by management on an annual basis.

Omada's Risk Management Committee has performed a risk assessment during the design and implementation of the control objectives and related controls described in this report. As part of its risk assessment, the Risk Management Committee identified the threats and vulnerabilities relevant to the security of Omada's business operations and rated the risk posed by each identified vulnerability. This rating allowed for the design and implementation of controls to mitigate the most significant risks to the security of Omada's service.

The risk assessments are performed by the Risk Management Committee annually, at a minimum, or in response to any major updates to the product, client base, or business plan.

When conducting a risk assessment, the Risk Management Committee first identifies threats and vulnerabilities relevant to the security of business operations. The Risk Management Committee then – for each identified vulnerability – considers:

a) The likelihood of impact (i.e., the likelihood of the vulnerability being exploited), and
b) The severity of impact (i.e., how damaging an exploitation of the vulnerability would be).

These estimations of impact potential and impact severity are then used in conjunction to establish a risk ranking for each vulnerability. Findings and recommended changes to internal processes and controls are documented and implemented in a timely manner.

Information and Communication

Omada records and tracks internal assets in the Inventory List and identifies risks associated with each third party. This list includes internal systems supporting application functionality, development and deployment and those used to facilitate and track communication.

Critical Vendors:

Microsoft Azure Cloud: Omada contracts with Azure (Microsoft) as their cloud hosting provider and serves as the hosting platform for Omada's infrastructure. Microsoft Azure tooling also performs critical functions such as backups, logging, and monitoring.

Microsoft 365: Omada uses Microsoft 365 as the primary email provider and document repository.

Internal Communication and Information Systems

Omada has implemented various methods of internal communication to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employees, as well as annual training programs tailored to employees' roles and responsibilities.

Communication with Customers and Third Parties

Various web-based conferencing platforms are used to communicate with customers and third-party vendors. These occur on an “as needed” basis based on customer or third-party request.

Major changes to the system and incidents affecting the security and availability of user information are communicated to third parties in a timely manner.

Monitoring

Monitoring identified risk is done by the Risk Management Committee, as described above. This monitoring activity is iterative and occurs quarterly as part of the regular cycle of the risk management process.

Omada utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. Omada’s monitoring tools are implemented to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. Data loss prevention policies are enabled on Microsoft Azure and Microsoft 365. Monitoring software is configured to send alerts to IT personnel if an issue is detected.

The entity performs internal vulnerability scans in real time; the software is configured to create alerts for identified vulnerabilities, and identified vulnerabilities are researched and resolved.

Control Activities

Information Security

An Information Security Policy has been formally documented and implemented to provide policies and procedures governing the protection of confidential and sensitive information. The Information Security Policy is available on Omada’s platform.

The Information Security Policy is reviewed and updated by management on an annual basis. The Information Security Policy defines information security responsibilities for all personnel. Employees are required to sign the Information Security Policy, which includes guidelines for workplace conduct, upon hire. Where security responsibilities apply, roles are related to the policy and procedures that define their activity within their associated responsibilities. Security Awareness Training is provided to all employees upon hire and on an annual basis thereafter to ensure that personnel understand their security roles and responsibilities.

Omada also communicates security roles and responsibilities to vendors and other third parties. Marketing and contractual materials that describe the services and scope of work provided to clients are documented and maintained to ensure that employees, contractors, vendors, and clients understand their roles and responsibilities.

Secure Software Development

Omada applies a systematic approach to software development so that changes to customer impacting services are reviewed, tested, approved, and well communicated. Prior to deployment to production environments, changes are:

- Developed: in a development environment that is segregated from the production environment. Customer content is not used in test and development environments.
- Reviewed: by peers for technical aspects and appropriateness.

- Tested: to confirm the changes will behave as expected when applied and not adversely impact performance.
- Approved: by authorized team members to provide appropriate oversight and understanding of business impact.

Rollback procedures are documented so that team members can revert back to the previous state if needed. Customer content is not used in test and development environments.

Omada's change management tickets are managed and documented with required approval in Clubhouse.

Identity and Access Management

Access management processes exist so that Omada's employee and contractor user accounts are added, modified, or disabled in a timely manner and are reviewed on a periodic basis. In addition, password configuration settings for user authentication to Omada's systems are managed in compliance with Omada's Password Policy, which is part of the Information Security Policy.

Users must be approved for logical access by senior management prior to receiving access to Omada's systems. Management authorization is required before employment is offered and access is provided by appropriate IT personnel. Users must also be assigned a unique ID before being allowed access to system components. User IDs are authorized and implemented as part of the new hire onboarding process. Access rights and privileges are granted to user IDs based on the principle of least privilege and RBAC protocols. Access is limited to that which is required for the performance of job duties for individual users, and generic access by Omada's employees is not allowed.

Any access to the cloud environment is granted by appropriate personnel on a daily basis and is automatically revoked at the end of each day.

Changes to user access to the network and in-scope applications, databases, and servers for transferred employees are authorized by management and are modified by appropriate personnel within one business day of the transfer date. Access to systems for terminated users is removed within one business day of termination. Administrative access to systems is restricted to employees with a business need or as a requirement of their job function.

User access to the network and in-scope applications, databases, and servers is reviewed on a quarterly basis by management; inappropriate user access identified is removed in a timely manner.

Third-Party Risk Management

When choosing a new vendor, Omada follows a standard due diligence process. Third-party providers are researched, interviewed, reviewed internally, and then selected. Before entering into a contract with a new high risk or critical risk vendor, management approves the results of the review. A statement of work is required to define the terms of service, timelines, and deliverables. Service level agreements (SLAs) are recommended to define performance consistency, shared defined responsibilities, and system redundancy, if applicable. Once implemented, third-party service providers are monitored. Omada periodically obtains independent attestations, including SOC reports, for identified key vendors and performs reviews

to evaluate the impact of the findings on the entity's control objectives. Omada requires third parties to sign a nondisclosure agreement (NDA) prior to sharing information with them.

In addition, contracts must also include clauses stipulating that the Third-Party Vendor will comply with applicable laws, regulations, and regulatory guidance. Where sensitive and confidential information is shared, the contract must include clauses requiring data security responsibility and notification in the event of a breach. The Third-Party Vendor contract defines the types of information gathered by Omada as well as the uses for that information within the organization. This includes specifics on confidential information. Contracts and changes to contracts are approved by the entity and third party in a timely manner.

Perimeter Security

Omada undertakes various steps and implements controls to secure its application's perimeter:

- Anti-virus protection is implemented across all relevant systems; the software scans endpoints on a daily basis, and updates to the software are automatically installed on endpoints.
- An application penetration test of Internet facing applications and servers is performed on an annual basis and covers risks such as poor input validation, cross-site scripting and SQL injection vulnerabilities. Identified risks are researched and resolved in a timely manner.
- The RBAC requires that the use of shared user IDs for privileged access to information systems is prohibited for any systems supporting or processing services for confidential and sensitive data. This privileged access is further restricted to the appropriate users who require this level of access to perform their job responsibilities, and this access is periodically reviewed.
- All access rights are removed in a timely manner upon termination of employment, contract or agreement.
- Where Public Key Infrastructure (PKI) is used, it is protected by "hardening" the underlying operating system(s) and restricting access to Certificate Authorities.
- Firewall devices and software are implemented to secure network perimeters using a limited approval ruleset. Firewalls are monitored regularly.

Data Protection

Policies and procedures for data protection are documented, made available to employees on the Omada platform, and reviewed by management on an annual basis.

Omada maintains a system of controls and requirements to prevent unauthorized access, modification, destruction, or disclosure of sensitive and confidential data. Omada classifies its data by identifying the types of data that are being processed and stored and determining the sensitivity of the data and the likely impact arising from compromise, loss, or misuse. Unless otherwise required by law, Omada retains Sensitive & Confidential Data only for as long as necessary to fulfill the purposes for which it is collected and processed or to meet its legal and client contractual obligations. Record retention and storage procedures are reviewed on an annual basis; data identified that has been retained past its retention period is securely disposed.

Omada's Information Security Policy defines the appropriate encryption standards, which are based on Federal Information Processing Standards (FIPS), National Institute of Standards (NIST), and Open Web Application Security Project (OWASP) recommendations.

