University Community (faculty, staff and students) and
Authorized Users of University’s IT Resources (e.g., consultants, vendors, etc.)

<table>
<thead>
<tr>
<th>SUBJECT (R*)</th>
<th>EFFECTIVE DATE (R)</th>
<th>PROCEDURE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT SECURITY PROCEDURE: SHARING ACCESS TO IT RESOURCES; PASSWORD MANAGEMENT</td>
<td>October 2007</td>
<td>1930.020b</td>
</tr>
</tbody>
</table>

PROCEDURE STATEMENT (R)

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 the Guidelines for Password Management.

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

REASON FOR PROCEDURE (O*)

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.

DEFINITION (R)

Individual: Refers to any current student, faculty or staff member 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, the campus network, FIU dial-ups, Voice Mail, FIU e-mail, and all PantherSoft systems and records.

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.

RESPONSIBILITIES (O)

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.

- In case of employees who are transferring or separating from employment with FIU, to adhere to the Separation from
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 305-348-3712 or by sending email to http://security.fiu.edu/ or submitting an incident report at http://security.fiu.edu/.

- To notify the IT Security Office immediately concerning instances where individuals have used others’ access code(s) to access an IT resource by calling 305-348-3712 or by sending email to http://security.fiu.edu/ or submitting an incident report at http://security.fiu.edu/.

- To read and adhere to the Guidelines for Password Management.

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.

Individuals:

- To refrain from accessing any University IT resource using another person’s access code(s).

- To keep confidential their access code(s) and prevent access codes from being disclosed.

- To notify the IT Security Office immediately concerning incidents where access codes may have been disclosed, compromised, or stolen by calling 305-348-3712 or by sending email to http://security.fiu.edu/ or submitting an incident report at http://security.fiu.edu/.

- To read and adhere to the Guidelines for Password Management.

RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)

Division of Information Technology
Florida International University

RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*)

IT Security Office
Florida International University
11200 S.W. Eighth Street, LIB 328
Miami, Florida 33199
Telephone Number: (305) 919-4299

The University Policies and Procedures Library is updated regularly. In order to ensure a printed copy of this document is current, please access it online at http://policies.fiu.edu/.

For any questions or comments, the “Document Details” view for this procedure online provides complete contact information.

FORMS/ONLINE PROCESSES (O)

Guidelines for Password Management
Separation from Employment/Transfer Clearance Form

Link(s) to the above referenced Forms available in the "Document Details" Section of the online version of this policy document.

R*=Required   O*=Optional