**University of Alabama at Birmingham**

**DATA CLASSIFICATION RULE**

Approved and Implemented: February 22, 2017

Reviewed/Updated: June 28, 2021

**Related Policies, Procedures, and Resources**

[Data Protection and Security Policy](http://www.uab.edu/it/home/component/k2/item/822-data-protection-and-security-policy)

[Data Access Policy](http://www.uab.edu/policies/content/Pages/UAB-IT-POL-0000789.aspx)

[Acceptable Use Policy](http://www.uab.edu/policies/content/Pages/UAB-IT-POL-0000004.aspx)

[Data Protection Rule](https://www.uab.edu/it/home/policies/data-classification/data-protection-rule)

[Data custodian responsibilities](https://www.uab.edu/it/home/policies/data-classification/data-custodians)

**1.0 Introduction**

The objective of this data classification requirement is to assist the UAB community in the classification of data and systems to determine the appropriate level of security.

**2.0 Scope and Applicability**

All UAB data stored, processed, or transmitted must be classified in accordance with this rule.  Based on classification; users are required to implement appropriate security controls.

**3.0 Classifying Data**

All UAB data must be classified into one of the three following categories.

1. **Public Data:**  This data classification is for data that is low risk. The loss of the data’s confidentiality, integrity or availability **would not** cause harm to UAB’s mission, safety, finances or reputation. This is data that UAB has chosen or is required to disclose to the public.

Examples include but are not limited to: *public phone directory, course catalogs, public research findings, enrollment figures, public web sites, general benefits data, press releases, newsletters, etc.*

1. **Sensitive Data:** Thisdata classification is for data that is moderate risk because it should be kept confidential. The loss of the data’s confidentiality, integrity or availability **could** cause harm to UAB’s mission, safety, finances or reputation. Privacy may be required by law or contract. Access to these data shall require authorization and legitimate need-to-know.

Examples include but are not limited to: *FERPA, budgetary plans, proprietary business plans, patent pending information, and data protected by law.*

1. **Restricted/PHI Data:** This data classification is for data that is high risk because it is sensitive data that is highly-confidential in nature. The loss of the data’s confidentiality, integrity or availability **would** cause harm to UAB’s mission, safety, finances or reputation. Privacy and Security are typically required by law or contract.

Examples include but are not limited to: HIPAA, PHI, Social Security Numbers, credit card numbers (PCI DSS), GLBA data, Export Controlled data, FISMA regulated data, login credentials, and information protected by non-disclosure agreements.

|  |
| --- |
| **Note regarding Classification of Research Data** –The classification of research data depends on several factors that can and often do change as research progresses. It is incumbent upon the Researcher to know the type of data, the circumstances governing the data, and classify it accordingly. [More information](https://www.uab.edu/it/home/policies/data-classification/predefined-classifications#s_4-0). |

Responsibilities for Protection and Security of these data may be found in the [Data Protection and Security Policy](http://www.uab.edu/it/home/component/k2/item/822-data-protection-and-security-policy).

\* Abbreviations Used: *FERPA (Family Educational Rights and Privacy Act), HIPPA (Health Insurance Portability and Accountability Act) PHI (protected health information), PCI DSS (Payment Card Industry Data Security Standard), GLBA (Gramm-Leach-Bliley Act) and FISMA (Federal Information Security Management Act)*

**Change History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Description** | **Approval** | **Date** |
| 1.0 | Final version – approved by President Watts | Dr. Ray Watts | 2/22/2017 |
| 1.1 | Added specific related policies, rules & guidance - Data Protection and Security Policy, Data Access Policy, Acceptable Use Policy, Data Protection Rule, Data custodian responsibilities  Removed export controlled information and internal communications from examples under Sensitive Data |  | 12/15/2017 |
|  | Reviewed - no changes/updates |  | 6/4/2018 |
|  | Reviewed - no changes/updates |  | 6/3/2019 |
| 2.0 | Updated links to Data Protection Rule and Data custodian responsibilities  Updated link to more information on research data  Further defined the classification levels in terms of risk to help the UAB community’s understanding. | Dr. Curt Carver | 6/28/2021 |