CPTC Procedure: Internet Native Banner (INB) Account Management

The purpose of this procedure is to establish an authorized method for creating, altering, and decommissioning INB accounts at Coastal Pines Technical College (CPTC).

Note: this procedure is a derivative of a section of the TCSG Security Guidelines. Any changes or differences in the TCSG document will supersede the CPTC procedure.

INB Account Request:

There are three milestones that require action for INB accounts by the College Banner Project Leader (BPL). They are as follows:

- Initial creation of the INB account.
- Altering of permissions due to a change in employee job responsibilities.
- Decommissioning of the INB account once an employee is terminated.

The initial creation of an INB account is preceded by a few events, they are as follows:

- Employee is hired and onboarded by HR.
    - In this process, HR creates the Active Directory account for the employee.
- The Registrar generates a Banner ID for the employee.
- The Vice President (VP) of Student Affairs opens a ticket requesting specific access for the employee.
    - This ticket will include the Banner Access Security Form.
    - The form must be signed by the appropriate VP(s) and includes the employee Banner ID.
- The VP may:
    - request permissions that are similar to another employee.
    - specify the Banner forms that the employee will require access to so that they can perform their job duties.

INB Account Creation:

Once these steps have been followed, the BPL will login to Banner Access Management and create the employee's INB account. This includes granting permissions (query or maintenance) to Banner forms, entering a complex password, authorizing login, and associating the employee Banner account with the corresponding INB account. Ellucian defines Read-Only access as Query access and Read/Write as Maintenance access.

After the Banner account is associated with the new INB account, the employee's UDC Identifier and Banner ID are added to the respective Attribute fields in Active Directory. Within 30 minutes, Active Directory should sync these updated attributes with Okta. Okta will then allow the employees to authenticate and access protected data using their INB accounts.

Altering INB Account Permissions:

INB account permissions will be altered for one (or more) of the following reasons.

- The employee has changed positions.
- The employee's job responsibilities have changed due to other staffing changes.

- The employee's INB account permissions are identified by the KMS Separation of Duties (SoD) report as being inappropriate.

Altering the permissions of an INB account requires a ticket from the Vice President of Student Affairs or the department head for the employee needing the change, i.e. VPAA or VPAS. *Note: Approval by the Vice President of Student Affairs may still be necessary depending on the data access or system ownership.*

The ticket should include a detailed list of permissions that need to be granted or revoked as well as a completed Banner Access Security Form. Only necessary permissions should be requested and granted in compliance with the principle of least privilege.

If an employee's permissions are indicated as inappropriate by the KMS SoD report, it is the responsibility of the BPL and the department head for the employee to identify the appropriate permissions for the job duties of that employee. With any permissions change, a ticket is required. If the employee in question requires permissions that do place their INB account on the KMS SoD report, written justification by the department head of the forms in question is required.

Decommissioning INB Account:

Deprovisioning an INB account is completed once HR informs the BPL of the termination/separation of any employee. When this occurs, the BPL performs the following actions:

- All Banner security classes are removed from the INB account.
- INB account authorization is disabled.
- INB account login is disabled.
- INB account Oracle password is manually expired.

Data Owners

Data Owners are individuals who have been identified as being responsible for certain types of data. These Data Owners can request that their direct reports, or other employees, receive access to the data they own, but the ultimate approval still falls on the VP over each module of Banner. (This can be seen on the Banner Access Security Form)

- Recruiting – Vice President for Student Affairs / Executive Director of Student Affairs
- Admissions – Vice President for Student Affairs / Admissions Director
- Transfer Work – Vice President for Student Affairs / Registrar
- General Student – Vice President for Student Affairs / Admissions Director
- Registration – Vice President for Student Affairs / Registrar / Vice President for Academic Affairs
- Housing – N/A
- Faculty – Vice President for Academic Affairs

Responsibility

The Banner Project Leader is primarily responsible for executing this procedure, but ultimate responsibility falls on the Executive Director of Information Technology for ensuring this procedure is implemented.

Adopted: September 19, 2023
Effective Date: September 19, 2023