Consensus Assessments Initiative Questionnaire (CAIQ) v4.1 - Completed

BreathEasy | Campus | Effective September 18, 2026

Completed by BreathEasy Administrative Services LLC for BreathEasy | Campus. Answers describe the service as it operates on the effective date. Where a control is provided by an infrastructure provider, the answer says so.

Contact: help@breatheasy.net

The official CSA CAIQ v4.1 workbook with these same answers is included in the district packet.

A&A

A&A-01.1
Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. Audit and assurance expectations are set in the published data security policy. BreathEasy Administrative Services LLC is a two-member company. Both members perform operational duties. One member is designated security officer and incident commander; the other is designated privacy officer and backup incident commander, so incident response and district contact do not depend on one person.

A&A-01.2
Are audit and assurance policies, procedures, and standards reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company. The security policy is reviewed at least annually by the security officer.

A&A-02.1
Are independent audit and assurance assessments conducted according to relevant standards at least annually?

Answer: No

Ownership: Company. BreathEasy Administrative Services LLC does not currently hold its own SOC 2 report. Underlying infrastructure (AWS, Cloudflare) operates under SOC 2 Type II and ISO 27001 certifications; provider reports are available on request. This completed questionnaire, the published security policy, and the named sub-processor list are provided for review.

A&A-03.1
Are independent audit and assurance assessments performed according to risk-based plans and policies, and in response to significant changes or emerging risks?

Answer: No

Ownership: Company. Independent assessments are not currently performed; infrastructure providers are independently audited (SOC 2 Type II, ISO 27001).

A&A-04.1
Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?

Answer: Yes

Ownership: Company. Controls are mapped to FERPA and state student-privacy obligations in the published policies and district addendum.

A&A-05.1
Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting

evidence and aligned with relevant auditing standards?

Answer: Yes

Ownership: Company. Security reviews, findings, and remediation are managed by the security officer and documented.

A&A-06.1

Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. Findings from security reviews are tracked to resolution before affected changes deploy.

A&A-06.2

Is the remediation status of audit findings regularly reviewed and reported to relevant stakeholders?

Answer: Yes

Ownership: Company. Remediation status is reviewed by the security officer; a summary of the most recent review is available to districts on request.

AIS

AIS-01.1

Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. Application security practices are documented in the data security policy.

AIS-01.2

Are application security policies and procedures reviewed and updated at least annually, or upon any significant changes?

Answer: Yes

Ownership: Company.

AIS-02.1

Are baseline requirements to secure applications established, documented, and maintained?

Answer: Yes

Ownership: Company. Baseline: server-side input validation, database-enforced tenancy, least-privilege roles, encryption in transit and at rest.

AIS-03.1

Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?

Answer: No

Ownership: Company. Formal security metrics reporting is not yet established; security events and lockouts are logged and reviewable.

AIS-04.1

Is a secure SDLC process defined and implemented for application requirements analysis, planning, design, development, testing, deployment, and operation per organizationally designed security requirements?

Answer: Yes

Ownership: Company. Version-controlled development with release-preparation security review.

AIS-05.1

Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and meeting organizational delivery goals?

Answer: Yes

Ownership: Company. Changes must pass type checking, production build, and rendered verification before deployment.

AIS-05.2

Is testing automated when applicable and possible?

Answer: Yes

Ownership: Company. Build and type checks are automated; rendered verification is performed per change.

AIS-06.1

Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?

Answer: Yes

Ownership: Shared. Deployments ship through the managed platform's standardized, version-controlled pipeline.

AIS-06.2

Is the deployment and integration of application code automated where possible?

Answer: Yes

Ownership: Shared.

AIS-07.1

Are application security vulnerabilities remediated following defined processes?

Answer: Yes

Ownership: Company. Known high-severity vulnerabilities are resolved before affected changes deploy.

AIS-07.2

Is the remediation of application security vulnerabilities automated when possible?

Answer: No

Ownership: Company. Remediation is manual and tracked.

AIS-08.1

Are processes, procedures, and technical measures defined and implemented to secure APIs?

Answer: Yes

Ownership: Shared. Server functions validate input and re-check authorization; database access is parameterized; TLS everywhere; Cloudflare edge protection in front.

AIS-08.2

Are reviews and updates for any improvements conducted at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

BCR

BCR-01.1

Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. Continuity commitments (RTO/RPO 24 hours, daily backups, 35-day retention) are published in the security policy.

BCR-01.2

Are the policies and procedures reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

BCR-02.1

Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?

Answer: Yes

Ownership: Company. RTO 24 hours and RPO 24 hours are defined for full-service outage.

BCR-02.2
Are the risk assessment and impact analysis reviewed and updated at least annually or upon significant changes?

Answer: Yes

Ownership: Company.

BCR-03.1
Are strategies being established to reduce the impact of business disruptions, and are resiliency and recovery from business disruptions being improved?

Answer: Yes

Ownership: Shared. Globally redundant edge delivery, managed database with point-in-time recovery.

BCR-04.1
Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?

