PRIVACY TERMS

This Privacy Terms is executed as of 24-Dec-2024 ("Effective Date") between Cayuga Onondaga BOCES, incorporated and registered in Auburn, NY 13021 located at 1787 west Genesee St Rd ("Subscriber") and **Zoho Corporation** incorporated and registered in the United States of America with company number 3019282 whose registered office is at 4141 Hacienda Drive, Pleasanton, California 94588, USA including its affiliated group entities ("Zoho") who are parties to the online terms of service or other electronically/physically signed service agreement ("Agreement") under which Subscriber has purchased ManageEngine Endpoint Central (on-premise), ManageEngine ADManager Plus (on-premise) and ManageEngine Service Desk Plus (on-premise) from Zoho ("Zoho Services").

In the course of providing Zoho Services under the Agreement, Zoho may process Personal Information on behalf of the Subscriber. Accordingly, the parties agree as follows:

1. Interpretation

1.1 **"Data Subject"** means the individual who is identifiable by the Personal Information or to whom the Personal Information otherwise pertains;

1.2 "**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information; and

1.3 "**Personal Information**" means any information relating to an identified or identifiable natural person that is provided to Zoho by, or on behalf of, Subscriber through Subscriber's use of the Zoho Services.

1.4 "**CCPA**" means the California Consumer Privacy Act (Cal. Civ. Code s.1798.100 to s.1798.199.100) as amended by the California Privacy Rights Act (CPRA), including its implementing regulations thereto, that become effective on or after the effective date of this Privacy Terms ;

1.5 "**Commercial Purpose**", "**Sale**"/"**Sell**", "**Share**" have the same meaning as given under sections 1798.140 of the CCPA.

Capitalized terms used but not defined in this Privacy Terms will have the meanings provided in the Agreement.

2. Processing of Personal Information

2.1 Zoho shall process the Personal Information only on behalf of the Subscriber and in compliance with its instructions, unless otherwise required by applicable laws. Subscriber agrees that its instructions to Zoho for processing Personal Information are:

(i) to process such data strictly in accordance with the Agreement;

(ii) to process data where such processing is initiated by Subscriber via the user interface of the Zoho Services;

(iii) to process data for fraud prevention, spam filtering, and service improvement, including automation; and

(iv) to process data to comply with other documented reasonable instructions provided by Subscriber (eg., via email) where such instructions are consistent with the Agreement. Zoho shall not be obliged to act in accordance with any instructions outside the scope of the Agreement except with the prior written agreement of both parties.

3. Sub-processors

3.1 Subscriber understands that Zoho engages sub-contractors and third party service providers listed by Zoho in its websites for providing (a) specific functionalities of Zoho Services and (b) certain essential functions such as fraud detection, spam filtering and improvement of services (collectively "Sub-processors") and that certain data, including Personal Information, may be shared by Zoho to the Sub-processors or may be collected by Sub-processors in the process of providing such functionalities.

3.2 If Subscriber requests Zoho for information on data processing by Sub-processors, such as for conducting a data protection impact assessment, Zoho shall make commercially reasonable efforts to provide relevant information to Subscriber.

3.3 Zoho warrants that it (i) publishes and maintains a list of Sub-processors on its website; and (ii) will inform Subscriber prior to appointment of any new Sub-processor.

3.4 Upon notification regarding Zoho's intention to engage a new Sub-processor, Subscriber may, within 10 days, object to the appointment of such new Sub-processor by notifying Zoho. In the event Subscriber objects to appointment of a new Sub-processor, Zoho shall recommend to the Subscriber, to the extent feasible, commercially reasonable changes in the configuration or use of the Zoho Services to avoid data collection or processing by the Sub-processor ("Reasonable Alternative"). If Zoho is unable to provide Subscriber with a Reasonable Alternative, Subscriber may, upon written notice to Zoho, terminate use of Zoho Services and be entitled to full refund of subscription fee for unused portion of the subscription period.

