Section:	X.3.7	
Title:	Information Systems Access	
Effective Date:	October 1, 2019	
Approved By:	Chief Information Officer and Vice President for Information Technology and Campus Safety	
Responsible Unit:	Division of Information Technology and Campus Safety (609) 771-3353; itoffice@tcnj.edu	
Related Documents:		
History:		
Version	Date	Notes
1.0	10/01/2019	New policy; initial release

I. INTRODUCTION

The purpose of this policy is to provide guidance in meeting The College of New Jersey's ("TCNJ" or the "College") obligation to ensure that access to information technology systems and services is based upon authorization and that unauthorized access is prevented.

This Policy applies to the entire TCNJ campus community. Specifically, it applies to:

- All units, faculty, staff, and workforce members that create, process, maintain, transmit, or store institutional data on any college owned device, whether or not it is connected to the campus network and whether or not it is college or self-managed;
- All college computer and telecommunications systems, including externally hosted systems that are accessed via TCNJ authentication systems or owned by the college;
- Personally owned devices, in accordance with TCNJ policy
- Any third-party provider (example contingent workers) with a contractual relationship with the college that maintains institutional data.

II. DEFINITIONS

N/A

III. POLICY

A. TCNJ Information Technology establishes the framework for provisioning and de-provisioning access for students, staff and faculty to TCNJ systems and

applications that create, process, maintain, transmit, or store institutional data. The objective is to provide the required access while protecting the College's institutional data from compromises or breaches due to inadequate access and authentication management practices, as well as capture the information needed for compliance-related audit trails. Well-structured access management results in College personnel and students having access to the right services at the right times based on their current position or job responsibilities.

B. Access to systems that create, process, maintain, transmit, or store institutional data is primarily role-based. Affiliation with TCNJ determines an individual's eligibility for standard TCNJ account access. Administrative and privileged access to TCNJ systems, as well as access to departmentally-provided services, are initiated and the responsibility of the individual's department or unit. TCNJ departments are responsible for ensuring that individual requests for access to systems are limited to systems and access levels required for the individual's work-related responsibilities.

C. Generating a TCNJ Profile, granting and revoking access to our Enterprise Systems varies based on your role at TCNJ (Student, Staff, Faculty, Adjunct, etc) The rules associated with each group can be found here. Access Management Matrix.

Access Control Requirements	Description
User Identification	The identification of authorized users of the information system and the specification of access privileges is fundamental to access control. Eligible college users are granted one unique user identification and password on the college network to ensure accurate auditing of access and actions; departments will not share individual user IDs for system access. Eligible non-TCNJ users must follow the established process for sponsored affiliates, guest accounts, or documented trusted relationships. There are instances where SSO is not available for applications. In these cases, individual login credentials will need to be given to or created by the end users.

Responsible Use Notification and User Acceptance Login Banner	Where technically feasible, TCNJ SSO login and active directory login must include notification of user requirement to abide by the Computer Acceptable Use policy and provide for one-time user acknowledgment of such requirement. Currently this a form signed by new employees through HR.
Principle of Least Privilege	Individuals should be granted the minimum access sufficient to complete their job responsibilities. Individuals that are granted privileged access should use the least privileged account for day-to-day activities; privileged accounts should only be used when the elevated privilege is required.
Separation of Duties	No one person should have responsibility for more than one related function. For example, the person with the authority to grant access should not be the person who fulfills the request, or audit functions should not be performed by the personnel responsible for administering access. At no time should any person have the ability to fulfill and grant access to themselves.
Training and Compliance	Prior to being granted access to any enterprise system or application or database, staff members must complete the appropriate required institutional or unit-specific training. In some instances, staff members may be required to formally attest to their agreement with terms and conditions before access is provided.
Additional Access Controls for Restricted and High Data	In addition to enforcing authorized access at the information system level, additional role-based access enforcement mechanisms should be employed wherever feasible at the application level for Restricted and Confidential data.
Unauthorized Access	Users must not attempt to gain access to college information systems or databases for which they have not been given proper authorization.
Session Termination	All users are required to logoff or lock their systems when they are finished with their current session or are away from their workstation.

Access Revocation or Termination	Authorized access of TCNJ faculty, staff, and workforce members should be revoked in accordance with the Access Management Matrix. The Access Management Matrix applies to employees or students who are: ● Leaving TCNJ or whose employment or affiliate status is terminated; ● Transferring from one position to another with different responsibilities and levels of access required
Access Review	User, privileged, and shared accounts should be reviewed at least annually.
Regulatory and Contractual Compliance	Systems or devices that must adhere to specific regulatory and/or contractual compliance are mandated to meet those specific requirements or implement alternative compensating controls with proper documentation.