Omada requires secure sockets layer (SSL) for Application Gateways. Internet Protocol Security (IPSec) is enabled. Transparent data is encrypted with a service managed key in Microsoft Azure. TLS 1.2 or greater is required.

Omada enables Data Loss prevention in all environments to protect sensitive data.

Physical Security and Environmental Controls

Controls are in place to protect against external and environmental hazards, such as fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters. The Omada infrastructure is hosted in Microsoft Azure, which is responsible for the hosted data's environmental security. All Omada data is physically secured by Microsoft Azure, the data hosting provider. Microsoft Azure provides sufficient physical controls to protect sensitive data, and Omada regularly reviews Microsoft Azure audit reports to ensure that their security and compliance needs are met.

Change Management

A Product Change Management Policy has been formally documented and implemented to guide the processes of change request, documentation, review, evaluation, approval, scheduling, testing, and implementation. The policy is reviewed by management on an annual basis and is made available to employees on the Omada platform. Changes that may affect system availability and system security are communicated to management and any partners who may be affected via email.

Omada requires a branch strategy be followed in the change management process. Each change in a branch undergoes unit and integration tests, as well as an automated testing suite. Changes are documented in a form that ensures each change is easily identifiable and limited in scope. Changes are made in a manner which prevents malicious activity, by requiring the change initiator to be different from the change approver, thus reducing the risk of fraud without collusion.

Changes are documented in a formalized ticketing system and are authorized, tested and approved prior to migration into the production environment. The user who develops and tests a change cannot also migrate the same change into production. Separate development, test, and production environments are maintained.

System configuration standards are formally documented and implemented to ensure that all systems and network devices are properly and securely configured. CIS and NIST hardening standards, as well as configurations in Microsoft Azure, are used as a basis for Omada's system configuration standards. Servers and workstations are configured to automatically download and apply patches.

Incident Response

An Incident Response Policy and Procedures manual has been formally documented and implemented to guide preparation, detection, response, analysis and repair, communication, follow-up, and training for any class of security breach or incident. The policy is reviewed on an annual basis by management and is made available to employees on the Omada platform. The responsibilities in the event of a breach, the steps of a breach, and the importance of information security are defined for all employees. The Incident Response Policy is made available to employees via the Omada platform and is reviewed and updated by management on an annual basis. The Incident Response Team employs industry-standard diagnosis procedures (such as incident identification, registration and verification, as well as initial incident classification and

prioritizing actions) to drive resolution during business-impacting events. Omada's Incident Response Plan is tested on an annual basis.

Omada reviews, triages, and communicates all incident alerts to Omada whereupon the Incident Response Team starts the incident response process. Post-mortems are convened after any significant operational issue, regardless of external impact. Documentation of the investigation is conducted to determine that the root cause is captured and that preventative actions may be taken for the future.

Training and Testing

Upon hiring, and annually thereafter, all employees must successfully complete training courses covering basic information security practices that support the functioning of an effective risk management program. The training courses are designed to assist employees in identifying and responding to social engineering attacks (phishing, pharming, and tailgating) and in avoiding inappropriate security practices (for example, writing down passwords or leaving sensitive material unattended).

Performance evaluations are performed for employees by management annually. If an employee is found to be violating company policies, additional training is provided, or other disciplinary actions are taken.

Data Backup and Recovery

Omada has developed and implemented a comprehensive data backup and recovery process to ensure that all sensitive and confidential data is backed up, retained, and recoverable based on services provided by Microsoft Azure in their cloud hosting platform. Backups for databases and servers are configured to be performed on a daily basis; access to backups is restricted to appropriate personnel. Following a significant business disruption, Omada immediately assesses the extent to which the disruption corrupted or lost any of the critical product data. If required, Omada will immediately restore corrupted or lost data from the most recent backup or restore service by migrating to another region to deploy services from.

Business Continuity and Disaster Recovery

Omada has a Business Continuity and Disaster Recovery Plan (BCDRP), which is overseen by the CEO and the Risk Management Committee, to document standards and procedures for responding to and recovering from a significant business disruption. Disaster Recovery involves the policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a business disruption. The BCDRP considers the company's data architecture and deployment models; physical locations of operations; critical support and development systems; and reliance on third parties. Omada's standards align with the business continuity objectives of continuous delivery and service.

Omada is committed to:

- Providing its partners and users with an excellent user experience, free of service disruptions or product downtime.
- Continual and open communication with clients, partners, employees, and suppliers during a service disruption include SLAs to restore service.
- Robust oversight of third-party suppliers critical to its products' availability.

The Business Continuity and Disaster Recovery Plan is tested on an annual basis and updated in response to improvements identified during testing.

Complementary Subservice Organization Controls

Omada's controls related to its Information Technology Environment and Operations System cover only a portion of overall internal control for each user entity of Omada. It is not feasible for applicable trust services criteria related to security and availability to be met solely by Omada. Therefore, each user entity's internal control for security and availability must be evaluated in conjunction with Omada's controls described in Section 4 of this report, taking into account related complementary subservice organization controls (CSOCs) expected to be implemented at the subservice organization that follows.

	CSOCs	Relevant Trust Services Criteria
	Microsoft Azure	
1.	Microsoft Azure is responsible for maintaining logical security over the servers and other hardware devices upon which Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System is hosted.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.6
2.	Microsoft Azure is responsible for notifying Omada of any security incidents related to security and confidentiality over the servers and other hardware devices upon which the Identity Cloud, the Cloud Environment, and Supporting Information Technology System is hosted.	CC 7.2
3.	Microsoft Azure is responsible for maintaining physical security over its data center housing the servers used to host the Identity Cloud, the Cloud Environment, and Supporting Information Technology System.	CC 6.4
4.	Microsoft Azure is responsible for notifying Omada of any major changes made to its system that could impact the security and confidentiality of Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System.	CC 8.1
5.	Azure is responsible for the encryption settings on the instances that contain data pertinent to Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System.	CC 5.2 CC 6.1 CC 6.6 CC 6.7 CC 6.8 CC 7.1
6.	Microsoft Azure is responsible for purging confidential data from its platform once it has reached the end of its retention period.	CC 6.5
7.	Microsoft Azure is responsible for managing the authentication settings for its platform, including providing a log-in screen for users.	CC 5.2 CC 6.1
	Microsoft 365	

	CSOCs	Relevant Trust Services Criteria
1.	Microsoft is responsible for maintaining logical security over the servers and other hardware devices upon which the document repository is located.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.6
2.	Microsoft is responsible for notifying Omada of any security incidents related to security and availability over the servers and other hardware devices upon which the document repository is located.	CC 7.2
3.	Microsoft is responsible for maintaining physical security over its data center housing the servers used to host the document repository.	CC 6.4
4.	Microsoft is responsible for notifying Omada of any major changes made to its system that could impact the security and confidentiality of Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System.	CC 8.1
5.	Microsoft is responsible for the encryption settings on the 365 instances that contain data pertinent to Omada Identity Cloud, the Cloud Environment, and Supporting Information Technology System.	CC 5.2 CC 6.1 CC 6.6 CC 6.7 CC 6.8 CC 7.1
6.	Microsoft is responsible for managing the authentication settings for its platform, including providing a log-in screen for users.	CC 5.2 CC 6.1

Complementary User-Entity Controls

The processes of Omada were designed with the assumptions that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve the criteria included in this report.

This section highlights those internal control responsibilities that Omada believes should be present for each user organization and has considered in developing its control policies and procedures described in this report. In order for user organizations to rely on the control structure's policies and procedures reported on herein, each user must evaluate its own internal control structure to determine if the following procedures are in place. Furthermore, the following list of control policies and procedures is intended to address only those policies and procedures surrounding the interface and communication between Omada and each user. Accordingly, this list does not allege to be, and is not, a complete listing of the control policies and procedures that provide a basis for the assertions underlying the report and control environments for Omada's user organizations.