Answer: Yes

Ownership: Company.

BCR-05.1
Is relevant documentation developed, identified, and acquired both internally and from external parties, to support business continuity and operational resilience plans?

Answer: Yes

Ownership: Company.

BCR-05.2
Is business continuity and operational resilience documentation available to authorized stakeholders?

Answer: Yes

Ownership: Company. Continuity terms are published in the district packet.

BCR-05.3
Is business continuity and operational resilience documentation reviewed at least annually or upon significant changes?

Answer: Yes

Ownership: Company.

BCR-06.1
Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?

Answer: Yes

Ownership: Company. Restore procedures are tested at least annually.

BCR-07.1
Are communication channels with all relevant stakeholders established and maintained during business continuity and resilience procedures?

Answer: Yes

Ownership: Company. District contacts and help@breatheasy.net channels are maintained for incident communication.

BCR-08.1
Are backups performed periodically?

Answer: Yes

Ownership: Shared. Automated daily backups with point-in-time recovery.

BCR-08.2
Is the confidentiality, integrity, and availability of the backup ensured?

Answer: Yes

Ownership: Shared. AES-256 encrypted backups, 35-day rolling retention.

BCR-08.3

Can backups be restored appropriately for resiliency?

Answer: Yes

Ownership: Shared. Restores tested at least annually.

BCR-09.1

Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?

Answer: Yes

Ownership: Provider. Inherited from infrastructure providers. The application runs on managed platforms: Cloudflare's edge network (application delivery) and Amazon Web Services us-east-2 (database, authentication, file storage). Both providers hold SOC 2 Type II and ISO 27001 for the infrastructure they operate; their reports are available to districts on request.

BCR-09.2

Is the disaster response plan updated at least annually, and when significant changes occur?

Answer: Yes

Ownership: Provider.

BCR-10.1

Is the disaster response plan exercised annually or when significant changes occur?

Answer: Yes

Ownership: Provider.

BCR-10.2

Are local emergency authorities included, if possible, in the exercise?

Answer: N/A

Ownership: Provider.

BCR-11.1

Are business-critical equipment supplemented with both locally redundant and geographically dispersed equipment located at a reasonable minimum distance, in accordance with applicable industry standards?

Answer: Yes

Ownership: Provider. Inherited from infrastructure providers. The application runs on managed platforms: Cloudflare's edge network (application delivery) and Amazon Web Services us-east-2 (database, authentication, file storage). Both providers hold SOC 2 Type II and ISO 27001 for the infrastructure they operate; their reports are available to districts on request.

CCC

CCC-01.1

Are policies and procedures for managing the risks associated with applying changes to assets owned, controlled, or used by the organization established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. All changes ship through version control with release-preparation review.

CCC-01.2

Are the policies and procedures reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

CCC-02.1

Is a defined quality change control, approval and testing process, incorporating baselines, testing, and release standards, established, maintained and implemented?

Answer: Yes

Ownership: Company.

CCC-03.1

Is a change management procedure implemented to manage the risks associated with applying changes to assets, owned, controlled or used by the organization?

Answer: Yes

Ownership: Company.

CCC-04.1

Is a procedure to authorize the addition, removal, update, and management of assets owned, controlled, or used by the organization, implemented and enforced?

Answer: Yes

Ownership: Company.

CCC-05.1

Are provisions to limit changes directly impacting service customer-owned environments (tenants) to explicitly authorized requests included within service level agreements?

Answer: Yes

Ownership: Company. Material changes affecting student data are communicated to district contacts before taking effect.

CCC-06.1

Are change management and configuration baselines established, documented and implemented for all relevant authorized changes on organizational assets?

Answer: Yes

Ownership: Shared.

CCC-06.2

Are the baselines reviewed and updated at least annually or upon significant changes?

Answer: Yes

Ownership: Shared.

CCC-07.1

Are detection measures implemented with proactive notification if changes deviate from established baselines?

Answer: No

Ownership: Shared. Automated baseline drift detection is not separately implemented beyond platform-managed infrastructure.

CCC-08.1

Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?

Answer: Yes

Ownership: Company. Emergency changes follow the same version-controlled path with after-the-fact review.

CCC-08.2

Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?

Answer: Yes

Ownership: Company.

CCC-09.1

Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?

Answer: Yes

Ownership: Shared. Deployments can be rolled back to the previous known-good release.

CEK

CEK-01.1

Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Shared. Encryption standards (TLS 1.2+, AES-256) are published in the security policy.

CEK-01.2
Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually, upon significant changes?

Answer: Yes

Ownership: Company.

CEK-02.1
Are cryptography, encryption, and key management roles and responsibilities defined and implemented?

Answer: Yes

Ownership: Shared. Providers manage infrastructure keys; the company manages application secrets in managed secret storage.

CEK-03.1
Are data protection at-rest and in-transit, and where applicable in use, provided using cryptographic libraries certified to approved standards?

Answer: Yes

Ownership: Provider. Provider-managed cryptographic libraries (TLS, AES-256).