3.5 Zoho shall ensure that Personal Information is not disclosed to employees, subcontractors, or other persons or entities unless they have a legitimate educational interest and only for purposes necessary to provide services under the Agreement. Zoho agrees that it shall not disclose any Personal Information other than as required in this DPA. Zoho shall ensure that all employees and sub-processors comply with the terms of this DPA and are provided with any training on all applicable state and federal laws and regulations that protect the confidentiality of Personal Information before being provided access to Personal Information If disclosure of Personal Information is required by law or court order, Zoho shall notify the Subscriber, unless prohibited by law. Subscriber will notify New York State Education Department no later than the time the PII disclosure is required unless such notice is expressly prohibited by law or the court order.

4. Data Subject Requests

4.1 Zoho shall promptly notify the Subscriber about any request received directly from the Data Subject without responding to that request unless it has been otherwise authorized to do so. Subscriber hereby agrees that Zoho is authorised to respond in the first instance to any request in order to determine if the request is in respect of Personal Information processed by Zoho on behalf of the Subscriber.

4.2 Zoho shall implement appropriate technical and organizational measures to enable the Subscriber to comply with Data Subject's requests to Subscriber to delete, rectify, access, or restrict processing Data Subject's data. Where Subscriber requests Zoho's assistance under this section and Zoho has already enabled Subscriber to comply with such requests by implementing appropriate technical and organizational measures, Zoho shall have the right to charge the Subscriber for any reasonable costs or expenses incurred by Zoho in order to assist Subscriber with request(s) from Data Subjects.

5. Confidentiality and Security

5.1 Zoho shall ensure that its personnel engaged in the processing of Personal Information are (i) informed of the confidential nature of the Personal Information; and (ii) subject to confidentiality obligation or professional or statutory obligations of confidentiality.

5.2 Zoho shall implement appropriate technical and organisational security measures as specified under Appendix 1 to protect the Personal Information against any Security Incident.

6. Breach Notification

6.1 Zoho shall notify Subscriber without undue delay after becoming aware of any Security Incident. Zoho shall take all commercially reasonable efforts to remediate the Security Incident and prevent recurrence. Zoho's obligation specified herein shall not apply to Security Incidents caused by Subscriber or its authorized users.

6.2 Zoho shall take the following steps to identify Security Incidents and notify the Subscriber upon learning of an unauthorized release of Personal Information :

a. Provide prompt notification to the BOCES no later than seven (7) calendar days from the date of discovery of a Security Incident. The Contractor shall provide notification to the BOCES' Data Privacy Officer, by email at dataprivacyofficer@cayboces.org

b. Zoho shall investigate any breach or unauthorized release of Personal Information and reasonably cooperate with the BOCES and law enforcement to protect the integrity of any investigation of any breach or unauthorized release of PII by providing relevant information and updates regarding remediation activities .

c. Where a Security Incident is solely attributed to Zoho, due to zoho's failure to implement its Security Measures described in Appendix 1, Zoho shall pay for the full cost of the notification, provided that such notification shall be carried out via the tools implemented by Zoho.

7. Audit

7.1 Zoho shall, upon request by Subscriber, demonstrate its compliance with this Privacy Terms or Appendix 1 by way of reports of audits conducted in the previous 12 months by qualified and independent third party auditors. Subscriber acknowledges that all documents and information disclosed by Zoho ("Audit Information") constitute Zoho's confidential information. Accordingly, Subscriber shall take reasonable measures to protect the confidentiality of the Audit Information from unauthorized access, use or disclosure. Subscriber may use the audit reports only for the purposes of meeting its regulatory audit requirements or confirming compliance with the requirements of this Privacy Terms by Zoho.

7.2 Where the information provided by Zoho under above clause is not sufficient to demonstrate compliance with Privacy Terms or Appendix 1, Subscriber may request Zoho for further information or audit of Zoho's data processing facilities. Subscriber agrees that any audit of Zoho's data processing facilities will be subject to an audit plan mutually agreed upon by both parties.

8. CCPA Warranties and Prohibitions

8.1 Parties acknowledge that Zoho will be service provider (as the term is defined under CCPA) and will comply with all applicable obligations under the CCPA in providing Zoho Services to the Subscriber, and will protect Personal Information with the same level of protection as required under CCPA.