	Complementary User-Entity Control	Relevant Trust Services Criteria
1.	User entities should establish and maintain controls for the initiation, modification, and termination of authorized users with access to Omada's System. User entities should review their access control at least every six months and advise Omada about any irregularities or access by unauthorized users.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.7
2.	User entities should regularly review their communication protocols for both incoming and outgoing data files and ensure that such protocols include validation that the data sent or received are encrypted and are accessible only by authorized users.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.7 CC 6.8
3.	User entities utilize only current and supported software, operating systems, and communication protocols under current support contracts with their respective vendors and are patched timely and completely in accordance with the vendors' specifications and/or other service alerts.	CC 2.3 CC 5.2 CC 6.1 CC 6.6 CC 6.7 CC 6.8 CC 7.1 CC 7.2 CC 8.1
4.	User entities are responsible for notifying Omada, in an expedient manner, when changes are made to technical, billing, or administrative contact information.	CC 2.3
5.	User entities are responsible for administrating their own users' access and strictly enforcing their password policies.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.7
6.	User entities must maintain confidential user identification information furnished to them by Omada, including any information related to password or other authentication methods.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.7
7.	User entities are responsible for developing, testing, and maintaining their own disaster recovery and business continuity plans that address their inability to access or utilize Omada's services.	CC 7.5 CC 9.1
8.	User entities are responsible for immediately reporting systems availability issues to Omada in a clear and comprehensive manner. User entities are responsible for following up with Omada if their initial notification is not acknowledged by Omada in a timely manner.	CC 7.1 CC 7.2 CC 7.3 CC 7.4 CC 7.5 CC 8.1

	Complementary User-Entity Control	Relevant Trust Services Criteria
9.	User entities are responsible for creating, maintaining, monitoring, and expediently informing Omada about their own security, including physical and cyber-security.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.4 CC 6.5 CC 6.6 CC 6.7 CC 6.8
10.	User entities remit to Omada data that has been validated, de-duplicated, authorized, and verified as correct, complete, timely, and free of output or input errors.	CC 2.1
11.	User entities process data sent by Omada and ensure that the data is validated, authorized, verified as correct, complete, timely, and free of input or output errors.	CC 2.1
12.	User entities are responsible for immediately notifying Omada of any actual or suspected information security breaches or fraud, of any nature or any kind.	CC 7.1 CC 7.2 CC 7.3 CC 7.4 CC 7.5
13.	User entities are responsible for determining whether Omada's security infrastructure is appropriate for their needs and for notifying Omada of any requested modifications.	CC 5.2 CC 6.1 CC 8.1
14.	User entities are responsible for developing policies and procedures to protect their systems from unauthorized use or unintentional modification, addition, or deletion.	CC 5.3
15.	User entities are responsible for informing Omada of any existing, modified, or new regulatory issues that may affect the services provided by Omada to the user entity.	CC 2.1
16.	User entities must comply with regulatory requirements for notification of breach under the applicable laws.	CC 6.1 CC 6.6 CC 6.7 CC 6.8
17.	User entities are responsible for planning, implementing, and monitoring a "strong password" policy on their remotely accessed resources, including Secure File Transfer Protocol (SFTP) or portal sites.	CC 5.2 CC 6.1
18.	User entities are responsible for planning, implementing, and creating strong desktop security management controls, including, but not limited to, unauthorized access to mass media storage and visual recording devices.	CC 5.2 CC 6.1 CC 6.6 CC 6.7 CC 6.8
19.	User entities are responsible for and must maintain controls over access, modification, and destruction of confidential information.	CC 6.5
20.	User entities are responsible for purging sensitive data from Omada instances that is no longer needed.	CC 6.5

Section 4: Information Provided by the Service Auditor

In planning the nature, timing, and extent of our testing of the controls specified by Omada, we considered the aspects of Omada's control environment and tested those that we considered necessary.

In addition to the tests of operating effectiveness of specific controls described below, our procedures included tests of the following components of the internal control environment of Omada:

- Management controls and organizational structure
- Risk assessment process
- Information and communication
- Control activities
- Monitoring

Our tests of the control environment included the following procedures, to the extent we considered necessary:

1. An analysis of Omada's organizational structure, including the segregation of functional responsibilities, policy statements, processing manuals and personnel controls,
2. Inquiry with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to, and applying controls, and
3. Observations of personnel in the performance of their assigned duties, or evidence thereof.

The control environment was considered in determining the nature, timing, and extent of the testing of controls and controls relevant to the achievement of the applicable trust services criteria.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity

For tests of controls requiring the use of Information Provided by the Entity ("IPE") (e.g., controls requiring system-generated populations for sample-based testing), we perform a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

1. Inspect the source of the IPE,
2. Trace or tie data between the IPE and the source, and/or
3. Inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

Trust Services Criteria and Related Controls

On the pages that follow, the description of the controls to achieve the trust services criteria have been specified by and are the responsibility of Omada. The "Test Description" and the "Test Results" are the responsibility of the service auditor. Controls which appear more than once and are mapped to multiple trust services criteria have been shaded.

Section 4.1: Trust Services Criteria and Related Controls

CONTROL ENVIRONMENT			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	**CC 1.1.1**	Employees are required to sign the Information Security Policy, which includes guidelines for workplace conduct, upon hire.
		CC 1.1.2	Management has established authority and appropriate lines of reporting for key personnel via an Organization Chart.
		CC 1.1.3	Performance evaluations are performed for employees by management annually.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	**CC 1.2.1**	Management has established authority and appropriate lines of reporting for key personnel via an Organization Chart.
		CC 1.2.2	The Company has established a Board of Directors that is independent from management; the Board meets on a periodic basis to provide oversight over internal controls.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	**CC 1.3.1**	Management has established authority and appropriate lines of reporting for key personnel via an Organization Chart.
		CC 1.3.2	The Company has established a Board of Directors that is independent from management; the Board meets on a periodic basis to provide oversight over internal controls.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**CC 1.4.1**	Upon hire, and annually thereafter, all employees must successfully complete training courses covering basic information security practices that support the functioning of an effective risk management program.
		CC 1.4.2	Prior to hire, in accordance with the Omada Employee Screening Procedure, employees are required to complete a background check performed by an independent agency.

CONTROL ENVIRONMENT			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 1.4.3	Employees are required to sign the Information Security Policy, which includes guidelines for workplace conduct, upon hire.
		CC 1.4.4	Management has established authority and appropriate lines of reporting for key personnel via an Organization Chart.
		CC 1.4.5	Performance evaluations are performed for employees by management annually.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	**CC 1.5.1**	Employees are required to sign the Information Security Policy, which includes guidelines for workplace conduct, upon hire.
		CC 1.5.2	Performance evaluations are performed for employees by management annually.

COMMUNICATION AND INFORMATION			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	**CC 2.1.1**	The Information Security policy outlining information technology roles and objectives is documented, made available to employees, and reviewed on an annual basis by management.
		CC 2.1.2	Incident response policies and procedures documenting the roles and responsibilities in the result of an incident are documented, made available to employees, and reviewed by management on an annual basis.
		CC 2.1.3	The Risk Management Committee meets on a quarterly basis to oversee the achievement of the entity's risk management objectives; meeting minutes are maintained.
		CC 2.1.4	The entity performs a Risk Assessment on an annual basis to evaluate the achievement of risk management objectives and to identify threats and vulnerabilities; findings and recommended changes to internal processes and controls are documented and implemented in a timely manner.
		CC 2.1.5	The entity maintains a complete inventory of all third parties identifying the risks associated with each third party; the inventory is reviewed on an annual basis for completeness and accuracy.
		CC 2.1.6	The entity periodically obtains independent attestations, including SOC reports, for identified key vendors and performs reviews to evaluate the impact of the findings on the entity's control objectives.
		CC 2.1.7	The entity performs internal vulnerability scans in real time; the software is configured to create alerts for identified vulnerabilities, and identified vulnerabilities are researched and resolved.

COMMUNICATION AND INFORMATION			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 2.1.8	An external penetration test is performed on an annual basis, and identified risks are researched and resolved in a timely manner.
		CC 2.1.9	Before entering into a contract with a new high risk or critical risk vendor, the entity conducts a due diligence review to help identify potential risks and management approves the results of the review.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	**CC 2.2.1**	Employees are required to sign the Information Security Policy, which includes guidelines for workplace conduct, upon hire.
		CC 2.2.2	Upon hire, and annually thereafter, all employees must successfully complete training courses covering basic information security practices that support the functioning of an effective risk management program.
		CC 2.2.3	The Information Security policy outlining information technology roles and objectives is documented, made available to employees, and reviewed on an annual basis by management.
		CC 2.2.4	Incident response policies and procedures documenting the roles and responsibilities in the result of an incident are documented, made available to employees, and reviewed by management on an annual basis.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	**CC 2.3.1**	The entity requires third parties to sign a nondisclosure agreement prior to sharing information with them.
		CC 2.3.2	New third parties sign a contract that communicates the conditions and responsibilities of third parties and includes a clause on the sharing of confidential information.

