Policy & Procedure No. IT-003

Northshore Technical Community College

Title:	Access and Identity Management
Effective Date:	11/20/2017
Last Revision Date:	11/20/2017
Cancellation:	
Office:	Information Technology (IT)

Access and Identity Management Policy

PURPOSE

This policy establishes principles, provisions, responsibilities, and actions by which the identity, specifically the electronic identity, of natural persons who have a relationship with Northshore Technical Community College (NTCC) as well as their access privileges are managed across the College.

SCOPE

This policy applies to those responsible for the management of user accounts or access to shared information or network devices. Such information can be held within a database, application, or shared file space. This policy covers departmental accounts as well as those managed centrally. This section also applies to any and all applications, systems, clients, servers, devices, portals, or third party used by the College. Access permissions are managed, incorporating the principles of least privilege and segregation of duties. Security validation or screening shall be included within the NTCC Office of Human Resources processes, including performing background checks.

INFORMATION SECURITY TEAM

The Information Security Team (IST) is responsible for the review, approval, and management of user accounts or access to shared information systems or network devices. The IST functional ownership is listed as follows; however, any functional area not listed should be approved by a position listed within the IST Team.

IST Function	**Responsible Position(s)**
Finance/Accounting	Vice Chancellor of Finance/Director of Accounting
Student AR	Vice Chancellor of Finance/Director of Accounting
Student/Academics	Provost & Vice Chancellor of Academic Affairs
Financial Aid	Associate Provost of Student Affairs/Director of Financial Aid
Human Resources	Director of Human Resources
Workforce Development	Vice Chancellor of Strategic Initiatives
Information Technology	Director of IT/Network Engineer
Other function(s) not listed	Appropriate Vice Chancellor/Director of IT or Network Engineer and/or employee’s supervisor

IDENTITY MANAGEMENT

All systems, applications, and software utilized by NTCC shall comply with the following list of requirements:

- Each user, including Employee, independent contractor, third party users, shall review and sign the End User Security Agreement form IT-002.
- Each user shall be assigned a unique ID that is created in approved identity management repositories.
- User accounts or IDs issued to third parties or independent contractor shall be configured to automatically expire at the end of the contract or engagement date.
- User accounts or IDs **shall not** be created locally within applications, devices, and systems unless approved by the Information Security Team (IST).
- User accounts or IDs used for guest networks shall be strictly limited and isolated for guests only and access shall be automatically removed or disabled upon completion of engagement or 30 days, whichever occurs first.
- A user account or ID and password must be presented each time a user logs into the network.
- System Administrator accounts will not be granted direct remote access to any NTCC network or application. System administrators shall authenticate to the network using their standard user account credential and then, if performing any system administrative job function, authenticate using their unique privileged level account credentials.
- System administrators shall use privileged accounts only for approved system administrator purposes.

PASSWORDS

All users, systems, and applications shall comply with the following:

- Passwords **must not** be stored in clear text or reversible encryption formats.
- Passwords **must not** be transmitted in clear text or insecure protocols.
- Passwords must comply with Password Requirements.
- Passwords must be stored and transmitted in compliance with Encryption.

For any user account issued by NTCC or approved third party or any additional user account created to facilitate operational processes for the College, all users shall take reasonable precautions to protect the confidentiality, integrity, and secrecy of their password, including but not limited to:

- Notify the Information Security Team (IST) in the event of an actual or suspected password compromise.
- **Never** share their passwords with any other person.

- **Never** write down passwords or use and store passwords in a readable electronic form, including batch files, automatic login scripts, software or keyboard macros, or terminal function keys.
- Where possible, not locally "cache" any passwords or select the option to "remember my password" within a client application as selecting this option will likely store the password in an insecure manner.
- **Never** store or "cache" passwords within any system or application not approved, managed, owned, or hosted by NTCC. (i.e. Cloud or Internet services)
- Never transmit passwords over email or other forms of electronic communication without use of data encryption compliant with Encryption.

Note: It is not the intention of this policy to create inefficient or frustrating processes for users of any technology; and as such, the IST will gladly review any proposed solution that may securely ease the burden of authentication for any NTCC process.

