VII 01 28 Faculty/Staff Computer and Banner Account Creation/Deletion Policy

Purpose:

The purpose of this policy is to establish procedures for requesting, enabling, and disabling of computer accounts and accesses for faculty and staff.

Policy:

A. Disabling of accounts

a. All accounts, regardless of role, will be disabled after 30 days if the account is not accessed via computer, portal, or email logon. If the employee is no longer employed by Volunteer State, the account will be deleted. If the employee is actively employed, the account will be re-enabled via request to the IT helpdesk.

b. Risk tolerance: A 30-day window of inactivity is considered to be a low security risk, except in cases noted in the account role tables below.

B. Definition of roles

a. Access policies are defined by a role-based perspective. The roles defined below are designed with the understanding that future roles may be defined in the future, and that an individual may have more than one role. For example, a staff member may also be an adjunct faculty.

b. The primary roles are:

i. Full-time faculty member

ii. Adjunct faculty member

iii. Full-time staff

iv. Part-time/temporary staff

v. Volunteer/non-employee/contractor

vi. Elevated security accounts (may exist in departments such as Financial Aid, Information Technology, Business and Finance, Records and Admissions and may be full-time or part-time.)

C. Breakdown of access type

a. In order to simplify access and define risk and tolerance, the access levels are defined as follows:

i. Basic: Email access, computer logon, wireless network access, network folder access, self-service Banner (SSB).

ii. All access to systems beyond basic is granted by account role. Such systems that require elevated access are:

1. D2L

2. Banner INB

3. Other departmental and college systems

b. Accounts will be created and deleted based upon triggers. These triggers are based upon Banner as the source of authority. All accounts, as noted above, are subject to a 30-day inactivity-based disable. Account triggering activities are:

i. Employment start date

ii. Employment end date by resignation

iii. Termination

iv. Date of retirement

D. Access tables

a. The tables below lay out creation and deletion activities for each account role, as well as risk and tolerance for each role.

Role	Access Type	Account Creation	Actions on Creation	Account De-provision Timing	Actions on De-provision	Risk And Tolerance
Full-time Faculty						
	Basic	On completion of onboarding by Human Resources.	Notifications: Human Resources, Payroll, Department Head, Information Technology, Campus Police	Account will be disabled on last working day, retirement date, or termination. Notifications: Human Resources, Payroll, Department Head, Information Technology, Campus Police	Department heads will be granted 30 days email and network folder access for review. After 30 days, account will be deleted.	**Low Risk:** Basic account access caries little risk to systems or sensitive information.
	Banner INB	Upon request to Information Technology and approval of Banner Data Approvers for access.	Notifications: Information Technology, Department Head, Data Approvers	Last working date or request by department head.		**Low risk**: INB access granted to this role carries low risk of manipulation of data.
	D2L	Automatic creation from Banner once basic account is created.	Part of basic notification.	Last working date.	De-provisioned with basic account.	**Low Risk:** Account carries low risk to data or systems.
	Other college systems	Upon request to Information Technology or departmental system administrator	Notifications: Information Technology, Department Head	Last working day		**Low Risk:** These accounts carry little risk to systems or sensitive information.

Role	Access Type	Account Creation	Actions on Creation	Account Deprovision Timing	Actions on Deprovision	Risk And Tolerance
Adjunct Faculty						
	Basic	-Access will not be granted until one week before the semester of their employment begins. Exceptions to this rule can be made by a request by Deans to Information Technology. - Deans are responsible for requesting accounts for their division by completing and submitting an Adjunct Faculty Account Authorization form. -Information Technology will create a computer account that is disabled. The account will be enabled during the Account Re-Activation process described in the next column.	-The division office will run the Banner process to set up the adjunct faculty in FLAC. -The automated adjunct account re-activation process will then activate the account until ten days after the semester begins or ten days after the Banner process was run, whichever is later. This is to allow the adjunct faculty member time to acknowledge the FLAC contract for the semester. -Adjunct faculty must acknowledge their FLAC contract within this ten-day window.	Once the adjunct faculty member has acknowledged the FLAC contract an automated process will extend the account access until: Ten days into the Spring semester for Fall adjunct faculty Ten days into the Fall semester for Spring adjunct faculty Ten days into the Fall semester for Summer adjunct faculty	Account will be deleted.	**Low Risk:** Basic account access caries little risk to systems or sensitive information.
	Banner INB	No INB access will be granted to adjunct faculty.	Part of basic notification.	De-provisioned with basic account	Account is deleted.	**Low Risk:** Account carries low risk to data or systems.

