Data Classification and Handling Policy

Version number	5.0
Last Approved	Feb 13, 2026
Classification	PUBLIC

Overview

The Data Classification and Handling Policy defines the levels of data classification and the types of information that fall into each category. This policy also defines the appropriate level of security and access controls for each classification and outlines handling requirements, including client data access and manipulation provisions.

Applicability

The applicability of this statement falls under purview of the Security Documentation Overview .

Scope

This policy applies to all Company employees and contractors that access, process, or store sensitive Company data.

Definitions

Confidential / Sensitive Data	A generalized term that typically represents data classified as confidential according to the data classification scheme defined in this document. This term is often used interchangeably with sensitive data.
Data Owner	An individual or group of people who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems.
Data Custodian	An employee of the Company who has administrative or operational responsibility over information assets.
Institutional Data	All data owned or licensed by the Company.
Information Assets	Definable pieces of information in any form, recorded or stored, on any media that is recognized as “valuable” to the Company.

Non-public Information	Any information that is classified as Internal/ information according to the data classification scheme defined in this document.
Personal Data	Any information related to a natural person or 'Data Subject', which can be used to directly or indirectly identify the person.

Classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the Company should that data be disclosed, altered, or destroyed without authorization. The classification of data helps determine what security controls are appropriate for safeguarding that data.

All institutional data should be classified into one of four sensitivity classifications:

Public

Data should be classified as Public when the unauthorized disclosure, alteration, or destruction of that data would results in little or no risk to the Company and its affiliates. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data. **Public data is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions.** The integrity of Public data should be protected. The impact on the Company should Public data not be available is typically low. Examples of Public data include directory information and research publications.

Internal

Data should be classified as Internal when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to the Company or its affiliates. By default, all information assets that are not explicitly classified as Public, Confidential, or Restricted should be treated as Internal data. A reasonable level of security control should be applied to internal data. Access to Internal data must be requested and authorized. Access to Internal data may be authorized to groups of persons by their job classification or responsibilities ("role-based" access) and may also be limited by one's department. **Internal Data is moderately sensitive in nature.** The risk for negative impact to the Company, should this information not be available when needed, is typically moderate. Examples of Internal data include Company records such as financial reports, human resources information, some research data, and budget information.

Confidential

Data should be classified as Confidential when the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to the Company or its affiliates. A high level of security controls should be applied. Access to Confidential data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the Company who require such access in order to perform their jobs ("need-to-know"). Access to Confidential data must be individually requested and then authorized. **Confidential data is highly sensitive and requires a high level of security controls.** In addition, the negative impact on the Company (should this data be incorrect, improperly disclosed, or not available when needed) is typically high. Examples of Confidential data include sensitive technical and procedural documentation, customer contracts, and source code.

Restricted

Data should be classified as Restricted when the unauthorized disclosure, alteration, or destruction of that data could cause the highest level of risk to the Company or its affiliates. Examples of Restricted data include all client data, and highly sensitive security documentation (e.g. penetration test results). **Restricted data is highly sensitive and requires the highest level of security controls.** Access to Customer Personal Data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the Company that require this information on a "need-to-know" basis. Restricted data may not be shared externally, even under NDA, with the exception of sub-processors that are contractually bound to security requirements at least as rigorous as the Company's.

Data Handling Requirements

For each classification, several data handling requirements are defined to appropriately safeguard the information. It is important to understand that overall sensitivity of institutional data encompasses not only its confidentiality but also the need for integrity and availability.

The following table defines required safeguards for protecting data based on their classification. 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 & Restricted**
Access Controls	• No restriction for viewing • Authorization by Data Owner 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 Owner 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 Owner or designee grants permission for access, plus approval from supervisor • Authentication and authorization required for access • Confidentiality agreement required