COMMUNICATION AND INFORMATION			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 2.3.3	Major changes to the system and incidents affecting the security and availability of user information are communicated to third parties in a timely manner.

RISK ASSESSMENT			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**CC 3.1.1**	Policies and procedures outlining the objectives and procedures for risk assessment are documented, made available to employees, and reviewed by management on an annual basis.
		CC 3.1.2	The Information Security policy outlining information technology roles and objectives is documented, made available to employees, and reviewed on an annual basis by management.
		CC 3.1.3	The Risk Management Committee meets on a quarterly basis to oversee the achievement of the entity's risk management objectives; meeting minutes are maintained.
		CC 3.1.4	The entity performs a Risk Assessment on an annual basis to evaluate the achievement of risk management objectives and to identify threats and vulnerabilities; findings and recommended changes to internal processes and controls are documented and implemented in a timely manner.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	**CC 3.2.1**	Policies and procedures outlining the objectives and procedures for risk assessment are documented, made available to employees, and reviewed by management on an annual basis.
		CC 3.2.2	The Information Security policy outlining information technology roles and objectives is documented, made available to employees, and reviewed on an annual basis by management.
		CC 3.2.3	The Risk Management Committee meets on a quarterly basis to oversee the achievement of the entity's risk management objectives; meeting minutes are maintained.

RISK ASSESSMENT			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 3.2.4	The entity performs a Risk Assessment on an annual basis to evaluate the achievement of risk management objectives and to identify threats and vulnerabilities; findings and recommended changes to internal processes and controls are documented and implemented in a timely manner.
		CC 3.2.5	The entity maintains a complete inventory of all third parties identifying the risks associated with each third party; the inventory is reviewed on an annual basis for completeness and accuracy.
		CC 3.2.6	The entity periodically obtains independent attestations, including SOC reports, for identified key vendors and performs reviews to evaluate the impact of the findings on the entity's control objectives.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	**CC 3.3.1**	Policies and procedures outlining the objectives and procedures for risk assessment are documented, made available to employees, and reviewed by management on an annual basis.
		CC 3.3.2	The Risk Management Committee meets on a quarterly basis to oversee the achievement of the entity's risk management objectives; meeting minutes are maintained.
		CC 3.3.3	The entity performs a Risk Assessment on an annual basis to evaluate the achievement of risk management objectives and to identify threats and vulnerabilities; findings and recommended changes to internal processes and controls are documented and implemented in a timely manner.

RISK ASSESSMENT			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	**CC 3.4.1**	Policies and procedures outlining the objectives and procedures for risk assessment are documented, made available to employees, and reviewed by management on an annual basis.
		CC 3.4.2	The Risk Management Committee meets on a quarterly basis to oversee the achievement of the entity's risk management objectives; meeting minutes are maintained.
		CC 3.4.3	The entity performs a Risk Assessment on an annual basis to evaluate the achievement of risk management objectives and to identify threats and vulnerabilities; findings and recommended changes to internal processes and controls are documented and implemented in a timely manner.
		CC 3.4.4	The entity maintains a complete inventory of all third parties identifying the risks associated with each third party; the inventory is reviewed on an annual basis for completeness and accuracy.
		CC 3.4.5	The entity periodically obtains independent attestations, including SOC reports, for identified key vendors and performs reviews to evaluate the impact of the findings on the entity's control objectives.

MONITORING ACTIVITIES			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	**CC 4.1.1**	The entity uses monitoring software to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs, and unusual system activity; the software is configured to send alerts to IT personnel if an issue is detected.
		CC 4.1.2	The Risk Management Committee meets on a quarterly basis to oversee the achievement of the entity's risk management objectives; meeting minutes are maintained.
		CC 4.1.3	The entity performs a Risk Assessment on an annual basis to evaluate the achievement of risk management objectives and to identify threats and vulnerabilities; findings and recommended changes to internal processes and controls are documented and implemented in a timely manner.
		CC 4.1.4	The entity maintains a complete inventory of all third parties identifying the risks associated with each third party; the inventory is reviewed on an annual basis for completeness and accuracy.
		CC 4.1.5	The entity periodically obtains independent attestations, including SOC reports, for identified key vendors and performs reviews to evaluate the impact of the findings on the entity's control objectives.
		CC 4.1.6	The entity performs internal vulnerability scans in real time; the software is configured to create alerts for identified vulnerabilities, and identified vulnerabilities are researched and resolved.
		CC 4.1.7	An external penetration test is performed on an annual basis, and identified risks are researched and resolved in a timely manner.

MONITORING ACTIVITIES			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC4.2	COSO Principle 17: 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.	**CC 4.2.1**	The entity uses monitoring software to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs, and unusual system activity; the software is configured to send alerts to IT personnel if an issue is detected.
		CC 4.2.2	The Risk Management Committee meets on a quarterly basis to oversee the achievement of the entity's risk management objectives; meeting minutes are maintained.
		CC 4.2.3	The entity performs a Risk Assessment on an annual basis to evaluate the achievement of risk management objectives and to identify threats and vulnerabilities; findings and recommended changes to internal processes and controls are documented and implemented in a timely manner.
		CC 4.2.4	The entity periodically obtains independent attestations, including SOC reports, for identified key vendors and performs reviews to evaluate the impact of the findings on the entity's control objectives.
		CC 4.2.5	The entity performs internal vulnerability scans in real time; the software is configured to create alerts for identified vulnerabilities, and identified vulnerabilities are researched and resolved.
		CC 4.2.6	An external penetration test is performed on an annual basis, and identified risks are researched and resolved in a timely manner.
		CC 4.2.7	Major changes to the system and incidents affecting the security and availability of user information are communicated to third parties in a timely manner.

CONTROL ACTIVITIES			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	**CC 5.1.1**	The Information Security policy outlining information technology roles and objectives is documented, made available to employees, and reviewed on an annual basis by management.
		CC 5.1.2	The Risk Management Committee meets on a quarterly basis to oversee the achievement of the entity's risk management objectives; meeting minutes are maintained.
		CC 5.1.3	The entity performs a Risk Assessment on an annual basis to evaluate the achievement of risk management objectives and to identify threats and vulnerabilities; findings and recommended changes to internal processes and controls are documented and implemented in a timely manner.
		CC 5.1.4	New third parties sign a contract that communicates the conditions and responsibilities of third parties and includes a clause on the sharing of confidential information.
		CC 5.1.5	The entity maintains a complete inventory of all third parties identifying the risks associated with each third party; the inventory is reviewed on an annual basis for completeness and accuracy.
		CC 5.1.6	The entity periodically obtains independent attestations, including SOC reports, for identified key vendors and performs reviews to evaluate the impact of the findings on the entity's control objectives.

CONTROL ACTIVITIES			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	**CC 5.2.1**	Users are required to log-in to the network and in-scope applications, databases, and servers using a unique user ID and password.
		CC 5.2.2	Passwords for the network and in-scope applications, databases, and servers are configured to meet the entity's standards.
		CC 5.2.3	New user access to the network and in-scope applications, databases, and servers is authorized by the hiring manager prior to access being granted by appropriate personnel.
		CC 5.2.4	Changes to user access to the network and in-scope applications, databases, and servers for transferred employees are authorized by management and are modified by appropriate personnel within one business day of the transfer date.
		CC 5.2.5	Access to the network and in-scope applications, databases, and servers for terminated users is removed within one business day of termination.
		CC 5.2.6	Administrative access to the network and in-scope applications, databases, and servers is restricted to appropriate personnel.
		CC 5.2.7	User access to the network and in-scope applications, databases, and servers is reviewed on a quarterly basis by management; inappropriate user access identified is removed in a timely manner.
		CC 5.2.8	Firewall devices and software are implemented globally to secure network perimeters using a limited approval ruleset.