CEK-04.1
Are encryption algorithms following industry standards utilized for protecting data, based on the data classification and associated risks?

Answer: Yes

Ownership: Shared. TLS 1.2+ in transit; AES-256 at rest.

CEK-05.1
Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?

Answer: Yes

Ownership: Shared.

CEK-06.1
Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?

Answer: Yes

Ownership: Shared.

CEK-07.1
Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?

Answer: Yes

Ownership: Shared.

CEK-08.1
Are service providers providing service customers with the capacity to manage their own data encryption keys?

Answer: No

Ownership: Company. Customer-managed encryption keys are not offered; keys are managed by the providers and the platform.

CEK-09.1
Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?

Answer: No

Ownership: Provider. Key management systems are audited within provider SOC 2 / ISO 27001 programs.

CEK-09.2
Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?

Answer: No

Ownership: Provider. Covered by provider certification programs.

CEK-10.1
Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?

Answer: Yes

Ownership: Provider.

CEK-11.1
Are private keys provisioned for a unique purpose managed, and is cryptography secret?

Answer: Yes

Ownership: Shared.

CEK-12.1
Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?

Answer: Yes

Ownership: Provider. Provider-managed key rotation; application secrets can be rotated on demand.

CEK-13.1
Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?

Answer: Yes

Ownership: Shared.

CEK-14.1
Are processes, procedures and technical measures to securely destroy cryptographic keys when they are no longer needed, defined, implemented, and evaluated, and include provisions for legal and regulatory requirements?

Answer: Yes

Ownership: Provider.

CEK-15.1
Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?

Answer: N/A

Ownership: Provider.

CEK-16.1
Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?

Answer: Yes

Ownership: Provider.

CEK-17.1
Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?

Answer: Yes

Ownership: Provider.

CEK-18.1

Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?

Answer: Yes

Ownership: Shared. Application secrets reside in managed secret storage with least-privilege access.

CEK-19.1

Are processes, procedures, and technical measures to use compromised keys to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) defined, implemented, and evaluated to include legal and regulatory requirement provisions?

Answer: N/A

Ownership: Provider.

CEK-20.1

Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?

Answer: Yes

Ownership: Shared.

CEK-21.1

Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?

Answer: Yes

Ownership: Provider.

DCS

DCS-01.1

Are policies and procedures for physical and environmental security established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Provider. Inherited from infrastructure providers. The application runs on managed platforms: Cloudflare's edge network (application delivery) and Amazon Web Services us-east-2 (database, authentication, file storage). Both providers hold SOC 2 Type II and ISO 27001 for the infrastructure they operate; their reports are available to districts on request.

DCS-01.2

Are policies and procedures for physical and environmental security reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Provider.

DCS-02.1

Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?

Answer: N/A

Ownership: Provider. No company-owned data center equipment; provider handles equipment disposal.

DCS-02.2

Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?

Answer: Yes

Ownership: Provider. Provider media sanitization follows NIST SP 800-88.

DCS-02.3

Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually or upon significant changes?

Answer: N/A

Ownership: Provider.

DCS-03.1

Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?

Answer: Yes

Ownership: Provider.

DCS-03.2

Does a relocation or transfer request require written or cryptographically verifiable authorization?

Answer: Yes

Ownership: Provider.

DCS-03.3

Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Provider.

DCS-04.1

Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?

Answer: Yes

Ownership: Company. Fully remote company; district data is accessed only via browser and never stored on workstations.

DCS-04.2

Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

DCS-05.1

Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?

Answer: N/A

Ownership: Company. No physical media is used.

DCS-05.2

Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually, or upon significant changes?

Answer: N/A

Ownership: Company.

DCS-06.1

Is the classification and documentation of physical and logical assets based on the organizational business risk?

Answer: Yes

Ownership: Company. Data classification is published in the security policy.

DCS-06.2

Are assets' classifications reviewed and updated at least annually or upon significant changes?

Answer: Yes

Ownership: Company.

DCS-07.1
Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?
Answer: Yes
Ownership: Shared. Cloud assets are cataloged within the managed platforms.

DCS-07.2
Is the catalogue reviewed and updated at least annually or upon significant changes?
Answer: Yes
Ownership: Shared.

DCS-08.1
Are physical security perimeters designed and implemented to safeguard personnel, data, and information systems?
Answer: Yes
Ownership: Provider.

DCS-09.1
Is equipment identification used as a method for connection authentication?
Answer: N/A
Ownership: Provider.

DCS-10.1
Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?
Answer: Yes
Ownership: Provider.

DCS-10.2
Are access control records retained periodically, as deemed appropriate by the organization?
Answer: Yes
Ownership: Provider.

DCS-11.1
Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?
Answer: Yes
Ownership: Provider.

DCS-12.1
Are datacenter personnel trained to safely manage adverse events, including but not limited to unauthorized ingress and egress attempts?
Answer: Yes
Ownership: Provider.

DCS-13.1
Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?
Answer: Yes
Ownership: Provider.

DCS-14.1
Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?
Answer: Yes
Ownership: Provider.

DCS-15.1
Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?
Answer: Yes
Ownership: Provider.

