DATA CLASSIFICATION OVERVIEW

Understanding methods to organize and protect data

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz

Data Governance Enablement Team
June 2026

WHAT IS DATA CLASSIFICATION?

Data Classification is the process of categorizing data based on:

- Sensitivity
- Value
- Potential impact if disclosed, altered, or lost

The goal is to ensure information receives the **right level of protection based on risk**, rather than treating all data the same.

Benefits

- ✅ Consistent handling of data
- ✅ Better risk-based decisions
- ✅ Support for compliance requirements
- ✅ Clear expectations for storage, sharing, and protection

Data Classification at the University of Colorado

Why CU Uses Classification

- Align protections with risk
- Support compliance obligations
- Enable responsible data sharing
- Create consistency across domains

Data Classification vs Data Access

Data Classification

"How sensitive is the data?"

Based on risk

Stays consistent

Drives controls

Data Access

"Who can use the data?"

Based on business need

Varies by role

Enforces controls

Example

- A dataset may be classified as **Highly Confidential (L4)**.
- That does **not** mean everyone at CU can access it.
- Only authorized individuals with a legitimate business need should have access.

WHAT WE NEED FROM YOU

During the Beta Test

For each data asset:

1. Review each data definition
2. Consider the impact of unauthorized disclosure
3. Select the most appropriate classification level
4. Note any uncertainties or edge cases
5. Provide feedback on classification framework usability

Don't worry about:

- ✗ Access permissions
- ✗ Security controls
- ✗ Criticality rankings
- ✗ System ownership

THE 5-LEVEL FRAMEWORK

Level	Classification	Risk
L1 Public	**May be made public** • ***Examples:*** *Academic catalogs, Public websites, Marketing materials, Public research publications*	**None or Minimal**
L2 University Internal	**Access limited to CU personnel and contractors** • ***Examples:*** *Internal communications, Employee intranet content, Internal procedures, Training materials*	**Low**
L3 Confidential	**Access restricted to authorized individuals** • ***Examples:*** *Employee evaluations, Non-public student information, Internal financial reports, Contractually protected information, Non-public research records* **Note:** Need-to-know access becomes increasingly important at this level.	**Moderate**
L4 Highly Confidential	**Access limited by strict technical controls and monitored through auditing** • ***Examples:*** *Social Security Numbers, Health information, Authentication credentials, Sensitive research data, Security vulnerability details*	**High**
L5 Restricted	**Access limited by strict technical controls defined by legal compliance or regulation** • ***Examples:*** *Certain regulated HIPAA/FERPA datasets, Federal Tax Information (FTI), IRB Level 5 research data, Data with heightened contractual obligations*	**Highest / Regulatory**

THE 30-SECOND DECISION TREE

1. **Is the data subject to heightened regulatory, contractual, or legal requirements requiring max protection?**
   - **Yes** → *L5 Restricted*
   - **No** → Continue
2. **Could disclosure lead to identity theft, discrimina fraud, security compromise, or significant institu harm?**
   - **Yes** → *L4 Highly Confidential*
   - **No** → *Continue*
3. **Could unauthorized disclosure cause moderate ha violate confidentiality expectations?**
   - **Yes** → *L3 Confidential*
   - **No** → *Continue*
4. **Is the information intended for internal university only with minimal risk if disclosed?**
   - **Yes** → *L2 University Internal*
   - **No** → *Continue*
5. **Has the information been intentionally approved f public release?**
   - **Yes** → *L1 Public*

L 5	• Federal Tax Information (FTI) • IRB Level 5 Research Data • Contractually restricted datasets • Certain HIPAA/FERPA-regulated records
L 4	• Social Security Numbers • Health information • Passwords & authentication credentials • Sensitive research data • Security vulnerabilities
L 3	• Personnel records • Non-public student information • Internal financial reports • Contracts • Non-public research records
L 2	• Internal communications • Procedures • Training materials • Intranet content
L 1	• Public websites • Academic catalogs • Marketing materials • Published research

"IMPACT TEST" CHEAT SHEET

When uncertain, ask:
"***If this data appeared on the front page of the newspaper tomorrow, what would happen?***"

Outcome	Classification
Nobody would care	L1 - Public
It would be awkward but manageable	L2 – University Internal
We'd need to investigate and notify stakeholders	L3 - Confidential
People could be harmed or systems compromised	L4 – Highly Confidential
We could face major legal, regulatory, or contractual consequences	L5 - Restricted

Rule of Thumb:
Classify based on the potential impact of unauthorized disclosure, **not** who currently has access.

KEY TAKEAWAYS

Remember These Four Things

- ✅ Classify based on sensitivity and risk
- ✅ Use the Decision Tree when unsure
- ✅ Classification ≠ Access
- ✅ Focus on the data, not the user