CONTROL ACTIVITIES			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 5.2.9	Anti-virus software is installed on all servers and workstations and is configured to scan endpoints in real time; updates to the software are automatically installed on servers and workstations.
		CC 5.2.10	Encryption is used for data transmissions and defined points of connectivity.
		CC 5.2.11	Access to the cloud environment is granted by appropriate personnel on a daily basis and is automatically revoked at the end of each day.
		CC 5.2.12	The Information Security policy outlining information technology roles and objectives is documented, made available to employees, and reviewed on an annual basis by management.
		CC 5.2.13	The entity performs internal vulnerability scans in real time; the software is configured to create alerts for identified vulnerabilities, and identified vulnerabilities are researched and resolved.
		CC 5.2.14	An external penetration test is performed on an annual basis, and identified risks are researched and resolved in a timely manner.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	**CC 5.3.1**	Policies and procedures outlining the objectives and procedures for change management are documented, made available to employees, and reviewed by management on an annual basis.
		CC 5.3.2	Policies and procedures for data protection are documented, made available to employees, and reviewed by management on an annual basis.

CONTROL ACTIVITIES			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 5.3.3	The Information Security policy outlining information technology roles and objectives is documented, made available to employees, and reviewed on an annual basis by management.
		CC 5.3.4	Incident response policies and procedures documenting the roles and responsibilities in the result of an incident are documented, made available to employees, and reviewed by management on an annual basis.
		CC 5.3.5	Policies and procedures outlining the objectives and procedures for risk assessment are documented, made available to employees, and reviewed by management on an annual basis.

LOGICAL AND PHYSICAL ACCESS CONTROLS			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC6.1	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 6.1.1**	Users are required to log-in to the network and in-scope applications, databases, and servers using a unique user ID and password.
		CC 6.1.2	Passwords for the network and in-scope applications, databases, and servers are configured to meet the entity's standards.
		CC 6.1.3	New user access to the network and in-scope applications, databases, and servers is authorized by the hiring manager prior to access being granted by appropriate personnel.
		CC 6.1.4	Changes to user access to the network and in-scope applications, databases, and servers for transferred employees are authorized by management and are modified by appropriate personnel within one business day of the transfer date.
		CC 6.1.5	Access to the network and in-scope applications, databases, and servers for terminated users is removed within one business day of termination.
		CC 6.1.6	Administrative access to the network and in-scope applications, databases, and servers is restricted to appropriate personnel.
		CC 6.1.7	User access to the network and in-scope applications, databases, and servers is reviewed on a quarterly basis by management; inappropriate user access identified is removed in a timely manner.
		CC 6.1.8	Encryption is used for data transmissions and defined points of connectivity.

LOGICAL AND PHYSICAL ACCESS CONTROLS			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 6.1.9	The Information Security policy outlining information technology roles and objectives is documented, made available to employees, and reviewed on an annual basis by management.
CC6.2	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 6.2.1**	New user access to the network and in-scope applications, databases, and servers is authorized by the hiring manager prior to access being granted by appropriate personnel.
		CC 6.2.2	Changes to user access to the network and in-scope applications, databases, and servers for transferred employees are authorized by management and are modified by appropriate personnel within one business day of the transfer date.
		CC 6.2.3	Access to the network and in-scope applications, databases, and servers for terminated users is removed within one business day of termination.
		CC 6.2.4	Administrative access to the network and in-scope applications, databases, and servers is restricted to appropriate personnel.
		CC 6.2.5	User access to the network and in-scope applications, databases, and servers is reviewed on a quarterly basis by management; inappropriate user access identified is removed in a timely manner.
		CC 6.2.6	Access to the cloud environment is granted by appropriate personnel on a daily basis and is automatically revoked at the end of each day.

LOGICAL AND PHYSICAL ACCESS CONTROLS			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC6.3	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 6.3.1**	New user access to the network and in-scope applications, databases, and servers is authorized by the hiring manager prior to access being granted by appropriate personnel.
		CC 6.3.2	Changes to user access to the network and in-scope applications, databases, and servers for transferred employees are authorized by management and are modified by appropriate personnel within one business day of the transfer date.
		CC 6.3.3	Access to the network and in-scope applications, databases, and servers for terminated users is removed within one business day of termination.
		CC 6.3.4	Administrative access to the network and in-scope applications, databases, and servers is restricted to appropriate personnel.
		CC 6.3.5	User access to the network and in-scope applications, databases, and servers is reviewed on a quarterly basis by management; inappropriate user access identified is removed in a timely manner.
		CC 6.3.6	Access to the cloud environment is granted by appropriate personnel on a daily basis and is automatically revoked at the end of each day.

LOGICAL AND PHYSICAL ACCESS CONTROLS			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	***N/A***	The design of the controls of this criterion is the responsibility of the subservice organization Microsoft Azure; thus, the service auditor does not render an opinion of the design of the controls for this criterion.
CC6.5	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 6.5.1**	Record retention and storage procedures are reviewed on an annual basis.
		CC 6.5.2	Policies and procedures for data protection are documented, made available to employees, and reviewed by management on an annual basis.
		CC 6.5.3	Firewall devices and software are implemented globally to secure network perimeters using a limited approval ruleset.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**CC 6.6.1**	Firewall devices and software are implemented globally to secure network perimeters using a limited approval ruleset.
		CC 6.6.2	Anti-virus software is installed on all servers and workstations and is configured to scan endpoints in real time; updates to the software are automatically installed on servers and workstations.
		CC 6.6.3	Encryption is used for data transmissions and defined points of connectivity.
		CC 6.6.4	The entity performs internal vulnerability scans in real time; the software is configured to create alerts for identified vulnerabilities, and identified vulnerabilities are researched and resolved.

LOGICAL AND PHYSICAL ACCESS CONTROLS			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 6.6.5	An external penetration test is performed on an annual basis, and identified risks are researched and resolved in a timely manner.
		CC 6.6.6	The entity uses monitoring software to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs, and unusual system activity; the software is configured to send alerts to IT personnel if an issue is detected.
CC6.7	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 6.7.1**	Backups for databases and servers are configured to be performed on a daily basis; access to backups is restricted to appropriate personnel.
		CC 6.7.2	New user access to the network and in-scope applications, databases, and servers is authorized by the hiring manager prior to access being granted by appropriate personnel.
		CC 6.7.3	Changes to user access to the network and in-scope applications, databases, and servers for transferred employees are authorized by management and are modified by appropriate personnel within one business day of the transfer date.
		CC 6.7.4	Access to the network and in-scope applications, databases, and servers for terminated users is removed within one business day of termination.
		CC 6.7.5	Administrative access to the network and in-scope applications, databases, and servers is restricted to appropriate personnel.
		CC 6.7.6	User access to the network and in-scope applications, databases, and servers is reviewed on a quarterly basis by management; inappropriate user access identified is removed in a timely manner.

LOGICAL AND PHYSICAL ACCESS CONTROLS			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 6.7.7	Firewall devices and software are implemented globally to secure network perimeters using a limited approval ruleset.
		CC 6.7.8	Anti-virus software is installed on all servers and workstations and is configured to scan endpoints in real time; updates to the software are automatically installed on servers and workstations.
		CC 6.7.9	Encryption is used for data transmissions and defined points of connectivity.
		CC 6.7.10	Access to the cloud environment is granted by appropriate personnel on a daily basis and is automatically revoked at the end of each day.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	**CC 6.8.1**	Anti-virus software is installed on all servers and workstations and is configured to scan endpoints in real time; updates to the software are automatically installed on servers and workstations.
		CC 6.8.2	Encryption is used for data transmissions and defined points of connectivity.
		CC 6.8.3	The entity performs internal vulnerability scans in real time; the software is configured to create alerts for identified vulnerabilities, and identified vulnerabilities are researched and resolved.
		CC 6.8.4	An external penetration test is performed on an annual basis, and identified risks are researched and resolved in a timely manner.
		CC 6.8.5	Firewall devices and software are implemented globally to secure network perimeters using a limited approval ruleset.

LOGICAL AND PHYSICAL ACCESS CONTROLS			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 6.8.6	The entity uses monitoring software to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs, and unusual system activity; the software is configured to send alerts to IT personnel if an issue is detected.

