COALITION FOR PUBLIC SAFETY TRAINING IN SCHOOLS, INC.

DATA SECURITY & PROTECTION POLICY

COALITION FOR PUBLIC SAFETY TRAINING IN SCHOOLS, INC.
DATA SECURITY AND PROTECTION POLICY

ARTICLE I
PURPOSE

Coalition for Public Safety Training in Schools, Inc. (CPSTS) must restrict access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting our customers, incurring penalties for non-compliance and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively.

It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user awareness and avoid accidental loss scenarios, so it outlines the requirements for data breach prevention.

ARTICLE II
SCOPE

Section 1. In Scope. This data security policy applies all customer data, personal data, or other company data defined as sensitive by CPSTS. Therefore, it applies to every computer, mobile device, server, database and IT system that handles such data, including any device that is regularly used for email, applications, web access or other work-related tasks. Every user who interacts with company IT services is also subject to this policy.

Section 2. Out of Scope. Information that is classified as Public is not subject to this policy. Other data can be excluded from the policy by company management based on specific business needs, such as that protecting the data is too costly or too complex.

ARTICLE III
POLICY

Section 1. Principles. The company shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities as effectively and efficiently as possible.

Section 2. General.

(a) Each user shall be identified by a unique user credentials (user ID/password) so that individuals can be held accountable for their actions.

(b) The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.

(c) Each user shall read this data security policy and the login and logoff guidelines, and sign a statement as a condition for access.

(d) Records of user access may be used to provide evidence for security incident investigations.

(e) Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.

Section 3. <u>Access Control Authorization.</u> Access to CPSTS IT resources and services will be given through the provision of a unique user account and complex password. Accounts are provided based on CPSTS staffing rolls and is kept current.

Passwords are managed by information technology support. Requirements are established for password length, complexity and expiration.

Role-based access control (RBAC) will be used as applicable to secure access to all file-based resources in all CPSTS file repositories.

Section 4. Network & System Access.

(a) All employees and contractors shall be given network/system access in accordance with business access control procedures and the least-privilege principle.

Section 5. <u>User Responsibilities.</u>

(a) All users must lock their screens whenever they leave their work area to reduce the risk of unauthorized access.

(b) All users must keep their workplace clear of any sensitive or confidential information when they leave.

(c) All users must keep their passwords confidential and not share them.

Section 6. <u>Application and Information Access.</u>

(a) All CPSTS staff and contractors shall be granted access to the data and applications required for their job roles.

(b) All CPSTS staff and contractors shall access sensitive data and systems only if there is a business need to do so and they have approval from an authorized representative of CPSTS.

(c) Sensitive systems shall be physically or logically isolated in order to restrict access to authorized personnel only.

Section 7. Access to Confidential, Restricted Information.

(a) Access to data classified as 'Confidential' or 'Restricted' shall be limited to authorized persons whose job responsibilities require it, as determined by management.

(b) Personally Identifiable Information (PII) includes any information that can be associated with or traced to any individual, including an individual's name, address, telephone number, e-mail address, credit card information, social security number, or other similar specific factual information/ regardless of the media on which such information is stored (e.g., on paper or electronically) and includes such information that is generated, collected, stored or obtained.

(c) All CPSTS staff, consultants, subcontractors, agents, etc. will comply with all applicable privacy and other laws and regulations relating to protection, collection, use, and distribution of Personally Identifiable Information (PII).

(d) In no event may PII be sold or transferred to third parties, or otherwise provide third parties with access thereto.

(e) CPSTS staff, consultants, subcontractors, agents, etc. shall notify data owners as soon as is practicable, but no later than twenty-four (24) hours, after they become aware of or suspect that any PII has been breached, mis-handled, or otherwise unlawfully used.

ARTICLE IV
TECHNICAL GUIDELINES

Access control methods to be used shall include:

Auditing of attempts to log on to any device on the company network or data repositories.
Windows permissions to files and folders
Role-based access model
Server access rights
Firewall permissions (as applicable)
Web authentication rights
Database access rights and access control lists (ACLs).
Encryption at rest and in flight/mobile
Change passwords frequently (at a minimum once every 120 days)

Access control applies to all networks, servers, workstations, laptops, mobile devices, web applications and websites, cloud storages, and services.

ARTICLE V
REPORTING REQUIREMENTS

This Article describes the requirements for reporting incidents that occur:

(a) Timely incident reports shall be produced and handled by the technical staff/agents. The reports are stored indefinitely for audit and review purposes.

(b) High-priority incidents discovered shall be immediately escalated.

(c) Security logs and associated reports will be reviewed as is necessary.

ARTICLE VI
ENFORCEMENT

This Article describes the penalties for access control violations.

Any CPSTS user found in violation of this policy is subject to disciplinary action, up to and including removal from organization. Any third-party partner or contractor found in violation may have their access terminated and may be subject to legal action or recourse.

ARTICLE VII
REVISION HISTORY

This Article records each policy revision.

Version	Date of Revision	Author	Description of Changes
1.0	September 17, 2020	Paul C. Balassa/ Marc Spicer	Initial Version
2.0	August 3, 2022	William Taylor/ Deanna Banks	Electronic Version

I, Deanna Banks do hereby certify:

1. That I am the duly elected Secretary of Coalition for Public Safety Training in Schools, Inc., a Maryland non-stock, non-profit Corporation.

2. That the foregoing Data Security and Protection Policy, comprising five (5) pages, including this page, constitute the Data Security and Protection Policy of the Corporation as of the 17th day of September, 2020.

IN WITNESS WHEREOF, I have executed this certificate as of the 20th day of August, 2022.

Coalition for Public Safety Training in Schools, Inc.

By: Deanna Banks
CPSTS, Inc. Secretary

Signature: _____

Date: _____

DOWNLOAD SUBMIT PRINT