FIU FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

IT Security: Sharing Access to IT Resources; Password Management # 1930.022

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 2007	June 9, 2021	Division of Information Technology/IT Security Office

POLICY STATEMENT

Individuals who have been granted physical or electronic access to a University IT resource by being personally issued a specific access code or codes shall not share the access code(s) with any other person. No individual should ask you for your access code(s) for any purpose. No one should access any University IT resource using another person's access code(s) and must read and adhere to FIU's Password Requirements. FIU Accounts and access to FIU resources shall be terminated upon termination of employment.

"Access code" is not to be confused with PantherID, which has been issued to you as a unique University identification number.

SCOPE

This policy applies to all faculty, staff, and students and authorized third party affiliates (consultants, vendors, person's of interest)

REASON FOR POLICY

The University is subject to federal and state laws that require that it have in place administrative and technical standards to safeguard the confidentiality, integrity and availability of the data it creates and maintains. One such administrative and technical standard is to limit access to the data based on the individual's need for such access. Access to University IT resources have been granted to students, faculty, and staff based on their roles and responsibilities at the University. This ensures that, as a member of the University Community, you have access to only those resources necessary to perform your studies, job function, and/or business transactions with the University. Limiting access to IT resources by using access codes enables the University to better monitor and control usage of its resources. In the case of PantherSoft, moreover, controlling access precludes individuals from being able to view system data and records to which they should not be privy, and it precludes individuals from initiating transactions which they are not authorized to perform.

DEFINITIONS

TERM	DEFINITIONS
Individual	Refers to any current student, faculty, staff of Florida International University, and to any other persons who are authorized to use University IT Resources.
IT Resources	Include, but are not limited to: FIU computers, campus network, Devices, Voice Mail, e-mail, applications, software, Panthersoft systems and records.
FIU Information Technology Resources (IRT)	Computing/networking equipment and technology-related services provided by the University.
FIU Network	The University's Intercampus network. FIUnet, including all connected sub-networks.
Access code	Refers to any password, PIN number, key card, or other device issued to an individual to allow his/her sole access to an IT resource. This is not to be confused with PantherID, which has been issued as a unique University identification number.

ROLES AND RESPONSIBILITIES

FIU Supervisory Staff:

- To issue or request issuance of appropriate access codes for students, faculty, staff, or others so they may gain access to those information resources which they properly need to conduct their studies, do their assigned jobs, and/or to conduct business for the University.
- To cancel or request cancellation of access codes for individuals who no longer have student, employment, or special authorization status. Follow the HR Separation of Employment Process.
- In case of employees who are transferring or separating from employment with FIU, to adhere to the Separation of Employment/Transfer Clearance Procedure.

FIU Staff:

- To notify the IT Security Office immediately concerning incidents where access codes may have been disclosed, compromised, or stolen by calling 305-348-1366 or by sending email to security@fiu.edu or submitting an incident report at https://askit.fiu.edu .
- To notify the IT Security Office immediately concerning instances where individuals have used others' access code(s) to access an IT resource.
- To read and adhere to the FIU Password Requirements.

Division of Information Technology:

- To issue/cancel individuals' access codes.
- To reset access codes that have been forgotten or compromised.
- To record and safeguard access code information for all central IT resources.

- Never ask for an individual's password (access code).

Individuals:

- To refrain from accessing any University IT resource using another person's access code(s).
- Should use two factor authentication to protect University accounts.
- To keep confidential their access code(s) and prevent access codes from being disclosed.
- Change password immediately upon indication of compromise.
- To notify the IT Security Office immediately concerning incidents where access codes may have been disclosed, compromised, or stolen by calling 305-348-1366 or by sending email to security@fiu.edu or submitting an incident report at http://askit.fiu.edu .
- Learn more about FIU's Password Requirements https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010192

RELATED RESOURCES

Security Office Website https://security.fiu.edu
FIU Account and Password information https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB001019100
Getting Started with Two Factor Authentication https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0011550
FIU's Password Requirements https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010192
Person of Interest Accounts https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010203
Separation & Retirement https://hr.fiu.edu/leadership/separation-retirement/

CONTACTS

Division of Information Technology
IT Security Office
11200 SW 8 St, PC534a
Miami, FL 33199
305-348-1366
security@fiu.edu
https://security.fiu.edu

HISTORY

Initial Effective Date: October 2007
Review Dates (*review performed, no updates*): May 20, 2024
Revision Dates (*updates made to document*): June 9, 2021 (formerly 1930.020b procedure converted into policy)