SYSTEM OPERATIONS			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC7.1	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 7.1.1**	The Information Security policy outlining information technology roles and objectives is documented, made available to employees, and reviewed on an annual basis by management.
		CC 7.1.2	Incident response policies and procedures documenting the roles and responsibilities in the result of an incident are documented, made available to employees, and reviewed by management on an annual basis.
		CC 7.1.3	Policies and procedures outlining the objectives and procedures for change management are documented, made available to employees, and reviewed by management on an annual basis.
		CC 7.1.4	Firewall devices and software are implemented globally to secure network perimeters using a limited approval ruleset.
		CC 7.1.5	Anti-virus software is installed on all servers and workstations and is configured to scan endpoints in real time; updates to the software are automatically installed on servers and workstations.
		CC 7.1.6	Encryption is used for data transmissions and defined points of connectivity.
		CC 7.1.7	The entity performs internal vulnerability scans in real time; the software is configured to create alerts for identified vulnerabilities, and identified vulnerabilities are researched and resolved.
		CC 7.1.8	An external penetration test is performed on an annual basis, and identified risks are researched and resolved in a timely manner.

SYSTEM OPERATIONS			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 7.1.9	The entity uses monitoring software to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs, and unusual system activity; the software is configured to send alerts to IT personnel if an issue is detected.
CC7.2	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 analyzed to determine whether they represent security events.	**CC 7.2.1**	Incident response policies and procedures documenting the roles and responsibilities in the result of an incident are documented, made available to employees, and reviewed by management on an annual basis.
		CC 7.2.2	Identified security incidents are documented and researched and resolved in a timely manner.
		CC 7.2.3	The Incident Response Plan is tested on an annual basis.
		CC 7.2.4	Firewall devices and software are implemented globally to secure network perimeters using a limited approval ruleset.
		CC 7.2.5	Anti-virus software is installed on all servers and workstations and is configured to scan endpoints in real time; updates to the software are automatically installed on servers and workstations.
		CC 7.2.6	The entity performs internal vulnerability scans in real time; the software is configured to create alerts for identified vulnerabilities, and identified vulnerabilities are researched and resolved.
		CC 7.2.7	An external penetration test is performed on an annual basis, and identified risks are researched and resolved in a timely manner.

SYSTEM OPERATIONS			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 7.2.8	The entity uses monitoring software to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs, and unusual system activity; the software is configured to send alerts to IT personnel if an issue is detected.
CC7.3	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 7.3.1**	Incident response policies and procedures documenting the roles and responsibilities in the result of an incident are documented, made available to employees, and reviewed by management on an annual basis.
		CC 7.3.2	Identified security incidents are documented and researched and resolved in a timely manner.
		CC 7.3.3	The Incident Response Plan is tested on an annual basis.
CC7.4	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 7.4.1**	Upon hire, and annually thereafter, all employees must successfully complete training courses covering basic information security practices that support the functioning of an effective risk management program.
		CC 7.4.2	Incident response policies and procedures documenting the roles and responsibilities in the result of an incident are documented, made available to employees, and reviewed by management on an annual basis.
		CC 7.4.3	Identified security incidents are documented and researched and resolved in a timely manner.
		CC 7.4.4	The Incident Response Plan is tested on an annual basis.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	**CC 7.5.1**	The Business Continuity and Disaster Recovery Plan is documented and is tested on an annual basis; policies and procedures are updated based on the results of the test.
		CC 7.5.2	Backups for databases and servers are configured to be performed on a daily basis; access to backups is restricted to appropriate personnel.

SYSTEM OPERATIONS			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 7.5.3	Incident response policies and procedures documenting the roles and responsibilities in the result of an incident are documented, made available to employees, and reviewed by management on an annual basis.
		CC 7.5.4	Identified security incidents are documented and researched and resolved in a timely manner.
		CC 7.5.5	The Incident Response Plan is tested on an annual basis.

CHANGE MANAGEMENT			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	**CC 8.1.1**	Policies and procedures outlining the objectives and procedures for change management are documented, made available to employees, and reviewed by management on an annual basis.
		CC 8.1.2	Changes are documented in a formalized ticketing system and are authorized, tested and approved prior to migration into the production environment.
		CC 8.1.3	Separate development, test, and production environments are maintained.
		CC 8.1.4	The user who develops and tests a change cannot also migrate the same change into production.
		CC 8.1.5	Servers and workstations are configured to automatically download and apply patches.

RISK MITIGATION			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**CC 9.1.1**	Policies and procedures outlining the objectives and procedures for risk assessment are documented, made available to employees, and reviewed by management on an annual basis.
		CC 9.1.2	The Risk Management Committee meets on a quarterly basis to oversee the achievement of the entity's risk management objectives; meeting minutes are maintained.
		CC 9.1.3	The entity performs a Risk Assessment on an annual basis to evaluate the achievement of risk management objectives and to identify threats and vulnerabilities; findings and recommended changes to internal processes and controls are documented and implemented in a timely manner.
		CC 9.1.4	The Business Continuity and Disaster Recovery Plan is documented and is tested on an annual basis; policies and procedures are updated based on the results of the test.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	**CC 9.2.1**	Policies and procedures outlining the objectives and procedures for risk assessment are documented, made available to employees, and reviewed by management on an annual basis.
		CC 9.2.2	The Risk Management Committee meets on a quarterly basis to oversee the achievement of the entity's risk management objectives; meeting minutes are maintained.
		CC 9.2.3	The entity performs a Risk Assessment on an annual basis to evaluate the achievement of risk management objectives and to identify threats and vulnerabilities; findings and recommended changes to internal processes and controls are documented and implemented in a timely manner.

RISK MITIGATION			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
		CC 9.2.4	The entity maintains a complete inventory of all third parties identifying the risks associated with each third party; the inventory is reviewed on an annual basis for completeness and accuracy.
		CC 9.2.5	The entity periodically obtains independent attestations, including SOC reports, for identified key vendors and performs reviews to evaluate the impact of the findings on the entity's control objectives.
		CC 9.2.6	The entity requires third parties to sign a nondisclosure agreement prior to sharing information with them.
		CC 9.2.7	New third parties sign a contract that communicates the conditions and responsibilities of third parties and includes a clause on the sharing of confidential information.

ADDITIONAL CRITERIA FOR AVAILABILITY			
TSP Ref. #	**TRUST SERVICES CRITERIA AND POINTS OF FOCUS**	**Control Number**	**Description of Omada Related Controls**
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 1.1.1**	The entity uses monitoring software to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs, and unusual system activity; the software is configured to send alerts to IT personnel if an issue is detected.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	**A 1.2.1**	The entity uses monitoring software to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs, and unusual system activity; the software is configured to send alerts to IT personnel if an issue is detected.
		A 1.2.2	Backups for databases and servers are configured to be performed on a daily basis; access to backups is restricted to appropriate personnel.
		A 1.2.3	The Business Continuity and Disaster Recovery Plan is documented and is tested on an annual basis; policies and procedures are updated based on the results of the test.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	**A 1.3.1**	The Business Continuity and Disaster Recovery Plan is documented and is tested on an annual basis; policies and procedures are updated based on the results of the test.

Section 4.2: Tests of Operating Effectiveness

Original Control Number	Control Description	Test Number	Test Description	Test Results
CC 1.1.1	Employees are required to sign the Information Security Policy, which includes guidelines for workplace conduct, upon hire and annually thereafter.	**CC 1.1.1.1**	Inspected the signed Information Security Policy for a sample of new hires during the Specified Period to determine that employees were required to sign Information Security Policy, including the guidelines for workplace conduct, upon hire for each selected new hire.	No Exceptions Noted.
CC 1.1.2	Management has established authority and appropriate lines of reporting for key personnel via an Organization Chart.	**CC 1.1.2.1**	Inspected the Organization Chart to determine that management had established authority and appropriate lines of reporting for key personnel via an Organization Chart during the Specified Period.	No Exceptions Noted.
CC 1.1.3	Performance evaluations are performed for employees by management annually.	**CC 1.1.3.1**	Inspected the performance evaluation for a sample of employees during the Specified Period to determine that performance evaluations were performed for employees by management for each selected employee.	No Exceptions Noted.
CC 1.2.2	The Company has established a Board of Directors that is independent from management; the Board meets on a periodic basis to provide oversight over internal controls.	**CC 1.2.2.1**	Inspected the list of Board of Directors to determine that the entity had established a Board of Directors that was independent from management.	No Exceptions Noted.
		CC 1.2.2.2	Inspected an example Board of Directors meeting presentation during the Specified Period to determine that the Board met periodically to provide oversight over internal controls.	No Exceptions Noted.

