CLIPTRAINING™

Data Classification

DC-001

CONTENTS

Introduction

This policy defines the classifications of ClipTraining data -- i.e., the categories of data that ClipTraining is responsible for safeguarding -- and the associated measures which are necessary to safeguard each classification.

Data commonly exists in many forms, including electronic, magnetic, optical, and traditional paper documents.

This policy applies to all employees, volunteers, interns, and contractors who have access to sensitive or confidential information as defined in this document. This policy covers data that are stored, accessed, or transmitted in any and all formats, including electronic, magnetic, optical, paper, or other non-digital formats.

Purpose

Data and information are important assets of ClipTraining and must be protected from loss of integrity, confidentiality, or availability in compliance with ClipTraining policy and guidelines, and state and federal laws and regulations.

The purpose of this policy is to provide a framework for the protection of data that is created, stored, processed or transmitted within ClipTraining. The classification of data are the foundation for the specification of policies, procedures, and controls necessary for the protection of Confidential Data.

Scope

This policy applies to all ClipTraining employees and affiliated organizations (i.e. vendors, contractors, etc...). For the purposes of this policy, affiliated organization refers to any organization associated with ClipTraining that uses ClipTraining information technology resources to create, access, store, or manage ClipTraining Data to perform their business functions. It also applies to any third party vendor creating, storing, or maintaining data per a contractual agreement.

Effective Date

This Data Classification/policy became effective on 02/01/2021

All data must be classified based on DC-001 by 07/01/2021

Authority

This policy is based on Nation Institute of Standards and Technology (NIST), International Organization of Standards (ISO), and General Data Protection Regulation (EU GDPR) standards that incorporates data polices with appropriate security controls. This policy is further meant to be the authoritative source of direction for data classification and data governance across ClipTraining.

Data Classification Schema

Data and information assets are classified according to the risks associated with data being stored or processed. Data with the highest risk need the greatest level of protections to prevent compromise; data with lower risk require proportionately less protections. Throughout this document, four levels of data classification will be used to classify Data based on how the data are used, its sensitivity to unauthorized disclosure, and requirements imposed by external agencies.

Data are typically stored in aggregate form in databases, tables, or files. In most data collections, highly sensitive data elements are not segregated from less sensitive data elements. For example, an Employee information system will contain Employee's directory information as well as their social security number. Consequently, the classification of the most sensitive element in a data collection will determine the data classification of the entire collection.

Impact Level

Security Objective	High	Moderate	Low
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on ClipTraining	The unauthorized disclosure of information could be expected to have a serious adverse effect	The unauthorized disclosure of information could be expected to have a limited adverse effect

Security Objective	High	Moderate	Low
privacy and proprietary information.	operations, ClipTraining assets, or individuals.	on ClipTraining operations, ClipTraining assets, or individuals.	on ClipTraining operations, ClipTraining assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on ClipTraining operations, ClipTraining assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on ClipTraining operations, ClipTraining assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on ClipTraining operations, ClipTraining assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on ClipTraining operations, ClipTraining assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on ClipTraining operations, ClipTraining assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on ClipTraining operations, ClipTraining assets, or individuals.

Data Classifications

A. **Public** - Data explicitly or implicitly approved for distribution to the public without restriction. It can be freely distributed without potential harm to the, affiliates, or individuals. Public data generally have a very low sensitivity since by definition there is no such thing as unauthorized disclosure, but it still warrants protection since the integrity of the data can be important. Examples include:

1. ClipTraining public web site.

2. Directory information for Employee except for those who have requested non-disclosure.
3. Corporate Biographies.
4. ClipTraining product descriptions
5. Press releases.

Impact Level: PUBLIC

B. **Proprietary** - Classification of data provided to or created and maintained by ClipTraining on behalf of a third party, such as a corporation or government agency, will vary depending on contractual agreements and/or relevant laws or regulations. The classification and security standards for proprietary data owned by the third party will be defined by the third party. Proprietary data owned by ClipTraining must be classified and protected according to ClipTraining data classification policy and security standards. Individuals managing or accessing proprietary data are responsible for complying with any additional requirements and security policies and procedures specified by the third party owner. Proprietary data include data classified by the federal government as Classified National Security Information (confidential, secret, top secret).

C. **Internal** - Data intended for internal ClipTraining business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. Internal data are generally not made available to parties outside the ClipTraining community. Unauthorized disclosure could adversely impact the, affiliates, or individuals. Internal data generally have a low to moderate sensitivity. This data are considered nonpublic. Examples include:

1. Financial accounting data that does not contain confidential information.
2. Departmental intranet.
3. Information technology transaction logs.
4. Employee ID number
5. Employee educational and performance records.
6. Directory information for Employee who have requested non-disclosure

Impact Level: LOW

D. **Confidential**- Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know.

Explicit authorization by the Data Steward is required for access because of legal, contractual, privacy, or other constraints. Unauthorized disclosure could have a serious adverse impact on the business or research functions of the ClipTraining or affiliates, the personal privacy of individuals, or on compliance with federal or state laws and regulations or contracts. This data are considered nonpublic. Confidential data have a very high level of sensitivity. Examples include:

1. Social Security Number, Client account number, or National ID Number.
2. Employee ID number (if it is the same as the Social Security Number).
3. Credit card number or account information
4. Personal identity information (PII): an individual's name; date of birth; address; telephone number; driver's license number or card or non-driver's identification number or card; social security number or card; place of employment; employee identification numbers or other personal identification numbers or cards; mother's maiden name; birth, death or marriage certificates; electronic identification numbers; electronic signatures; and any financial number, or password that can be used to access a person's financial resources, including, but not limited to, checking or savings accounts, credit or debit card information, demand deposit or medical information. For CLIPTRAINING purposes, PII also includes ones name in combination with a passport number.
5. Passport number.
6. Personnel records.
7. Medical records.
8. Authentication tokens (e.g., personal digital certificates, passwords, biometric data).