ONBOARDING NEW USERS

Screening

In accordance with relevant Federal and State laws and regulations, the NTCC Office of Human Resources shall perform background verification checks or credit checks on existing Employees or candidates for Employment.

Terms and Conditions of Access

Prior to granting access to Restricted, Confidential, or Uncategorized Data, NTCC shall verify that the End User Agreement is signed by Employees, independent contractors, and third party users of information assets. The NTCC Office of Human Resources will maintain all Employee related records as the appropriate process owner and IST shall maintain records of all independent contractor and third party user security agreements.

ACCESS CONTROL

Access to data and systems shall be configured based (1) on the Data Classification Level and (2) by the user's job role or responsibility. All systems should be tailored to restrict access to users who need such information to perform their job function (least privilege). All data shall be protected via access controls so that data is not improperly accessed, disclosed, modified, deleted, or rendered unavailable.

Default Minimum Access

All users shall be allowed to have read access to systems, applications, and resources that contain solely Public Data.

Access Based on Job Role

Access to systems that contain Restricted, Confidential, or Uncategorized Data shall be granted based on job role or responsibility, incorporating segregation of duties & internal controls when needed. The parameters of the access are based on user attributes proposed by the supervisor of the NTCC department and will be subject to the additional approval of the IST or Data Owner. Reviews of users' attributes with their access needs are to be performed by the application, system, or Data Owner on a periodic basis to confirm that the access is still necessary and required for that job role. The application, system, or Data Owner shall notify the Information Security Team (IST) if the role or access is no longer needed or appropriate.

Elevated Access

If access is required beyond the initially approved scope of the Job Role and is deemed necessary by the Data Owner, then the Data Owner or delegate must submit an Access Request and receive approval from the IST. Any extensions of temporary Elevated Access must be submitted to and approved by the IST. The IST shall keep all Access Request documentation of extensions on file in accordance with data retention policies. The Data Owner shall review users with Elevated Access periodically to confirm that the access is still necessary and required and shall notify the IST and the user (or the user's manager, if appropriate) if the Elevated Access is no longer needed or appropriate. Users no longer needing Elevated Access will have such access modified or removed.

Third Party Access

Third Party or independent contract users shall only be granted the access necessary to perform their contracted obligation as determined by the Data Owner and deemed appropriate by the IST.
On an annual basis, the Data Owner, assisted by the IST, shall perform a review of third party access.

Emergency Access

In the event of an emergency requiring immediate access, the same access control processes shall be followed, except that if the Data Owner is not available and the need for additional access is critical for continued operations or to address an active incident, then the Chief Information Security Officer/Director of Information Technology may authorize such access. The emergency access shall be documented with an Access Request and the emergency access shall be removed once the situation is resolved.
Resolution of the emergency is determined by Data Owner (or higher authority), CIO, and Vice Chancellor.

REMOTE ACCESS

NTCC shall ensure:

- Reasonable and appropriate technologies and measures to control remote access of systems.
- Secure authentication and cryptographic technologies utilized comply with Password and Encryption requirements.
- An additional factor of authentication (multi-factor) is required for privileged users, users accessing Restricted Data remotely, or for systems designated by the Data Owner or CISO to require multi-factor authentication.
- System configurations maintain the latest antivirus updates and operating system updates pursuant to the requirements within System Configuration.

Third party access to systems is restricted, unless specifically required to fulfill services contained within a signed agreement.

REMOVAL OR SUSPENSION OF ACCESS

Suspension of Access

If the Information Security Team (IST) has evidence or suspicion that an user account or ID is being used in violation of a NTCC policy or in a manner that may cause potential damage to NTCC systems, then the IST may immediately suspend or disable the user or account ID. The IST shall provide notification of the suspended access to the user's direct supervisor.

Standard Removal of Access

Employee, independent contractor, and third party user accounts or IDs created or issued by NTCC or OTS, or an account used solely for NTCC processes shall be disabled or decommissioned upon dismissal or termination of contract.

Supervisors or responsible parties shall notify the assigned NTCC Human Resources contacts as soon as possible, but no later than two business days, following the decision to dismiss an Employee. For contractors, or third party users, the responsible parties shall notify the IST and assigned

For planned dismissals, the Office of Human Resources or any other responsible party shall notify the IST of the planned date of dismissal and the affected the user(s). Access shall be removed for the Employee, contractor, or third party user as soon as possible, but no later than two business days after the date of dismissal.