Original Control Number	Control Description	Test Number	Test Description	Test Results
CC 1.4.1	Upon hire, and annually thereafter, all employees must successfully complete training courses covering basic information security practices that support the functioning of an effective risk management program.	**CC 1.4.1.1**	Inspected the Security Awareness and Incident Response Training log for a sample of new hires during the Specified Period to determine that employees successfully completed training courses covering basic information security practices upon hire for each selected new hire.	No Exceptions Noted.
		CC 1.4.1.2	Inspected the Security Awareness and Incident Response Training log for a sample of employees during the Specified Period to determine that employees successfully completed training courses covering basic information security practices annually for each selected employee.	No Exceptions Noted.
CC 1.4.2	Prior to hire, in accordance with the Omada Employee Screening Procedure, employees are required to complete a background check performed by an independent agency.	**CC 1.4.2.1**	Inspected the background check for a sample of new hires during the Specified Period to determine that, prior to hire, in accordance with the Omada Employee Screening Procedure, employees were required to complete a background check performed by an independent agency for each selected new hire.	No Exceptions Noted.
CC 2.1.1	The Information Security policy outlining information technology roles and objectives is documented, made available to employees, and reviewed on an annual basis by management.	**CC 2.1.1.1**	Inspected the Information Security Policy to determine that the Information Security policy outlining information technology roles and objectives was documented and reviewed by management during the Specified Period.	No Exceptions Noted.

Original Control Number	Control Description	Test Number	Test Description	Test Results
		CC 2.1.1.2	Observed the Omada Policy Report during the Specified Period to determine that the Information Security Policy was made available to employees.	No Exceptions Noted.
CC 2.1.2	Incident response policies and procedures documenting the roles and responsibilities in the result of an incident are documented, made available to employees, and reviewed by management on an annual basis.	**CC 2.1.2.1**	Inspected the Incident Response Policy to determine that the Incident Response Policy documenting the roles and responsibilities in the event of an incident was documented and reviewed by management during the Specified Period.	No Exceptions Noted.
		CC 2.1.2.2	Observed the Omada Policy Report during the Specified Period to determine that the Incident Response Policy was made available to employees.	No Exceptions Noted.
CC 2.1.3	The Risk Management Committee meets on a quarterly basis to oversee the achievement of the entity's risk management objectives; meeting minutes are maintained.	**CC 2.1.3.1**	Inspected the Risk Management committee meeting minutes for a sample of quarters during the Specified Period to determine that the Risk Management Committee met to oversee the achievement of the entity's risk management objectives and that meeting minutes were maintained for each selected quarter.	No Exceptions Noted.

Original Control Number	Control Description	Test Number	Test Description	Test Results
CC 2.1.4	The entity performs a Risk Assessment on an annual basis to evaluate the achievement of risk management objectives and to identify threats and vulnerabilities; findings and recommended changes to internal processes and controls are documented and implemented in a timely manner.	**CC 2.1.4.1**	Inspected the Risk Assessment to determine that the entity performed a Risk Assessment during the Specified Period to evaluate the achievement of risk management objectives and to identify threats and vulnerabilities and that findings and recommended changes to internal processes and controls were documented and implemented in a timely manner during the Specified Period.	No Exceptions Noted.
CC 2.1.5	The entity maintains a complete inventory of all third parties identifying the risks associated with each third party; the inventory is reviewed on an annual basis for completeness and accuracy.	**CC 2.1.5.1**	Inspected the inventory of third parties to determine that the entity maintained a complete inventory of all third parties identifying the risks associated with each third party and that the inventory was reviewed for completeness and accuracy during the Specified Period.	No Exceptions Noted.
CC 2.1.6	The entity periodically obtains independent attestations, including SOC reports, for identified key vendors and performs reviews to evaluate the impact of the findings on the entity's control objectives.	**CC 2.1.6.1**	Inspected SOC reports for key vendors to determine that the entity periodically obtained independent attestations for identified key vendors during the Specified Period.	No Exceptions Noted.
		CC 2.1.6.2	Inspected the reviews of SOC reports to determine that the entity performed reviews to evaluate the impact of the findings on the entity's control objectives during the Specified Period.	No Exceptions Noted.

Original Control Number	Control Description	Test Number	Test Description	Test Results
CC 2.1.7	The entity performs internal vulnerability scans in real time; the software is configured to create alerts for identified vulnerabilities, and identified vulnerabilities are researched and resolved.	**CC 2.1.7.1**	Observed the Microsoft Security Hub dashboard and alert configurations during the Specified Period to determine that the entity performed vulnerability scans in real time, that the software was configured to create alerts for identified vulnerabilities, and that identified vulnerabilities were researched and resolved.	No Exceptions Noted.
CC 2.1.8	An external penetration test is performed on an annual basis, and identified risks are researched and resolved in a timely manner.	**CC 2.1.8.1**	Inspected the external penetration test to determine that an external penetration test was performed during the Specified Period.	No Exceptions Noted.
		CC 2.1.8.2	Inspected an example change ticket to determine that identified risks were researched and resolved in a timely manner.	This control did not operate during the Specified Period, as there were no critical risks identified during the external penetration test; therefore, no testing was performed.
CC 2.1.9	Before entering into a contract with a new high risk or critical risk vendor, the entity conducts a due diligence review to help identify potential risks and management approves the results of the review.	**CC 2.1.9.1**	Inspected the due diligence review for a sample of new high risk vendors during the Specified Period to determine that, before entering into a contract, the entity conducted a due diligence review to help identify potential risks and the CEO approved the results of the review for each selected high risk vendor.	This control did not operate during the Specified Period, as there were no new high-risk vendors during the Specified Period; therefore, no testing was performed.

Original Control Number	Control Description	Test Number	Test Description	Test Results
CC 2.3.1	The entity requires third parties to sign a nondisclosure agreement prior to sharing information with them.	**CC 2.3.1.1**	Inspected the nondisclosure agreement for a sample of new third parties during the Specified Period to determine that the entity required third parties to sign a nondisclosure agreement prior to sharing information with them for each selected new third party.	No Exceptions Noted.
CC 2.3.2	New third parties sign a contract that communicates the conditions and responsibilities of third parties and includes a clause on the sharing of confidential information.	**CC 2.3.2.1**	Inspected the Service Level Agreement for a sample of new third parties during the Specified Period to determine that new third parties signed a contract that communicated the conditions and responsibilities of third parties and included a clause on the sharing of confidential information for each selected new third party.	No Exceptions Noted.
CC 2.3.3	Major changes to the system and incidents affecting the security and availability of user information are communicated to third parties in a timely manner.	**CC 2.3.3.1**	Inspected the email communication for a sample of major changes and incidents during the Specified Period to determine that major changes to the system and incidents affecting the security and confidentiality of user information were communicated to third parties in a timely manner for each selected major change or incident.	No Exceptions Noted.
CC 3.1.1	Policies and procedures outlining the objectives and procedures for risk assessment are documented, made available to employees, and reviewed by management on an annual basis.	**CC 3.1.1.1**	Inspected the Compliance and Risk Management Policy and the Supplier Risk Management Policy to determine that policies and procedures outlining the objectives and procedures for risk assessment were documented and reviewed by management during the Specified Period.	No Exceptions Noted.

Original Control Number	Control Description	Test Number	Test Description	Test Results
		CC 3.1.1.2	Observed the Omada Policy Report during the Specified Period to determine that policies and procedures outlining the objectives and procedures for risk assessment were made available to employees.	No Exceptions Noted.
CC 4.1.1	The entity uses monitoring software to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs, and unusual system activity; the software is configured to send alerts to IT personnel if an issue is detected.	**CC 4.1.1.1**	Observed the dashboard and logs for the Microsoft Azure Security monitoring tool during the Specified Period to determine that the entity used monitoring software to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs, and unusual system activity.	No Exceptions Noted.
		CC 4.1.1.2	Observed the alert configurations for the Microsoft Azure Security monitoring tool during the Specified Period to determine that the monitoring software was configured to send alerts to IT personnel if an issue was detected.	No Exceptions Noted.
CC 5.2.1	Users are required to log-in to the network and in-scope applications, databases, and servers using a unique user ID and password.	**CC 5.2.1.1**	Inspected the user lists for in-scope systems during the Specified Period to determine that users were required to login to the network and in-scope applications, databases, and servers using a unique user ID and password.	No Exceptions Noted.
CC 5.2.2	Passwords for the network and in-scope applications, databases, and servers are configured to meet the entity's standards.	**CC 5.2.2.1**	Observed the password configurations for in-scope systems during the Specified Period to determine that passwords for the network and in-scope applications, databases, and servers were configured to meet the entity's standards.	No Exceptions Noted.