DCS-16.1
Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?
Answer: Yes
Ownership: Provider.

DCS-17.1
Are datacenter security metrics established, monitored, and reported to secure data center assets and services?
Answer: Yes
Ownership: Provider.

DCS-18.1
Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure continuous operations?
Answer: Yes
Ownership: Provider.

DSP

DSP-01.1
Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the preparation, classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?
Answer: Yes
Ownership: Company. Data classification, handling, and lifecycle rules are published in the security policy and Schedule of Data.

DSP-01.2
Are data security and privacy policies and procedures reviewed and updated at least annually, or upon significant changes?
Answer: Yes
Ownership: Company.

DSP-02.1
Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?
Answer: Yes
Ownership: Shared. Live data permanently deleted within 30 days of request; backups age out at 35 days; provider sanitization per NIST SP 800-88.

DSP-03.1
Is a data inventory created and maintained for sensitive, regulated and personal information (at a minimum)?
Answer: Yes
Ownership: Company. The published Schedule of Data itemizes every stored element, source, purpose, and retention.

DSP-03.2
Is the inventory reviewed and updated at least annually or upon significant changes?
Answer: Yes
Ownership: Company.

DSP-04.1
Is data classified according to type and sensitivity levels?

Answer: Yes

Ownership: Company. Restricted / Confidential / Public classification is published.

DSP-05.1

Is data flow documentation created to identify what data is processed and where it is stored and transmitted?

Answer: Yes

Ownership: Company. Data flows are documented through the named sub-processor table (what each touches and where).

DSP-05.2

Is data flow documentation reviewed at defined intervals, at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

DSP-06.1

Is the ownership and stewardship of all relevant personal and sensitive data documented?

Answer: Yes

Ownership: Company. Districts own their data; the company acts as steward (school official under FERPA).

DSP-06.2

Is data ownership and stewardship documentation reviewed at least annually?

Answer: Yes

Ownership: Company.

DSP-07.1

Are systems, products, and business practices based on security principles by design and per industry best practices?

Answer: Yes

Ownership: Company. Least privilege and server-side enforcement by design.

DSP-08.1

Are systems, products, and business practices based on privacy principles by design and according to industry best practices?

Answer: Yes

Ownership: Company. Data minimization list published; optional capabilities off by default until authorized in writing.

DSP-08.2

Are systems' privacy settings configured by default and according to all applicable laws and regulations?

Answer: Yes

Ownership: Company.

DSP-09.1

Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?

Answer: No

Ownership: Company. A formal DPIA has not been conducted; the Schedule of Data, minimization list, and data flow documentation are published for district review.

DSP-10.1

Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?

Answer: Yes

Ownership: Company. Data is used only to deliver the contracted service; no advertising, sale, or profiling.

DSP-11.1

Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?

Answer: Yes

Ownership: Company. Requests are handled by the district as record holder; the company forwards and supports requests it receives.

DSP-12.1

Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?

Answer: Yes

Ownership: Company.

DSP-13.1

Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?

Answer: Yes

Ownership: Company. Sub-processor terms at least as restrictive as the district agreement; none may use data for their own purposes.

DSP-14.1

Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?

Answer: Yes

Ownership: Company. Districts are notified before a sub-processor change affecting student data.

DSP-15.1

Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?

Answer: Yes

Ownership: Company. Production student data is never copied into test, demo, or development environments.

DSP-16.1

Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?

Answer: Yes

Ownership: Company. Published retention schedule; district may set different periods by agreement.

DSP-17.1

Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?

Answer: Yes

Ownership: Shared.

DSP-18.1

Does the service provider ensure that a procedure is in place and communicated to service customers for managing and responding to requests by law enforcement authorities for the disclosure of personal data, in accordance with applicable laws and regulations?

Answer: Yes

Ownership: Company. Disclosure only when legally required; the district is informed first unless legally prohibited.

DSP-19.1

Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?

Answer: Yes

Ownership: Company. Physical locations documented: AWS us-east-2 (data at rest), Cloudflare US edge processing.

GRC

GRC-01.1
Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. Security and privacy policies are sponsored and reviewed by both company members. BreathEasy Administrative Services LLC is a two-member company. Both members perform operational duties. One member is designated security officer and incident commander; the other is designated privacy officer and backup incident commander, so incident response and district contact do not depend on one person.

GRC-01.2
Are the policies and procedures reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

GRC-02.1
Is there an established and maintained formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of risks?

Answer: No

Ownership: Company. A formal enterprise risk management program is not established; risk is addressed through the security policy and review process.

GRC-03.1
Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?

Answer: Yes

Ownership: Company.

GRC-04.1
Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?

Answer: Yes

Ownership: Company. Exceptions require security officer approval and documentation.

GRC-05.1
Has an information security program (including programs of all relevant CCM domains) been developed and implemented?

Answer: Yes

Ownership: Company. The published security policy spans the CCM domains relevant to the service.

GRC-06.1
Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?

