FLORIDA A&M UNIVERSITY
INFORMATION TECHNOLOGY SERVICES (ITS)

EXCELLENCE WITH CARING

iRattler (PeopleSoft) Security Procedures v2 – 12/20/2017

Security Access

1. Access to the PeopleSoft (iRattler) system is granted to Florida A&M University employees, persons of interest and other authorized personnel who have an approved business need to work within the system to view data and reports.
2. The iRattler System consists of the following applications: Human Capital Management System, Financial System Management, Campus Solutions and Enterprise Portal.
3. Access to the system is obtained by completing the iRattler Access Request Form. This form also contains a confidentiality statement. The requester must have a valid employee number and email address prior to submitting the request. The form must be signed by the requester and the requester’s supervisor. Access will not be granted if the form is incomplete.
4. The completed form should be submitted to Organizational Development and Training (ODT) for the appropriate training. If additional training is required, the corresponding office will contact the requester for training. Each employee or person of interest must successfully complete training correlating with the requested access checked on the iRattler Access Request form. The form may be faxed or emailed to ODT.
5. Upon successful completion of training through ODT, the access form is forwarded to the respective assistant/associate director (SME) of the respective application. If additional training is required the form is forwarded to the appropriate core office for approval and training.
6. After all training has been completed and the form has been approved by the SME, the form is submitted to ITS Security.
7. ITS security grants the appropriate access to the requester. The requester/user is contacted via email stating the requested access has been processed.

Modification to Existing Access

1. Access is modified when additional pages are required to perform an assigned task or if an end-user changes positions or departments.
2. A new completed iRattler Access Request form is required for modification of an end-user’s access. The process is the same as submitting a new request for access.
3. Upon successful completion of training through ODT, the access form is forwarded to the respective assistant/associate director (SME) of the respective application. If additional training is required the form is forwarded to the appropriate core office for approval and training.
4. After all training has been completed and the form has been approved by the SME, the form is submitted to ITS Security. If training is not required, the form is forwarded by ODT to the appropriate SME.
5. ITS security grants the appropriate access to the requester. The requester/user is contacted via email stating the requested access has been processed.

Removing or Deleting Access

1. Access is removed or deleted by written notification from the user's supervisor.
2. Access is removed from a user if the user changes positions or is no longer working in that particular department. The supervisor is responsible for notifying ITS of any employment changes within their respective area.
3. Access may also be removed from a user if the supervisor deems the access is no longer required by the user to perform their duties.
4. Termination of an employee's access is determined by the report received from Human Resources Exit Survey. This report lists the employee's separation date. The Human Resource profile for the employee is left open for sixty (60) days past the separation date to ensure the employee is able to view his/her pay advice and make necessary changes regarding their personal information.
5. All other applications and access, with the exception of Human Resources Self Service and Campus Solutions Student will be adjusted/removed.

Correction Mode

1. Correction mode is the ability to retrieve all rows and allows one to modify any row and insert new rows regardless of the sequence or effective date.
2. Correction mode is to be used only in an effort to correct a mistake; not for updating records due to other adjustments.
3. Correction mode access is granted primarily to the core offices (business owners) and ITS staff.
4. Correction mode may be used for data changes (incorrect information was provided), data entry errors, inserting pertinent information to maintain the history integrity, or an error message generated by PeopleSoft code.
5. Correction mode should not be used when it is possible to eliminate a sequence which will change the history of the record. Entering data using effective data creates an audit trail for the record.

Password Resets

Password resets are handled by the user through Password Manager. If the user is in need of assistance changing their password, the user should contact the HelpDesk at 850-412-4357 (HELP).

Temporary/Guest User Policy

1. Guest accounts are established by ITS Security team as deemed necessary by the Chief Information Security Officer, Chief Information Officer or a member of the Executive Council.
2. All request for a temporary/guest account must be done in writing, either an email or a memorandum.
3. The information in the document should be the name of the individual requiring a guest account, the purpose for the account usage, duration of account and contact information for the individual. A blank iRattler Access Request form will be forwarded to the guest user for signature. The signed form and letter documenting the request are stapled and filed together.
4. Upon receiving the requested information for a guest account, a member of the security team will inform the respective SME and obtain their signature.
5. ITS security grants the appropriate access to the guest user. The guest user is contacted via email stating the requested access has been processed and sharing the guest user id. A phone call is made to the guest user giving the password for the id.

Ronald E. Henry, II. Associate Vice President / Chief Information Officer

APPROVED 12/21/2017