Sensitive Removal of Access

Removal of access shall be considered sensitive when the user is being dismissed and:

- Has access to systems containing Confidential or Restricted Data.
- Has been granted privileged access.
- May inappropriately use NTCC data after dismissal.

In the event that access requires sensitive removal, the user's supervisor, the relevant Data Owner, or designee shall notify the Office of Human Resources and IST two days prior to the date of the planned dismissal, or earlier if operationally possible.

The IST shall work with the Data Owner, NTCC Leadership, or designee, to coordinate the actions required for removing access at a time closely aligned with the dismissal of the user.
At a minimum, sensitive dismissals requires access to be removed before the close of business that same day.

Change in Role or Position

In situations where the user has changed roles or positions and requires reduced or enhanced access, the user's manager should notify the IST and work with the relevant Data Owner to provide the user with appropriate access that is consistent with his or her job responsibilities.

Unnecessary or Inappropriate Access

In situations where a user has received unnecessary or inappropriate access, is abusing access, or otherwise violating policy, the IST may remove, disable, or restrict access upon becoming aware of the situation or receiving a request from the relevant Data Owner or supervisor.

Based on the potential operational impact, nature of the inappropriate access associated with the situations outlined above, or when deemed necessary by the Chief Information Security Officer (CISO), the IST shall further investigate the event. In instances where the CISO determines the actions by the Data Owner are clearly negligence or misuse, actions shall be taken in accordance with Policy Enforcement.

POLICY ENFORCEMENT

Privacy and Security Audits

NTCC, legislative auditors, or internal auditors may, from time to time, conduct audits of NTCC privacy and security practices to confirm conformance with the Information Security Policy.

Complaints of Privacy Violations

Any person may report suspected violations of the Information Security Policy. Complaints may be reported directly with the Chief Information Security Officer (CISO) or the Information Security Team (IST), and may be in writing, by telephone, or by email. Anonymous privacy complaints may be left on the Information Security Hotline or with the Office of Technology Services (OTS), End User Computing, and Support Services Team.

Reporting Obligations

It is the duty of all State Employees to immediately report, using one of the methods described above, any known or suspected violations of the Information Security Policy by an Agency, its Employees, third parties, and independent contractors. The intentional failure to report violations shall subject the non-reporting party to sanctions as outlined below.

Investigation of Complaints

All complaints regarding privacy and security policies and practices, and compliance therewith will be accepted and considered. Upon receipt of a privacy complaint, the Chief Information Security Officer (CISO), or a designee, shall investigate the allegations. In so doing, the CISO may interview Employees, collect documents, and review logs detailing access and use of data. All Employees shall cooperate fully with the CISO to ascertain all facts and circumstances regarding such complaints. The CISO shall create a report of findings in response to any privacy or security complaints, and shall include the proper assurance functions such as Human Resources, Legal, and Compliance entities during the course of an investigation, as needed. In addition, the CISO shall produce periodic reports for LCTCS concerning the status of privacy and security complaint(s) involving NTCC, its Employees, third parties, or independent contractors.

Non-Retaliation

Neither NTCC nor any Employee(s) shall undertake any action to intimidate, threaten, coerce, discriminate against, or any other retaliatory action ("reprisal") against persons who report a violation of this policy. Persons who engage in acts of reprisal shall be subject to sanctions as outlined below.

Sanctions

Violations of this Policy may result in disciplinary action, up to and including dismissal. Accordingly, NTCC shall notify the appointing authority responsible for the individual that has violated this policy. In addition, if NTCC has a reasonable belief that the individual has violated the law, NTCC shall refer violators to the relevant entity for prosecution, as well as commence legal action to recover damages from the individual. Violators may also be required to complete remedial training.

Policy Reference: Office of Technology Services Access & Identity Management Policy

Review Process:

X	Reviewing Council/Entity	Review Date	Approval Date
X	Leadership Team Committee	10/16/2017	11/20/2017
X	Chancellor	10/16/2017	
X	Director of IT	10/16/2017	

Distribution: Distributed Electronically via College’s Internet
Hard Copy Distribution to NTCC Deans of Campus Administration