	D2L	Automatic creation from Banner once basic account is created.				

Role	Access Type	Account Creation	Actions on Creation	Account Deprovision Timing	Actions on Deprovision	Risk And Tolerance
Full-time Staff						
	Basic	On completion of onboarding by Human Resources.	Notifications: Human Resources, Payroll, Department Head, Information Technology, Campus Police	Account will be disabled on last working day, retirement date, or termination. Notifications: Human Resources, Payroll, Department Head, Information Technology, Campus Police	Department heads will be granted 30 days email and network folder access for review. After 30 days, account will be deleted.	**Low Risk:** Basic account access caries little risk to systems or sensitive information.
	Banner INB	Upon request to Information Technology and approval of Banner Data Approvers for access.	Notifications: Information Technology, Department Head, Data Approvers	Last working date or request by department head.		**Low risk**: INB access granted to this role carries low risk of manipulation of data.
	D2L	Upon request from department head to Distributed Education.	Notifications: Department head	Last working date or request by department head.		**Low risk**: D2L access carries little risk to sensitive information.
	Other college systems	Upon request to Information Technology or departmental system administrator	Notifications: Information Technology, Department Head	Last working day		**Low Risk:** These accounts carry little risk to systems or sensitive information.

Role	Access Type	Account Creation	Actions on Creation	Account Deprovision Timing	Actions on Deprovision	Risk And Tolerance
Part-time/Temporary Staff						
	Basic	On completion of onboarding by Human Resources.	Notifications: Human Resources, Payroll, Department Head, Information Technology, Campus Police	Account will be disabled on last working day. Notifications: Human Resources, Payroll, Department Head, Information Technology, Campus Police	Department heads will be granted 30 days email and network folder access for review. After 30 days, account will be deleted.	**Low Risk:** Basic account access caries little risk to systems or sensitive information.
	Banner INB	Upon request to Information Technology and approval of Banner Data Approvers for access.	Notifications: Information Technology, Department Head, Data Approvers	Last working date or request by department head.		**Low risk**: INB access granted to this role carries low risk of manipulation of data.
	D2L	Not applicable				
	Other college systems	Upon request to Information Technology or departmental system administrator	Notifications: Information Technology, Department Head	Last working day		**Low Risk:** These accounts carry little risk to systems or sensitive information.

Role	Access Type	Account Creation	Actions on Creation	Account Deprovision Timing	Actions on Deprovision	Risk And Tolerance
Volunteer/non-employee/contractor						
	Basic	Department head will submit a Non-Employee Account Authorization form to Information Technology	Notifications: Human Resources, Payroll, Department Head, Information Technology, Campus Police	Account will be disabled on last working day. Notifications: Human Resources, Payroll, Department Head, Information Technology, Campus Police	Account will be deleted.	**Low Risk:** Basic account access caries little risk to systems or sensitive information.
	Banner INB	Access will not be granted. Exceptions to this rule can be made by request by a Vice President to the CIO.				
	D2L	Not applicable				
	Other college systems	Upon request to Information Technology or departmental system administrator	Notifications: Information Technology, Department Head	Last working day		**Low Risk:** These accounts carry little risk to systems or sensitive information.

Role	Access Type	Account Creation	Actions on Creation	Account Deprovision Timing	Actions on Deprovision	Risk And Tolerance
Elevated security accounts						
	Basic	On completion of onboarding by Human Resources.	Notifications: Human Resources, Payroll, Department Head, Information Technology, Campus Police	Account will be disabled on last working day, retirement date, or termination. Notifications: Human Resources, Payroll, Department Head, Information Technology, Campus Police	Account will be deleted.	**Low Risk:** Basic account access caries little risk to systems or sensitive information.
	Banner INB	Upon request to Information Technology and approval of Banner Data Approvers for access.				**High risk**: This elevated access caries high risk to systems and information and should be deleted on last working day.
	D2L	Not applicable				
	Other college systems	Upon request to Information Technology or departmental system administrator	Notifications: Information Technology, Department Head	Last working day		**Low Risk:** These accounts carry little risk to systems or sensitive information.

VSCC Source: President's Cabinet, March 5, 2018