Answer: Yes

Ownership: Company. BreathEasy Administrative Services LLC is a two-member company. Both members perform operational duties. One member is designated security officer and incident commander; the other is designated privacy officer and backup incident commander, so incident response and district contact do not depend on one person.

GRC-07.1
Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?

Answer: Yes

Ownership: Company. FERPA and applicable state student-privacy statutes are identified in the policies and addendum.

GRC-07.2
Are the identified requirements reviewed at least annually or upon significant changes?

Answer: Yes

Ownership: Company.

GRC-08.1

Is contact established and maintained with related special interest groups and other relevant entities?

Answer: No

Ownership: Company. Formal participation in special interest groups is not maintained.

HRS

HRS-01.1

Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. Background checks before any production access.

HRS-01.2

Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?

Answer: Yes

Ownership: Company.

HRS-01.3

Are background verification policies and procedures reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

HRS-02.1

Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company.

HRS-02.2

Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

HRS-03.1

Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. No district data is stored on workstations; browser access only.

HRS-03.2

Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

HRS-04.1

Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company.

HRS-04.2
Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

HRS-05.1
Are return procedures of organizationally-owned assets by terminated employees established and documented?

Answer: Yes

Ownership: Company. Access revoked the same day a role ends.

HRS-06.1
Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all relevant personnel?

Answer: Yes

Ownership: Company.

HRS-07.1
Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?

Answer: Yes

Ownership: Company. Signed confidentiality and data-handling agreements precede access.

HRS-08.1
Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?

Answer: Yes

Ownership: Company.

HRS-09.1
Are employee roles and responsibilities relating to information assets' security and privacy, established, documented and communicated?

Answer: Yes

Ownership: Company.

HRS-10.1
Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?

Answer: Yes

Ownership: Company.

HRS-11.1
Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?

Answer: Yes

Ownership: Company. Annual security awareness and FERPA training.

HRS-11.2
Are regular security awareness training updates provided?

Answer: Yes

Ownership: Company.

HRS-12.1

Are employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?

Answer: Yes

Ownership: Company.

HRS-12.2

Are employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?

Answer: Yes

Ownership: Company.

HRS-13.1

Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?

Answer: Yes

Ownership: Company.

IAM

IAM-01.1

Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. Identity and access rules are published: named accounts, least privilege, district-managed roles.

IAM-01.2

Are identity and access management policies and procedures reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

IAM-02.1

Are policies and procedures for the management of authentication credentials, including passwords, established, documented, approved, communicated, implemented, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. Password storage is handled by the managed authentication service (salted hashes); leaked-password screening enforced.

IAM-02.2

Are policies and procedures reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

IAM-03.1

Is the inventory of identities managed, stored, and regularly reviewed, and is their level of access monitored?

Answer: Yes

Ownership: Company. District IT administers staff accounts and roles; company access reviewed quarterly.

IAM-04.1

Is the separation of duties principle employed when implementing information system access?

Answer: Yes

Ownership: Company.

IAM-05.1

Is the least privilege principle employed when implementing information system access?

Answer: Yes

Ownership: Company. Least privilege by default; narrowest working role per staff member.

IAM-06.1

Is an identity access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?

Answer: Yes

Ownership: Company. Roles are assigned by district IT administrators; changes are logged.

IAM-07.1

Is a process in place to de-provision or modify identity access in a timely manner?

Answer: Yes

Ownership: Company. Manual same-day deprovisioning by district admin is default; automated lifecycle integration available on request.

IAM-08.1

Are reviews and revalidation of identity access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance, and at least annually or upon significant changes?

Answer: Yes

Ownership: Company. Districts review staff accounts each semester; company access reviewed quarterly and on personnel change.

IAM-09.1

Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated?

Answer: Yes

Ownership: Company.

IAM-10.1

Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?

Answer: Yes

Ownership: Company. Support access is granted per-need and logged in the support access log.

IAM-10.2

Are procedures implemented to prevent the accumulation of segregated privileged access?

Answer: Yes

Ownership: Company.

IAM-11.1

Are processes and procedures for service customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?

Answer: Yes

Ownership: Company. Districts control their own privileged roles.

IAM-12.1

Are processes, procedures, and technical measures that ensure identities' activities are identifiable through uniquely associated IDs defined, implemented, and evaluated?

Answer: Yes

Ownership: Company. Unique named accounts only; shared logins are not permitted.

IAM-13.1

Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?

Answer: Yes

Ownership: Shared. MFA is enforced through Google sign-in or the district identity provider when SSO is configured.

IAM-13.2
Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?
Answer: Yes
Ownership: Provider.

IAM-14.1
Are processes, procedures, and technical measures for the secure management of authentication credentials, including passwords, defined, implemented, and evaluated?
Answer: Yes
Ownership: Shared.

IAM-15.1
Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?
Answer: Yes
Ownership: Company. Every privileged action is re-authorized on the server; database policies enforce boundaries.

IPY

IPY-01.1
Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application interfaces (e.g., APIs)?
Answer: Yes
Ownership: Company.

IPY-01.2
Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?
Answer: Yes
Ownership: Company.

