



<b>SUBJECT:</b> RESPONSIBLE USE OF DATA ACCESS	<b>Effective Date:</b> 5-31-11	<b>Policy Number:</b> 12.3	
	<b>Supersedes:</b> New	<b>Page</b> 1	<b>Of</b> 2
	<b>Responsible Authority:</b> Associate Vice President, Information Resource Management and Chief Information Officer		

**APPLICABILITY/ACCOUNTABILITY:**

This policy is applicable to all employees, students, volunteers and contractors of the University with access to University data.

**POLICY STATEMENT:**

**I. POLICY**

Florida Atlantic University grants persons or entities access to certain University data in order to support the educational and research objectives of the University. For those granted access to University data, such data should only be used for the limited purpose for which access was given and should not be used for personal or commercial use or shared with other persons or entities unless in furtherance of job responsibilities or in response to a public records request coordinated through the Office of University Communications. Moreover, use and access must be in compliance with applicable federal, state, and local laws and regulations and all University regulations and policies, specifically including without limitation those pertaining to the privacy of student records.

An individual may not directly modify any data in his or her own personnel or student records or those of relatives stored in electronic databases maintained by the University except through the general employee or student portions of MyFAU or similar systems. In cases where an individual's job requires that the individual makes changes to his or her record or the record of a relative, that individual will request that another authorized individual make the required modifications on their behalf, and will not make the change him or herself. This restriction does not apply to systems that are deemed to be testing/development environments or do not hold official University information, or to record modifications that are part of a routine automated process.

## II. CONFIDENTIALITY AND WHISTLEBLOWER PROTECTIONS

If an individual suspects that someone is violating this policy, that individual has the responsibility to report the violation to their supervisor. Individuals reporting violations are protected from repercussions arising from the reporting of the violation by whistleblower protections under Florida Statute 112.3187.

## III. SANCTIONS

Violations of these policies described herein by an employee or student are grounds for disciplinary action up to and including termination or expulsion in accordance with applicable University and the Florida Board of Governors regulations and/or collective bargaining agreements. Such disciplinary actions may also include reprimand or suspension. Violations of these policies by volunteers or contractors are grounds for terminating their access rights and other appropriate sanctions.

Disciplinary or other action taken by the University does not preclude the possibility of criminal actions against an individual violating this policy. The filing of criminal charges similarly does not preclude action by the University.

## IV. RELATED INFORMATION

Additional guidance concerning access and use of University data can be found in [University Policy 1.9 \(Fraud\)](#), [University Policy 5.6 \(Identity Theft Prevention Program\)](#), and [University Regulation 4.008 \(Access to Student Records\)](#).

**INITIATING AUTHORITY:** Associate Vice President, Information Resource Management and Chief Information Officer

---

POLICY APPROVAL  
(For use by the Office of the President)

Policy Number:   12.3  

*Initiating Authority*

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Name: \_\_\_\_\_

*Policies and Procedures  
Review Committee Chair*

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Name: \_\_\_\_\_

*President*

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Name: \_\_\_\_\_

---

Executed signature pages are available in the Office of the General Counsel