			• Data masking implemented when practical
Copying and 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/fax.	• 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/fax • Copies must be labeled “Confidential” • Must be sent via Confidential envelope; data must be marked “Confidential”
Network Security	• May reside on a public network	• Protection with a network firewall required • IDS/IPS protection required • Protection with router ACLs optional • Servers hosting the data should	• Protection with a network firewall using "default deny" rule set required • IDS/IPS protection required • Protection with router ACLs optional

		not be accessible to entire Internet • May be in a common subnet where firewall policies are applied to the servers	• Servers hosting the data cannot be accessible to the entire Internet, nor to unprotected subnets, like guest wireless networks • Must have a firewall rule set dedicated to the common subnet • The firewall rule set should be reviewed periodically
Data Storage	• Storage on a secure server or device required	• Storage on a secure server or device required	• Storage on a secure server or device required • Encryption on backup media required • Paper/hard copy: do not leave unattended where others may see it; store in a secure location
Transmission	No restrictions	No restrictions	• Encryption required (e.g., via SSL or secure file transfer protocols) • Cannot transmit via e-

			mail unless encrypted and secured with a digital signature

SOC 2: CC6.7

The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

Client Data Access and Manipulation

Client data access is only authorized for Personnel with a business need to support clients and administer systems within the Company's application systems. This is the sole acceptable reason for granting client data access. It is prohibited to store client data on end user computing devices.

Access is granted individually or by security group membership, depending on job roles and responsibilities.

If Personnel is not granted access by default (per job requirements), then their access must be authorized by their reporting manager **and** the VP Information Security. This authorization is required before administrators may complete any individual request submitted for production account creation.

Important notes:

- Only designated application account administrators are authorized to create production accounts or to grant access to client implementations.
- Only designated internal environment owners are authorized to grant access to client data under their control.
- Client data is prohibited in test environments unless anonymized.
- Any unauthorized forms of client data manipulation (operations outside the normal course of providing, administering and supporting the services) is strictly prohibited without written authorization.
- Any individual who grants unauthorized access to or who makes or causes unauthorized changes to any form of production client data residing on Company- or client-owned computer systems will be subject to severe administrative action, up to and including immediate termination and possible legal prosecution.

SOC 2: C1.1

The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

Client Data Manipulation Authorization

New Client Activity (Contractual Agreement)

Authorized forms of client data manipulation are established as part of the client's initial contractual agreement.

Contracted Services Tasks (Contractual Agreement)

As part of normal operations within Company services, client administrators routinely make changes to their own data. When those administrative duties are outsourced to The Company (as a contracted service), Personnel assigned to

administer client data are authorized (by contractual agreement) to make appropriate changes within the scope of services rendered.

Electronic Support Request Ticket

Any approved support requests are acceptable forms of authorization, provided they come a standard support channel, used to assign work tasks to individuals or groups (as requested by clients, designated data owners, or Company management in support of troubleshooting efforts or customer submitted change requests).

Document control

> This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	Art Machado	
Author(s)	Art Machado, Angelina Kilmer, Paul Gordon	
Required Approver(s) and Approval Date	Art Machado - VP Information Security	Feb 13, 2026
Review cycle	ANNUAL	
Next review date	Feb 13, 2027	

Version History

Date	Author(s)	Version	Changes
Feb 13, 2026	Angelina Kilmer Paul Gordon	5.0	Annual review
Feb 25, 2025	Art Machado Angelina Kilmer Paul Gordon	4.0	Annual review
Nov 1, 2024	Angelina Kilmer	3.6	Changed Policy classification from Confidential to Public
Mar 13, 2024	Art Machado Sarah Zwicker Paul Gordon	3.5	Annual update, clarification of language and expanded examples to include reference to client data
Dec 1, 2023	Art Machado	3.4	Added provisions from depreciated Client Data Access and Manipulation policy; changed

			policy title and updated Overview to reflect changes
Feb 23, 2023	Art Machado Sarah Zwicker	3.3	Annual review + logo updated
Mar 24, 2022	Sarah Zwicker	3.2	Added Privacy considerations and components
Mar 16, 2022	Art Machado Sarah Zwicker	3.1	Title change for VP InfoSec, Annual Review
Jun 3, 2021	Art Machado	3.0	Updated data classifications
Mar 15, 2021	Sarah Zwicker	2.9	Changed owner
Feb 9, 2021	Sarah Zwicker	2.8	Reformatting, policies linked
Jan 26, 2021	John Cole	2.7	Annual review, role title change
Nov 23, 2020	Sarah Zwicker	2.6	Ownership change