North Carolina Office of Information Technology Services

18.12 NCID Service Policy

Purpose: To establish policy and procedures for use of NCID, an authentication and authorization service.

Reference: None.

For More Information: Contact ITS Directory Services

The Office of Information Technology Services (ITS) operates a statewide authentication and authorization service (NCID), an information technology system that verifies user credentials and controls access to technology resources based upon the user's credentials. As part of its responsibilities, ITS sets basic use policy to govern NCID subscribers. ITS also reviews use of the service for compliance with all applicable laws and regulations. Final authority for this policy lies with the State Chief Information Officer.

Definitions

Agency	Any agency, institution, board, commission, bureau, department, division, council, member of the Council of State, or officer of the legislative, executive or judicial branches of State government that subscribes to NCID. Agency also includes counties, cities, towns, villages, other municipal corporations or political subdivisions of the State or any agencies of such subdivisions, the University of North Carolina, community colleges, hospitals, county or city boards of education, other local public districts, units, or bodies that subscribe to NCID.
Authentication	The process of verifying credentials to ensure the identity of users.
Authorization	Authorization controls access to protected resources, determining what a user can do once the user has been authenticated.

Credential	A user id/password combination, or the user id/password combination with a digital certificate or a secure token.
Custodian	A custodian of records for a government agency is the public official in charge of an office having public records.
Directory Services	A database designed to perform massive reads and infrequent writes extremely quickly. A directory service combines the power of the directory database with an easy to use hierarchical namespace and chaining or referral protocol to provide a truly enterprise class infrastructure.
Logging	The tracking of transactions regardless of their success or failure.
Users	All persons who access information technology systems through NCID.

The NCID Service Policy sets the rules and requirements for use of the service. Compliance with this policy is mandatory for continued use of NCID.

The objectives of this policy are to:

- ensure that the use of NCID is related to, or for the benefit of, state government;
- inform users that NCID is subject to the same laws, regulations, policies, and other requirements as information communicated in other forms and formats;
- minimize disruptions to state government activities from inappropriate use of the NCID; and,
- maintain the integrity of NCID Service through the definition of roles and requirements for accessing the NCID directory.

Policy Scope

This policy applies to all NCID users.

Policy Hierarchy

Use of NCID is governed by federal and state laws, policy and standards established by the State CIO, and this policy. The State CIO policy is outlined in the *Enterprise Authentication and Authorization Services Policy*. Each agency may adopt additional policies for the individual users within the agency that meet the minimum requirements set forth in this policy.

In considering the need for additional restrictions and guidelines, each agency may consider its particular needs, mission, available technology, level of staff training, size, geographic diversity, and organizational culture.

Subscribing Agency Responsibilities

When using the NCID system, agencies agree to comply with federal and state laws, and statewide technology policies and standards. The NCID Services Policy is incorporated by reference to the NCID Service Level Agreement. An official's signature on a Service Level Agreement on behalf of an agency evidences the agency's agreement to abide by the NCID Service policy.

Each agency is responsible for the activity of its users and should familiarize each user with the NCID Service Policy provisions that apply to individual users and any additional restrictions or guidelines.

Each agency is responsible for determining access levels for its employee and contractor users.[1] Agencies accomplish the access levels through delegated administration, provisioning and de-provisioning of access, and workflow routing.

Each agency must also define rules for access to their systems and applications, including those access rules controlled by the individual application or system and not NCID.

Directory Access

Agency access to the NCID directory must occur through Oracle NetPoint Access Servers.

NCID Security

Individual users must take all reasonable precautions to prevent the use of their identity by unauthorized individuals. Transmission of information to locations outside of the agency's local area network may require the use of the Internet for transport. Individual users should realize that the Internet adheres to open standards and is inherently not secure. Agencies should ensure that a secure, encrypted connection exists to applications accessed through NCID when the data being accessed or transferred is confidential. NCID passwords will be encrypted in transit as well.

Credential Protection

Credential protection is governed by the Statewide Information Security Manual, Standards: 020106 – Managing Passwords; 050706 – Logon and Logoff from your Computer; and 100302 – Keeping Passwords/PIN Numbers Confidential.

[1] ITS is responsible for establishing citizen and business accounts.