8.2 Zoho warrants that it will notify the Subscriber if it determines that it can no longer meet its obligations under the CCPA. Upon the receipt of notification, the Subscriber may take reasonable and appropriate steps to stop and remediate the unauthorized use of Personal Information, if any.

8.3 Zoho will not :

i. Sell or Share the Personal Information;
ii. retain, use, or disclose Personal Information for any purpose (including a Commercial Purpose) other than for the purposes approved under Agreement;
iii. retain, use, or disclose Personal Information outside of its direct business relationship with the Subscriber.
iv. combine the Personal Information with the personal information it receives from or on behalf of another person(s), or it collects from its own interaction with the Data Subject, except as permitted under the CCPA and its regulations.

9. Return and Deletion Upon Termination

9.1 Zoho shall provide an option to Subscriber to export Personal Information via the user interface of the Zoho Services.

9.2 Upon termination or expiration of Zoho Services, unless required by applicable law, Personal Information shall be automatically deleted from Zoho's primary servers on completion of the next routine clean-up cycle (that occurs once in six months) and from its backups after 3 months of deletion from primary servers.

9.3 Upon the request of the Subscriber, Zoho shall provide confirmation of the completion of the relevant clean-up cycle as certification of destruction of the Personal Information.

9.4 The obligations of this agreement shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain Personal Information retain access to Personal Information.

10. New York Education Law Section 2-d compliance

10.1 Subscriber acknowledges that Personal Information will be protected in line with Subscriber's security measures listed in Appendix 1 to the Privacy Terms.
10.2 For the purposes of clause 5. b. (2) of New York Education Law Section 2-d, Subscriber acknowledges that the encryption standards in Zoho Services will be as described at: https://www.zoho.com/encryption.html

This Privacy Terms has been entered into on the date stated at the beginning of it.

Executed for and behalf of **Subscriber** by:

phorton ..... (signature)

Pamela Horton ..... (print name)

Director of Instructional Support Services ..... (position)

Executed for and behalf of **Zoho Corporation** by:

..... (signature)

Jai Anand N ..... (print name)

Chief Financial Officer ..... (position)

Appendix 1 to the Privacy Terms

Technical and Organizational Security Measures applicable to Cloud services offered by Zoho

Zoho has established, and will maintain at a minimum, an information security management system that includes the following:

Security Governance

1. A governance framework that supports relevant aspects of information security through appropriate policies and standards.
2. Formal documentation of the roles and responsibilities of employees with respect to governance of Information Security within Zoho that are communicated by the management to employees.
3. An information security program in accordance with the international standard ISO 27001 that includes technical, organizational and physical security measures in order to protect Personal Information against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction.
4. Formally documented information security policy, data privacy policy and other policies that are communicated periodically to employees responsible for the design, implementation and maintenance of security and privacy controls. The policies will be reviewed annually to keep them up-to-date.
5. Compliance with industry standard security measures as described at https://www.zoho.com/compliance.html.

Risk Management

1. Annual risk assessment, to prioritize mitigation of identified risks.
2. Established internal audit requirements and periodical audits on information systems and processes at planned intervals.
3. Assessment of the design and operating effectiveness of controls against the established control framework through which corrective actions related to identified deficiencies will be tracked to resolution.

Human Resources Security

1. Background verification of all employees having access to confidential data that includes verification of criminal records, previous employment records if any, and educational background.
2. Signing of confidentiality agreement and acceptable use policy by employees upon their employment with clauses on protection of confidential information.

3. Training on security and privacy awareness including training on Zoho's policies, standards and relevant technologies along with maintenance and retention of training completion records.
4. Employees will be required to adhere to the information security policies and procedures. Disciplinary process for non adherence will be defined and communicated.