IPY-01.3
Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?
Answer: Yes
Ownership: Company.

IPY-01.4
Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?
Answer: Yes
Ownership: Company.

IPY-01.5
Are interoperability and portability policies and procedures reviewed and updated at least annually, or upon significant changes?
Answer: Yes
Ownership: Company.

IPY-02.1
Are service customers able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?
Answer: No

Ownership: Company. A self-serve data API is not offered; full or partial exports are provided on request.

IPY-03.1
Are cryptographically secure network protocols implemented for the management, import, and export of data in accordance with industry standards?

Answer: Yes

Ownership: Shared. Exports are delivered over TLS.

IPY-04.1
Do agreements include provisions specifying service customers' data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the service customers d. Data deletion policy

Answer: Yes

Ownership: Company. Termination terms: full export, deletion within 30 days, backups age out at 35 days, written confirmation.

I&S

I&S-01.1
Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Shared.

I&S-01.2
Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Shared.

I&S-02.1
Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?

Answer: Yes

Ownership: Provider. Capacity and availability are managed and monitored by the platforms.

I&S-03.1
Are communications between environments, services, and applications monitored?

Answer: Yes

Ownership: Provider.

I&S-03.2
Are communications between environments, services, and applications encrypted?

Answer: Yes

Ownership: Shared. TLS 1.2+ for all connections.

I&S-03.3
Are communications between environments, services, and applications restricted to only authenticated and authorized connections, as justified by the business?

Answer: Yes

Ownership: Shared.

I&S-03.4
Are network configurations reviewed at least annually?

Answer: Yes

Ownership: Provider.

I&S-03.5
Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?

Answer: Yes

Ownership: Provider.

I&S-04.1
Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?

Answer: Yes

Ownership: Provider. Managed, hardened, patched infrastructure.

I&S-05.1
Are the environments separated into production and non production environments to reduce the risk of sensitive production data being used in non-production environments?

Answer: Yes

Ownership: Company. Production and non-production are separate; demo tenants use fictional students.

I&S-05.2
Is production data sanitized or protected before being used for any authorized non-production purpose?

Answer: Yes

Ownership: Company. Production student data is never used outside production.

I&S-06.1
Are applications and infrastructures designed, developed, deployed, and configured such that service customer (tenant) access is appropriately segmented, segregated, monitored, and restricted?

Answer: Yes

Ownership: Company. District and school boundaries are enforced by database row-level security plus application role checks.

I&S-07.1
Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?

Answer: Yes

Ownership: Provider.

I&S-08.1
Are high-risk environments identified and documented based on data sensitivity, threat exposure, and business impact?

Answer: Yes

Ownership: Company. Restricted data classification identifies the highest-sensitivity records.

I&S-09.1
Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?

Answer: Yes

Ownership: Provider. Cloudflare edge DDoS protection and managed WAF.

LOG

LOG-01.1
Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. Logging scope and retention are published in the security policy.

LOG-01.2

Are policies and procedures reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

LOG-02.1

Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?

Answer: Yes

Ownership: Company. Security events retained 18 months; access restricted by database policy.

LOG-03.1

Are security-related events identified and monitored within applications and the underlying infrastructure?

Answer: Yes

Ownership: Company. Sign-in attempts, lockouts/unlocks, role changes, and support access are logged with actor, IP, user agent, timestamp.

LOG-03.2

Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?

Answer: Yes

Ownership: Company. Automatic lockout after five failed sign-ins within ten minutes, with email alerts to the district security/IT contact and help@breatheasy.net.

LOG-04.1

Is audit log access restricted to authorized identities, and are records of that access maintained?

Answer: Yes

Ownership: Company. Log access is limited to district IT/admin roles and the company members; access is itself logged.

LOG-05.1

Are capabilities implemented and maintained to correlate and monitor security audit logs for the detection of suspicious or anomalous activity that deviates from typical or expected patterns?

Answer: Yes

Ownership: Company. Failed-sign-in pattern detection triggers automatic lockout and alerts.

LOG-05.2

Is a process established and followed to review and take appropriate and timely actions on detected anomalies?

Answer: Yes

Ownership: Company.

LOG-06.1

Is a reliable time source being used across all relevant information processing systems?

Answer: Yes

Ownership: Provider. Synchronized UTC time across managed infrastructure.

LOG-07.1

Are logging requirements for information meta/data system events established, documented, and implemented?

Answer: Yes

Ownership: Company.

LOG-07.2

Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment and as per relevant regulatory requirements?

Answer: Yes

Ownership: Company.

LOG-08.1

Are technical measures defined, implemented, and evaluated to enable service customers to detect and scrub or tokenize sensitive data from logs, in order to prevent unauthorized exposure as per applicable laws and regulations?

Answer: N/A

Ownership: Company. Logs exclude student record content by design.

LOG-09.1

Are audit records generated, and do they contain relevant security information?

Answer: Yes

Ownership: Company.

LOG-10.1

Are audit records protected from unauthorized access, modification, and deletion?