Original Control Number	Control Description	Test Number	Test Description	Test Results
CC 5.2.3	New user access to the network and in-scope applications, databases, and servers is authorized by the hiring manager prior to access being granted by appropriate personnel.	**CC 5.2.3.1**	Inspected the onboarding process and the user lists for in-scope systems for a sample of new hires during the Specified Period to determine that new user access to the network and in-scope applications, databases, and servers was authorized by the hiring manager prior to access being granted by appropriate personnel for each selected new hire.	No Exceptions Noted.
CC 5.2.4	Changes to user access to the network and in-scope applications, databases, and servers for transferred employees are authorized by management and are modified by appropriate personnel within one business day of the transfer date.	**CC 5.2.4.1**	Inspected the transfer ticket and the user lists for in-scope systems for a sample of employees who required access changes during the Specified Period to determine that changes to user access to the network and in-scope applications, databases, and servers for transferred employees were authorized by management and were modified by appropriate personnel within one business day of the transfer date for each employee who required an access change.	No Exceptions Noted.
CC 5.2.5	Access to the network and in-scope applications, databases, and servers for terminated users is removed within one business day of termination.	**CC 5.2.5.1**	Inspected the offboarding ticket and the user lists for in-scope systems for a sample of terminated employees during the Specified Period to determine that access to the network and in-scope applications, databases, and servers for terminated users was removed within one business day of termination for each selected terminated employee.	No Exceptions Noted.

Original Control Number	Control Description	Test Number	Test Description	Test Results
CC 5.2.6	Administrative access to the network and in-scope applications, databases, and servers is restricted to appropriate personnel.	**CC 5.2.6.1**	Inspected the administrative access rights to the network and in-scope applications, databases, and servers during the Specified Period to determine that administrative access to the network and in-scope applications, databases, and servers was restricted to appropriate personnel.	No Exceptions Noted.
CC 5.2.7	User access to the network and in-scope applications, databases, and servers is reviewed on a quarterly basis by management; inappropriate user access identified is removed in a timely manner.	**CC 5.2.7.1**	Inspected the user access reviews for the network and in-scope applications, databases, and servers for a sample of quarters during the Specified Period to determine that user access to the network and in-scope applications, databases, and servers was reviewed by management and inappropriate user access identified was removed in a timely manner for each selected quarter.	No Exceptions Noted.
CC 5.2.8	Firewall devices and software are implemented globally to secure network perimeters using a limited approval ruleset.	**CC 5.2.8.1**	Observed the firewall configurations during the Specified Period to determine that firewall devices and software were implemented to secure network perimeters using a limited approval ruleset.	No Exceptions Noted.

Original Control Number	Control Description	Test Number	Test Description	Test Results
CC 5.2.9	Anti-virus software is installed on all servers and workstations and is configured to scan endpoints in real time; updates to the software are automatically installed on servers and workstations.	**CC 5.2.9.1**	Observed the anti-virus console, logs, scanning schedule, and update configurations during the Specified Period to determine that anti-virus software was installed on all servers and workstations, was configured to scan endpoints in real time, and that updates to the software were automatically installed on servers and workstations.	No Exceptions Noted.
CC 5.2.10	Encryption is used for data transmissions and defined points of connectivity.	**CC 5.2.10.1**	Observed the Transparent Service Encryption, Application Gateways, HTTPS Encryption and TLS Encryption during the Specified Period to determine that encryption was used for data transmission and defined points of connectivity.	No Exceptions Noted.
CC 5.2.11	Access to the cloud environment is granted by appropriate personnel on a daily basis and is automatically revoked at the end of each day.	**CC 5.2.11.1**	Inspected the daily access report for a sample of days during the Specified Period to determine that access to the cloud environment was granted by appropriate personnel on a daily basis and was automatically revoked at the end of the day for each selected day.	No Exceptions Noted.
CC 5.3.1	Policies and procedures outlining the objectives and procedures for change management are documented, made available to employees, and reviewed by management on an annual basis.	**CC 5.3.1.1**	Inspected the Configuration and Change Management Policy to determine that policies and procedures outlining the objectives and procedures for change management were documented and reviewed by management during the Specified Period.	No Exceptions Noted.

Original Control Number	Control Description	Test Number	Test Description	Test Results
		CC 5.3.1.2	Observed the Omada Policy Report during the Specified Period to determine that policies and procedures outlining the objectives and procedures for change management were made available to employees.	No Exceptions Noted.
CC 5.3.2	Policies and procedures for data protection are documented, made available to employees, and reviewed by management on an annual basis.	**CC 5.3.2.1**	Inspected the Data Protection and Handling Policy to determine that policies and procedures for data protection were documented and reviewed by management during the Specified Period.	No Exceptions Noted.
		CC 5.3.2.2	Observed the Omada Policy Report during the Specified Period to determine that policies and procedures for data protection were made available to employees.	No Exceptions Noted.
CC 6.5.1	Record retention and storage procedures are reviewed on an annual basis.	**CC 6.5.1.1**	Inspected the review of retained data during the Specified Period to determine that record retention and storage procedures were reviewed.	No Exceptions Noted.
CC 6.7.1	Backups for databases and servers are configured to be performed on a daily basis; access to backups is restricted to appropriate personnel.	**CC 6.7.1.1**	Observed the Microsoft Azure backup configurations during the Specified Period to determine that backups for databases and servers were configured to be performed on a daily basis.	No Exceptions Noted.

Original Control Number	Control Description	Test Number	Test Description	Test Results
		CC 6.7.1.2	Inspected the access rights to backups during the Specified Period to determine that access to backups was restricted to appropriate personnel.	No Exceptions Noted.
CC 7.2.2	Identified security incidents are documented and researched and resolved in a timely manner.	**CC 7.2.2.1**	Inspected the incident response ticket for a sample of reported incidents during the Specified Period to determine that identified security incidents were documented and researched and resolved in a timely manner for each selected reported incident.	No Exceptions Noted.
CC 7.2.3	The Incident Response Plan is tested on an annual basis.	**CC 7.2.3.1**	Inspected the Incident Response Test to determine that the Incident Response Plan was tested during the Specified Period.	No Exceptions Noted.
CC 7.5.1	The Business Continuity and Disaster Recovery Plan is documented and is tested on an annual basis; policies and procedures are updated based on the results of the test.	**CC 7.5.1.1**	Inspected the Business Continuity and Disaster Recovery Plan to determine that the Business Continuity and Disaster Recovery Plan was documented during the Specified Period.	No Exceptions Noted.

Original Control Number	Control Description	Test Number	Test Description	Test Results
		CC 7.5.1.2	Inspected the Business Continuity and Disaster Recovery Plan and the Business Continuity and Disaster Recovery test to determine that the Business Continuity and Disaster Recovery Plan was tested during the Specified Period and that policies and procedures were updated based on the results of the test.	No Exceptions Noted.
CC 8.1.2	Changes are documented in a formalized ticketing system and are authorized, tested and approved prior to migration into the production environment.	**CC 8.1.2.1**	Inspected the change ticket for a sample of changes during the Specified Period to determine that changes were documented in a formalized ticketing system and were authorized, tested, and approved prior to migration into the production environment for each selected change.	No Exceptions Noted.
CC 8.1.3	Separate development, test, and production environments are maintained.	**CC 8.1.3.1**	Observed the development, test, and production environments during the Specified Period to determine that segregated development, test, and production environments were maintained.	No Exceptions Noted.
CC 8.1.4	The user who develops and tests a change cannot also migrate the same change into production.	**CC 8.1.4.1**	Inspected the change ticket for a sample of changes during the Specified Period to determine that the user who developed and tested a change did not also migrate the same change into production for each selected change.	No Exceptions Noted.

Original Control Number	Control Description	Test Number	Test Description	Test Results
CC 8.1.5	Servers and workstations are configured to automatically download and apply patches.	**CC 8.1.5.1**	Observed the System Center Configuration Manager (SCCM) configurations and the Windows server configurations during the Specified Period to determine that servers and workstations were configured to automatically download and apply patches.	No Exceptions Noted.