Identity and Access management of Zoho Personnel

1. Creation of unique identifiers for employees to access information systems and prohibition of sharing user accounts among employees.
2. User authentication to information systems protected by passwords that meet Zoho's password policy requirements derived based on NIST SP 800-63B standards.
3. Strong password configurations that include i) 8 character minimum length; ii) non dictionary words and iii) screening of passwords against list of known compromised passwords.
4. Mandatory Two factor authentication for access to information systems involving confidential data.
5. Secure remote access to the corporate network provisioned via SSL VPN with strong encryption and two factor authentication.
6. Adherence to the principles of least privilege and need-to-know and need-to-use basis for access control.
7. Approval mechanism from appropriate personnel to provide access to information systems.
8. Revocation of access that is no longer required in the event of termination or role change.
9. Recording of approval, assignment, alteration and withdrawal of access rights.
10. User access reviews on a half yearly basis and corrective actions whenever necessary.
11. Restrictions on administrative access to Personal Information and provision of access on a strictly need-to-know basis along with implementation of access-control measures such as mandatory two factor authentication.

Asset Management

1. Inventory maintenance of assets associated with information processing. Owners are assigned for each asset and rules for acceptable use of assets are defined. Assets assigned to employees are returned in the event of termination or role change.
2. Capacity management policies through which resources are continuously monitored and projections are made for future requirements.
3. Determined procedures in accordance with industry best practices for the reuse, secure disposal and destruction of electronic media to ensure that the data is rendered unreadable and unrecoverable.
4. Disposal of unusable devices by verified and authorized vendors which includes storing of such devices in a secure location until disposal, formatting any information

contained in the devices before disposal, degaussing and physical destruction of failed hard drives using shredder and crypto-erasing and shredding of failed SSDs.

Physical Security

1. Physical access to Zoho's data center is highly restricted and requires prior management approval. The data centers are housed in facilities that require electronic card key access. Additional two-factor authentication and biometric authentication are required to enter the data center premises and there is continuous monitoring of CCTV cameras and alarm systems.
2. Control of physical access to Zoho's development facilities using access cards and monitoring by security personnel.
3. Installation of CCTV cameras and review of access logs and CCTV footage in case of any incidents.
4. Defined visitor management process to authorize visitor entries and maintenance of access records of visitors.
5. Revocation of physical access to employees in the event of termination of employment or role change.

Network Security and Operations

1. A dedicated Network Operations Center (NOC), which operates 24x7 monitoring the infrastructure health.
2. Establishment and implementation of firewall rules in accordance to identified security requirements and business justifications.
3. Review of firewall rules on a quarterly basis to ensure that legacy rules are removed and active rules are configured correctly.
4. Establishment and maintenance of appropriate network segmentation, that includes use of virtual local area networks (VLANS) where appropriate, to restrict access to systems storing confidential data with a data storage layer that is designed to be not directly accessible from the Internet.
5. Clear separation of production, development and integration environments to ensure that production data is not replicated or used in non-production environments for testing purposes.
6. Management of access to production environments by a central directory and authentication for such access using a combination of strong passwords, two-factor authentication, and passphrase-protected SSH keys. Access to the production environment is facilitated through a separate network with strict rules.
7. Deployment of DDOS mitigation capabilities from well established service providers to prevent volumetric attacks and to keep the applications available and performing.

Secure Software Development

1. Well defined security process that is implemented and monitored throughout the SDLC taking into consideration confidentiality, availability and integrity requirements.
2. Implementation of secure software development policies, procedures, and standards that are aligned to industry standard practices such as OWASP, CSA, CWE/SANS including secure design review, secure coding practices, risk based testing and remediation requirements.
3. Training on secure coding principles and industry standards to personnel involved in the development and coding of products.
4. "Secure by design" approach by incorporating security risk assessments and Threat modeling in the planning and analysis phase of SDLC and review of the design to prevent new threats.
5. Examination of Source code changes for potential security issues using Zoho's proprietary SAST (static code analysis) tools and manual review process before deployment.
6. Web Application Firewall (WAF) layer that is embedded in all web applications for protection against Open Web Application Security Project (OWASP) threats, including SQL injections, Cross-site scripting (XSS) and remote file inclusions.
7. Maintenance of inventory of third party software that gets bundled in the products/services .
8. Alerts on potential security vulnerabilities in the third party software by Zoho's proprietory SCA(Software Composition Analysis) that is reviewed periodically to check its applicability and impact and to take steps to upgrade third party software to the latest version.
9. Appropriate checking and elimination procedures to ensure that the service is not affected by malware/viruses during development, maintenance and operation.
10. Appropriate security controls to ensure the confidentiality, integrity and availability of the CI/CD pipeline in the software development environment used to develop, deploy, and support the products.
11. Maintenance of clear distinction between the development, QA and production environments.