Answer: Yes

Ownership: Company. Security events are write-only to client roles; discipline and incident audit records are append-only with timestamped amendments.

LOG-11.1

Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?

Answer: No

Ownership: Provider. Cryptographic operation reporting is covered within provider programs.

LOG-12.1

Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?

Answer: No

Ownership: Provider.

LOG-13.1

Is physical access logged and monitored using an auditable access control system?

Answer: Yes

Ownership: Provider.

LOG-14.1

Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?

Answer: Yes

Ownership: Shared.

LOG-14.2

Are accountable parties immediately notified about anomalies and failures?

Answer: Yes

Ownership: Shared. Automated alerts email responsible contacts immediately.

SEF

SEF-01.1

Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. Incident response policy is published with severity classes and a fixed response sequence.

SEF-01.2

Are policies and procedures reviewed and updated annually, or upon significant changes?

Answer: Yes

Ownership: Company.

SEF-02.1
Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. Severity 1 containment target 4 hours; Severity 2 acknowledged within 1 hour during school hours.

SEF-02.2
Are policies and procedures for timely management of security incidents reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

SEF-03.1
Is a security incident response plan that includes a communication strategy for notifying relevant internal departments, impacted service customers, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. Notification path: district designated contact, with factual content for the district's own notices.

SEF-04.1
Is a structured approach followed to evaluate the effectiveness of incident response plans at planned intervals or upon significant changes?

Answer: Yes

Ownership: Company.

SEF-05.1
Are information security incident metrics established, monitored and reported?

Answer: No

Ownership: Company. Formal incident metrics reporting is not established; incidents are recorded and reviewed.

SEF-06.1
Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?

Answer: Yes

Ownership: Company.

SEF-07.1
Are processes, procedures, and technical measures defined, implemented, and evaluated for timely and effective response to security incidents in accordance with incident categories and severity levels?

Answer: Yes

Ownership: Company.

SEF-07.2
Are these processes and procedures reviewed, updated, and tested at least annually?

Answer: Yes

Ownership: Company.

SEF-08.1
Are processes, procedures, and technical measures for security breach notifications defined and implemented?

Answer: Yes

Ownership: Company. Districts notified without unreasonable delay and no later than 72 hours after confirmation; post-incident report within 15 business days.

SEF-08.2

Are material security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?

Answer: Yes

Ownership: Company.

SEF-09.1

Is a secure repository of security incident records established and maintained?

Answer: Yes

Ownership: Company. Security events are retained 18 months in a tamper-resistant store.

SEF-09.2

Are incident records regularly reviewed to identify patterns, root causes, and systemic vulnerabilities, and are relevant corrective measures implemented?

Answer: Yes

Ownership: Company.

SEF-10.1

Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?

Answer: Yes

Ownership: Company. Security contact: help@breatheasy.net with 'SECURITY' in the subject, monitored continuously.

SEF-10.2

Are points of contact reviewed and updated at least annually?

Answer: Yes

Ownership: Company.

STA

STA-01.1

Are policies and procedures for supply chain risk management established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Company. Sub-processor management is documented in the security policy and district addendum.

STA-01.2

Are policies and procedures for supply chain risk management reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

STA-02.1

Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Shared. Shared responsibility is documented: providers cover physical/data-center controls; the company covers application, access, and data handling.

STA-02.2

Are the policies and procedures that apply the SSRM reviewed and updated annually, or upon significant changes?

Answer: Yes

Ownership: Shared.

STA-03.1

Is the SSRM applied, documented, implemented, and managed throughout the supply chain?

Answer: Yes
Ownership: Shared.

STA-04.1
Is the service customer given SSRM guidance detailing information about SSRM applicability throughout the supply chain?

Answer: Yes
Ownership: Company. The district packet states the shared-responsibility split in plain language.

STA-05.1
Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM?

Answer: Yes
Ownership: Shared. This questionnaire marks ownership per control.

STA-06.1
Is the SSRM documentation reviewed and validated?

Answer: Yes
Ownership: Shared.

STA-07.1
Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?

Answer: Yes
Ownership: Company.

STA-08.1
Is an inventory of all supply chain relationships developed and maintained?

Answer: Yes
Ownership: Company. The named sub-processor inventory is published in the district addendum.

STA-09.1
Is a process defined, implemented, and enforced for establishing a Bill of Material for the service supply chain?

Answer: Yes
Ownership: Company. Dependencies are pinned and tracked in the project manifest and lockfile.

STA-09.2
Is the Bill of Material reviewed and updated at least annually or upon significant changes?

Answer: Yes
Ownership: Company.

STA-10.1
Are risk factors associated with supply chain relationships periodically reviewed?

Answer: Yes
Ownership: Company.

STA-11.1
Do service agreements between service providers and service customers (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy • Operational Resilience

Answer: Yes
Ownership: Company. District agreements cover scope, security requirements, incident procedures, audit rights, termination, portability, privacy, and resilience.

STA-12.1
Are supply chain agreements reviewed at least annually or upon significant changes?

Answer: Yes

Ownership: Company.

STA-13.1

Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?