Impact Level: HIGH or MODERATE

Data Security Standards

The following table defines required safeguards for protecting data and data collections based on their classification. Data security requirements for Proprietary Data are determined by the contracting agency and are therefore not included in the table below.

In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

Security Control Category	**Data Classification**		
	Public	**Internal**	**Confidential**
Access Controls	No restriction for viewing. Authorization by Data Steward or designee required for modification; supervisor approval also required if not a self-service function.	Viewing and modification restricted to authorized individuals as needed for business-related roles. Data Steward or designee grants permission for access, plus approval from supervisor. Authentication and authorization required for access	Viewing and modification restricted to authorized individuals as needed for business-related roles. Data Steward or designee grants permission for access, plus approval from supervisor. Authentication and authorization required for access. Confidentiality agreement required.
Copying/Printing (applies to both paper and electronic forms)	No restrictions.	Data should only be printed when there is a legitimate need. Copies must be limited to individuals with a need to know. Data should not be left unattended on a printer. Multifunction Printers must “wipe” or encrypt data when jobs are complete	Data should only be printed when there is a legitimate need. Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement. Data should not be left unattended on a printer. Copies must be labeled "Confidential".
Network Security	May reside on a public network. Protection with a firewall recommended. IDS/IPS protection recommended.	Protection with a network firewall required. IDS/IPS protection required. Protection with router ACLs optional.	Protection with a network firewall using "default deny" ruleset required. IDS/IPS protection required. Protection with router ACLs optional.

	Protection only with router ACLs acceptable.	Servers hosting the data should not be visible to entire Internet. May be in a shared network server subnet with a common firewall ruleset for the set of servers.	Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets like guest wireless networks. Must have a firewall ruleset dedicated to the system. The firewall ruleset should be reviewed periodically by an external auditor. Data should only be transmitted via encrypted tunnel or protocol.
System Security	Must follow general best practices for system management and security. Host-based software firewall recommended to be used.	Must follow ClipTraining-specific and OS-specific best practices for system management and security. Host-based software firewall required. Host-based software IDS/IPS recommended	Must follow ClipTraining-specific and OS-specific best practices for system management and security. Host-based software firewall required. Host-based software Data Loss Prevention (DLP) recommended.
Virtual Environments	May be hosted in a virtual server environment. All other security controls apply to virtual machines.	May be hosted in a virtual server environment. All other security controls apply to virtual machines. Should not share the same virtual environment/virtual machine with data of other security classifications.	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines. Cannot share the same virtual environment/virtual machine with data of other security classifications.
Physical Security	System must be locked or logged out when unattended. Host-based software firewall recommended.	System must be locked or logged out when unattended. Hosted in a secure location required; a Secure Data Center is recommended.	System must be locked or logged out when unattended. Hosted in a Secure Data Center required. Physical access must be monitored, logged, and

			limited to authorized individuals 24x7. Data should not be stored or shared on removable devices.
Remote Access to systems hosting the data	No restrictions.	Access restricted to local network or general ClipTraining Virtual Private Network (VPN) service. Remote access by third party for technical support limited to authenticated, temporary access via direct dial-in modem or secure protocols over the Internet.	Restricted to local network or secure VPN group. Unsupervised remote access by third party for technical support not allowed. Two-factor authentication required.
Data Storage	Storage on a secure server recommended. Storage in a secure Data Center recommended.	Storage on a secure server recommended. Storage in a secure Data Center recommended. Should not store on an individual's workstation or a mobile device.	Storage on a secure server required. Storage in Secure Data Center required. Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption. Encryption on backup media required (whether policy is in place or not.) AES Encryption required with 192-bit or longer key. Paper/hard copy: do not leave unattended where others may see it; store in a secure location.

Transmission	No restrictions.	No requirements	Encryption required (e.g., via SSL or secure file transfer protocols). Cannot transmit via e-mail unless encrypted and secured with a digital signature.
Backup/Disaster Recovery	Backups required; daily backups recommended.	Daily backups required. Off-site storage recommended.	Daily backups required. Off-site storage in a secure location required.
Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, paper, etc.)	Paper: no restrictions.	Media must be locked, destroyed or wiped when not in use.	Only approved devices used.
Training	General security awareness training recommended.	General security awareness training required.	General security awareness training required. .
Audit Schedule	As needed.	As needed.	Annual

Contracts with Third Parties

Contracts with third parties involving ClipTraining Data or ClipTraining client and customer data must include language requiring compliance with all applicable laws, regulations, and ClipTraining policies related to data and information security. Immediate notification to ClipTraining is required, if ClipTraining Data are used or disclosed in any manner other than allowed by the contract; and, to the extent practicable, mitigate any harmful effect of such use or disclosure.

Roles and Responsibilities

Everyone with any level of access to ClipTraining Data has responsibility for its security and is expected to observe requirements for privacy and confidentiality, comply with protection and control procedures, and accurately present the data in any type of reporting function. The following roles have specific responsibilities for protecting and managing ClipTraining Data and Data Collections.

A. **Chief Information Security Officer** - Provides advice and guidance on information and information technology security policies and standards.

B. **Cybersecop or other External Assessor**- Performs audits for compliance with data classification and security policy.

- *At times the Chief Information Security Officer and External Assessor may be the same*