Data Security and Management

1. Information classification scheme with data handling guidelines related to access control, physical and electronic storage, and electronic transfer.
2. Logical separation of each subscriber's service data from other subscriber' data by distributing and maintaining separate logical cloud space for each subscriber.
3. Deletion of data from active database upon termination of Zoho Services by the subscriber (clean-up occurs once in every 6 months), deletion of backup data within 3 months of deletion from active database and termination of accounts that remain unpaid and inactive for a continuous period of 120 days by giving prior notice to the subscriber.

Cryptography

1. Use of transport encryption for information that traverses across networks outside of the direct control of Zoho including, but not limited to the Internet, Wi-Fi and mobile phone networks.
2. Encryption of data transmission to Zoho services are made using TLS 1.2/TLS1.3 protocols, with latest and strong ciphers like AES_CBC/AES_GCM 256 bit/128 bit keys, authentication of message using SHA2 and use of ECDHE_RSA as the key exchange mechanism.
3. Encryption of sensitive Personal Information at rest using 256-bit Advanced Encryption Standard (AES). (The data that is encrypted at rest varies specific to Zoho services and also options are provided where the subscriber defines the fields to encrypt depending on their business need and data sensitivity).
4. Irreversible industry standard algorithm (bcrypt) will be used to hash and store the passwords of Zoho Services with randomly generated per user salt added to the input.
5. Zoho's in-house Key Management Service (KMS) to own and maintain encryption keys that includes additional layer of security by encrypting the data encryption keys using master keys.
6. Separation of master keys and data encryption keys by physically storing them in different servers with limited access.

Change Management

1. A change management policy that governs changes in all components of the service environment whereby all changes are planned, tested, reviewed and authorized before implementation into production.
2. Assessment of the potential impacts, including information security and privacy impacts of the changes.
3. Documented fall-back mechanisms including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.
4. Notification to subscriber of any changes that may affect subscribers in an adverse manner.

Configuration Management

1. Implementation of security hardening and baseline configuration standards in accordance with industry standards that are reviewed and updated periodically.
2. Predefined OS images with security baselines are used to build systems in development and production.
3. Hardening standards including (i) ensuring that unnecessary features, services, components, files, protocols and ports are removed from the production environment; and (ii) removing unnecessary user logins and disabling or changing default passwords.
4. Approval from the appropriate personnel to install any software package in the production environment.

Vulnerability Management

1. Vulnerability management plan designed to (i) identify promptly, prevent, investigate, and mitigate any cyber security vulnerabilities; (ii) analyze the vulnerability; (iii) perform recovery actions to remedy the impact.
2. Vulnerability assessments using automated scanners performed periodically on Zoho's internet facing systems.
3. Application penetration testing by Zoho's in house security personnel performed annually in accordance to defined test methodologies
4. Review of identified issues from vulnerability assessments and penetration testing, determination of its applicability, impact and priority and rectification in accordance with the SLA definition: High level vulnerabilities within 7 calendar days of discovery, Medium level vulnerabilities within 30 calendar days of discovery and Low level vulnerabilities within 60 calendar days of discovery.
5. Monitoring known vulnerabilities from common sources such as OWASP, CVE, NVD and other vendor security lists and installation of security relevant patches to product and/or supporting systems in accordance with Zoho's patch management policy.
6. Antivirus deployment by running the current version of industry standard anti-virus software as a part of which signature definitions are updated periodically within 24 hours of release, real time scans are enabled and alerts are reviewed and resolved by appropriate personnel.

