# NOTICE OF NEW REGULATION

**January 24, 2023**

## FLORIDA BOARD OF GOVERNORS

Division of Universities

University of North Florida

## REGULATION TITLE:

Data Classification & Security

## REGULATION NO.:

15.0060R

## SUMMARY:

The proposed new regulation incorporates current language from UNF policy 15.0060P Data Classification & Security. The new regulation addresses BOG regulation 3.005 *Examinations and Assessments*, which provides an exemption from disclosure under the public records provision of Florida Statutes Ch. 119.07(1). The exemption applies to all examination and assessment instruments, including developmental materials and work papers directly related thereto. The proposed regulation discusses the significance of protecting generated data and sets forth the parameters for data management and classifications.

## FULL TEXT:

The full text of the regulation being proposed is attached.

## AUTHORITY:

Florida Constitution, Article IX, Section 7(c)

Florida Statutes 1008.23

BOG Regulation 3.005

## UNIVERSITY OFFICIAL INITIATING THE PROPOSED REGULATION:

Jeff Durfee, Associate VP and CISO

## INDIVIDUAL TO BE CONTACTED REGARDING THE PROPOSED REGULATION:

Stephanie Howell, Paralegal, Office of the General Counsel, showell@unf.edu, phone (904)620-2828; fax (904)620-1044; Building 1, Room 2100, 1 UNF Drive, Jacksonville, FL 32224.

***Any comments regarding the new of the regulation must be sent in writing to the contact person on or before Wednesday, February 8, 2023, to receive full consideration.***

 Regulation

**Regulation Number**: 15.0060R

**Effective Date**: 02/27/23 **Revised Date**: N/A

# Subject: Data Classification & Security

**Responsible Division/Department**: Information Technology Services

**Check what type of Regulation this is:**

[x] New Regulation

[ ] Major Revision of Existing Regulation

[ ] Minor/Technical Revision of Existing Regulation

[ ] Reaffirmation of Existing Regulation

[ ] Repeal of Existing Regulation

##  OBJECTIVE AND PURPOSE

To educate the University community about the importance of protecting data generated, accessed, transmitted and stored by the University, to identify procedures that should be in place to protect the confidentiality, integrity and availability of University data, and to comply with local and federal regulations regarding privacy and confidentiality of information.

1. **STATEMENT OF REGULATION**

All members of the University community have a responsibility to protect University data from unauthorized generation, access, modification, disclosure, transmission or destruction, and are expected to be familiar with and comply with this regulation. Violations of this regulation can lead to disciplinary action up to and including dismissal, expulsion, and/or legal action. Any known violations of this regulation are to be reported to the University's Chief Information Security Officer (CISO).

1. **RESPONSIBILITY FOR DATA MANAGEMENT**

Data is a critical asset of the University. All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the University, irrespective of the medium on which the data resides and regardless of format (electronic, paper or other physical form).

Departments are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of University data in compliance with this regulation.

Data owned, used, created or maintained by the University is classified into the following three categories:

• Public

• Internal Use

• Restricted

Departments should carefully evaluate the appropriate data classification category for their information and ensure compliance with applicable Information Technology Services (ITS) [data security standards](https://www.unf.edu/its/polproc/index.html).

Departments may delete data records once they are no longer needed, subject to the State of Florida General Records Schedule and [UNF’s Records Management](https://www.unf.edu/controller/records-management/) practices.

**B. DATA CLASSIFICATIONS**

1. **PUBLIC DATA**

Public data is information that may or must be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. Public data, while subject to University disclosure rules, is available to all members of the University community and to all individuals and entities external to the University community.

1. **INTERNAL USE DATA**

Internal Use Data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Internal Use Data is information that is restricted to members of the University community who have a legitimate purpose for accessing such data.

1. **RESTRICTED DATA**

Restricted Data is information protected by statutes, regulations, University policies or contractual language. Restricted data must be protected from unauthorized access, modification, transmission, storage or other use by means of encryption or secure storage, as applicable, in accordance with [ITS data security standard](https://www.unf.edu/its/polproc/index.html)s. Restricted Data may be disclosed to individuals on a need-to-know basis only. Disclosure to parties outside the University should be authorized by the General Counsel’s Office.

The classifications and examples of each type of data are summarized in table 1.

**Table 1: Data Classification Categories**

|  |  |  |  |
| --- | --- | --- | --- |
| **Class**  | **Restricted**  | **Internal Use**  | **Public**  |
| **Legal Requirements**  | Protection of data is required by law or best practices  | UNF has best practice (due care) reasons to protect data  | Data approved for general access by appropriate UNF authority  |
| ***Risk level***  | ***High***  | ***Medium***  | ***Low***  |
| **Consequences of Exposure**  | The University’s reputation is tarnished by public reports of its failures to protect restricted records of students, employees, clients, or research. Such failure may subject the University to litigation.  | Data is disclosed unnecessarily or in an untimely fashion, which causes harm to UNF business interests or to the personal interests of an individual.  | Confusion is caused by corrupted information that may be displayed. |
| **Examples of Specific Data**  | * FERPA protected data
* Research – export controls, EAR, ITAR, safeguarding confidential information
* Faculty promotion, tenure, evaluations
* Aggregate human subjects research data
* Animal research
* Information required to be protected by contract
* Human subjects identifiable research data
* Trade secrets, intellectual property and/or proprietary research
* Attorney/client privileged records
* Payment Card Industry (PCI) data
* University banking records
* Restricted police records (e.g., victim information, juvenile records)
* Computer account passwords
* Gramm-Leach-Bliley
* Examination and assessment instruments, including developmental materials and workpapers directly related thereto
 | * Specific technical security measures
* Employment data
* Supporting documents for UNF business functions
* Proposal records
 | * Campus promotional material
* Annual reports
* Press statements
* Tuition information
* Course schedules
* University maps
* Job titles
* Job descriptions
* Employee work phone numbers (with special exceptions)
* Employee work locations (with special exceptions)
* Employee email addresses (with special exceptions)
 |

**III. STATEMENT OF PROCEDURES**

The CISO is the primary entity charged with developing regulation and procedures subordinate to and in support of this regulation. They are charged with the promotion of awareness within the University community, as well as responsibility for the creation, maintenance, enforcement and design of training on relevant security standards in support of this regulation and other applicable policies.

The CISO will receive and maintain reports of incidents, threats and malfunctions that may have a security impact on the University's information systems and will receive and maintain records of actions taken or policies and procedures developed in response to such reports. The CISO will assist the Internal Audit Department as appropriate, in conducting periodic audits to determine University compliance with this regulation.

The CISO must be notified in a timely manner if data classified as Restricted is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the University's information systems has taken place or is suspected of taking place.

*Approved by the BOT\_(date).*