Answer: Yes

Ownership: Company. Annual policy review includes conformance checks.

STA-14.1

Are policies that require all supply chain service providers to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?

Answer: Yes

Ownership: Company.

STA-15.1

Are the organization's service providers' IT governance policies and procedures reviewed at least annually or upon significant changes?

Answer: Yes

Ownership: Company. Provider posture is reviewed via their published compliance programs.

STA-16.1

Is a process defined and implemented for conducting risk-based security assessments of the supply chain?

Answer: Yes

Ownership: Company.

TVM

TVM-01.1

Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities and threats to protect systems against vulnerability exploitation?

Answer: Yes

Ownership: Company. Dependency and application security reviews occur during release preparation; high-severity issues block deployment.

TVM-01.2

Are threat and vulnerability management policies and procedures reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

TVM-02.1

Are policies and procedures to protect against malware and malicious instructions established, documented, approved, communicated, applied, evaluated, and maintained?

Answer: Yes

Ownership: Provider. Endpoint and infrastructure malware protection is provider-operated; no district data is stored on company workstations.

TVM-02.2

Are asset management and malware protection policies and procedures reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Provider.

TVM-03.1
Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?

Answer: No

Ownership: Company. Vulnerability detection is performed during release preparation rather than on a fixed monthly scan schedule.

TVM-04.1
Are a threat analysis process and procedures defined, implemented, and evaluated to identify, assess, and review the threat landscape for cloud systems?

Answer: Yes

Ownership: Company.

TVM-04.2
Are threat models built according to industry best practices to inform the risk mitigation strategy?

Answer: No

Ownership: Company. Formal threat models are not maintained; abuse cases are addressed in design review.

TVM-05.1
Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?

Answer: No

Ownership: Provider. Signature/indicator updates at the edge are provider-managed (continuous).

TVM-06.1
Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?

Answer: Yes

Ownership: Company. Third-party and open-source dependencies are reviewed during release preparation.

TVM-07.1
Are processes, procedures and technical measures defined, implemented and evaluated for the periodic performance of penetration testing by independent third parties?

Answer: No

Ownership: Company. Independent penetration testing has not been performed; infrastructure is covered by provider programs.

TVM-08.1
Are processes, procedures and technical measures defined, implemented and evaluated based on identified risks to support scheduled and emergency responses to vulnerability identification?

Answer: Yes

Ownership: Company.

TVM-09.1
Is vulnerability remediation prioritized using a risk-based method from an industry-recognized framework?

Answer: Yes

Ownership: Company. Severity-based prioritization; high-severity issues block release.

TVM-10.1
Is a risk-based method used for the prioritization and mitigation of threats, leveraging an industry-recognized framework to guide threat decision-making and protection measures?

Answer: Yes

Ownership: Company.

TVM-11.1

Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?

Answer: Yes

Ownership: Company.

TVM-12.1

Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?

Answer: No

Ownership: Company. Formal vulnerability metrics are not reported.

UEM

UEM-01.1

Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?

Answer: Yes

Ownership: Company. Company endpoints are managed by the two company members; district data is accessed only via browser and never stored locally.

UEM-01.2

Are universal endpoint management policies and procedures reviewed and updated at least annually, or upon significant changes?

Answer: Yes

Ownership: Company.

UEM-02.1

Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?

Answer: Yes

Ownership: Company. Staff handhelds and Chromebooks are district-owned and district-MDM-managed; the product ships as an installable web app.

UEM-03.1

Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?

Answer: Yes

Ownership: Company. Compatibility targets (Chromebooks, Windows, managed Android handhelds) are published in the product overview.

UEM-04.1

Is an inventory of all endpoints used and maintained to store, access and process company data?

Answer: Yes

Ownership: Company.

UEM-05.1

Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?

Answer: Yes

Ownership: Company.

UEM-06.1

Are all relevant interactive-use endpoints configured to require an automatic lock screen?

Answer: Yes

Ownership: Company.

UEM-07.1

Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?

Answer: Yes

Ownership: Company.

UEM-08.1

Is information protected from unauthorized disclosure on managed endpoints with storage encryption?

Answer: Yes

Ownership: Company. Full-disk encryption on company endpoints; no district data stored on them.

UEM-09.1

Are anti-malware detection and prevention technology services configured on managed endpoints?

Answer: Yes

Ownership: Company.

UEM-10.1

Are software firewalls configured on managed endpoints?

Answer: Yes

Ownership: Company.

UEM-11.1

Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?

Answer: No

Ownership: Company. DLP tooling is not deployed; mitigation is architectural (no district data on endpoints).

UEM-12.1

Are remote geo-location capabilities enabled for all managed mobile endpoints, in accordance with applicable laws and regulations?

Answer: No

Ownership: Company. Geo-location of endpoints is not used.

UEM-13.1

Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?

Answer: N/A

Ownership: Company. No company data resides on endpoints, so remote deletion is not applicable.

UEM-14.1

Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?

Answer: Yes

Ownership: Company. Third-party platform access is governed by their compliance programs and our sub-processor terms.