Security Logging and Monitoring

1. Use of centralized logging solution to aggregate and correlate events from various components including network devices, servers and applications.
2. Maintenance of audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events and retention of logs in accordance with applicable policies and regulations.
3. Host and application intrusion detection (IDS) technology to facilitate timely detection, investigation and response to incidents.
4. Restrictions on physical and logical access of logs by authorized personnel.

Business continuity and Disaster recovery

1. Disaster recovery and business continuity plans and processes (i) to ensure continuous availability of the services in case of any disaster; (ii) to provide an effective and accurate recovery.
2. Annual review of business continuity plan to evaluate its adequacy & effectiveness.
3. Redundancy mechanisms to eliminate single point of failure consisting of (i) dual or multiple circuits, switches, networks or other necessary devices; and (ii) storing of application data in a resilient storage that is replicated in near real time across data centers.

4. Taking periodic backups (incremental backups every day and weekly full backups) and storing them in an encrypted format both in primary and secondary datacenter.
5. Retention of backups for a period of thirty days and testing recovery of backups at planned intervals.
6. SLA for service availability with 99.9% monthly uptime as a part of which real time availability can be viewed in https://status.zoho.com.

Incident Management

1. An incident response plan and program containing procedures that are to be followed in the event of an information security incident.
2. Dedicated email (incidents@zohcorp.com) to which external parties can report security incidents and creating awareness among employees to report any potential security incident or weakness on time without any delay.
3. Tracking of security incidents, fixing of such incidents through appropriate actions, maintenance of such records in the incident registry and implementation of controls to prevent recurrence of similar incidents.
4. Incident management procedures that lays down the steps for notifying the client, and other stakeholders in a timely manner in accordance with breach notification obligations.
5. Implementation of appropriate forensic procedures including chain of custody for collection, retention, and presentation of evidence in the event of an information security incident likely to result in a legal action.

Third-Party Vendor Management

1. Vendor management policy through which Zoho evaluates and qualifies third party vendors as a part of which new vendors are onboarded only after understanding their processes and performing risk assessments.
2. Execution of agreements with vendors that require vendors to adhere to confidentiality, availability, and integrity commitments in order to maintain Zoho's security stance.
3. Annual reviews to monitor the operation of vendor's processes and security measures.

Parents' Bill of Rights for Data Privacy and Security

It is the responsibility of the Cayuga Onondaga BOCES ("BOCES") to adopt appropriate administrative, technical, and physical safeguards and controls to protect and maintain the confidentiality, integrity and availability of its data, data systems and information technology resources. All stakeholders, including students, teachers and administrators should be aware of their rights and expect their data to be kept private and confidential.

The BOCES is committed to protecting the privacy and security of data and in accord with New York Education Law Section 2-d, parents and eligible students can expect the following:

Supplemental Information Regarding Third Party Contractors

Any and all contracts between the Cayuga Onondaga BOCES and third-party contractors, under which a contractor will receive student data or principal or teacher data, shall include provisions requiring that the contractor maintain the confidentiality of shared student data or teacher or principal data in accordance with law, regulation and BOCES policy.

In addition, the BOCES will ensure that the contract or written agreement with a third party contractor includes a signed copy of the Parents' Bill of Rights and the contractor's privacy and security plan, in compliance with Part 121 of the New York State Education Commissioner's regulations. Click on the following link to see the contractor terms (insert contractor template here).

Parent Complaints

Any parent, eligible student, teacher or principal or eligible staff may file a written complaint regarding a breach or unauthorized release of student data and/or teacher or principal with the BOCES Data Protection Officers listed below.

Also, any additional questions or concerns regarding BOCES data security may be directed to the Data Protection Officers:

Stacy Tamburrino, Esq.
Labor Relations Specialist
1879 West Genesee Street Rd
Auburn, NY 13021
(315) 255-7683
stamburrino@cayboces.org

Pamela Horton
Director of Instructional Support Services
1879 West Genesee Street Rd
Auburn, NY 13021
(315) 255-7670
phorton@cayboces.org