For government employees and contractors, passwords must be at least eight characters long and contain at least one symbol.[2] Passwords for government employees and contractors shall be changed at least every 90 days.

For citizens and business users passwords must be at least eight characters long and contain at least one numeric character. Passwords for citizens and business users do not need to be changed; however, use of strong passwords and periodic password changes are recommended.

Passwords are not case sensitive for either government employees and contractors or citizens and business users.

Unsuccessful log on attempts will be limited to five before the account is locked.

User IDs are created for individual use. Users are responsible for their own IDs and how they are used. Passwords must not be shared with anyone.

Users shall not save their password on hard drives, diskettes, or other electronic media. To access systems through NCID, all users shall enter their password each time they log-in.

Credential Management

ITS delegates the authority to establish and validate user IDs for employees and contractors to the agency that requires an NCID account for access to work applications. Agencies are responsible disabling accounts when an employee or contractor credential needs to be disabled or terminated. Agencies also must notify ITS when such action is taken.

The ITS Service Desk is responsible for resetting locked out user IDs upon request and will maintain a log of all requests for resetting locked accounts.

In situations where government employees and contractors are unable to re-authenticate to NCID by failing to remember their passwords or responses to security questions, the ITS Service Desk will refer those individuals to the agency for which they work for re-validation of the account.

Privacy

[2] The following characters are NOT allowed: forward slash (/), backward slash (\), double quote ("), single quote ('), reverse single quote (`), and space.

The data collected and stored in NCID are limited to only that data that are necessary for business purposes. The data and its availability are governed by state and federal legal requirements.

Under the North Carolina Public Records Law, the following data elements are available for public inspection except in limited circumstances: Department, Division, E-mail Address, First Name, Last Name, Office Address, City, State, Zip Code and Title. Credentials (passwords and user IDs) and dates of birth are confidential as are the responses to a user's secret questions. Any disclosure of these data elements is governed by the "Disclosure" section below.

Records that are not available for public inspection include the names of tax payers and those individuals who are participating in the address confidentiality program.

Disclosure

The NCID system is in place to provide authentication and authorization services to agency applications and services. While ITS is the custodian of all user IDs in NCID, ITS will not disclose information in NCID that is related to agency information, such as application access by an NCID user, without the formal approval of the agency custodian, that is, the head of the agency, or the custodian's designee.

When a request for NCID information is received, ITS shall consult with agencies if specific agency information is included in the request. The agency shall determine whether to allow access to the records and/or systems. ITS will not release agency information to any source other than authorized agency personnel.

Archival

ITS provides the infrastructure for NCID.

ITS is responsible for records management, including access, distribution, classification, disposition and retention of NCID records, as required by the North Carolina Public Records Law and other applicable state and Federal statutes and regulations. ITS stores and removes records on NCID in keeping with the General Schedule for State Agency Records. ITS does not remove records government employee and contractor IDs from NCID without prior approval of the agency.

ITS, however, will disable employee and contractor accounts that have been inactive for twelve (12) months and will disable private citizen and business accounts that have been inactive for at least eighteen (18) months. ITS will archive private citizen and business accounts after twenty-four (24) months of inactivity.

Backup and Restoration

As part of the NCID infrastructure, ITS performs regular backups and provides business recovery capability.

Disaster Recovery/Business Recovery Planning

ITS provides backup, restoration, and disaster recovery services for NCID and directory information of users.

ITS provides backup fail-over servers to handle user accounts and authentication and authorization data in the event of a non-recoverable failure to a server.

Enforcement

ITS takes security measures to protect the reliability, availability and integrity of NCID. To accomplish this function, ITS uses appropriate measures to detect security breaches and other violations of system integrity. ITS reviews the security of all network activity, to ensure that use does not violate federal and state laws, and this policy. By using NCID, individual users agree to be subject to and abide by policies governing use. A violation of this policy may result in immediate suspension of NCID to the agency application and/or individual users.

If a validated security incident occurs, ITS will notify the agencies affected within 24 hours of confirmation.

Deviations

All deviations to this policy must be approved by the State CIO.

LAWS RELATING TO AUTHENTICATION AND AUTHORIZATION SERVICE[3]

Federal:

United States Code, Title 18, Section 1030. "Fraud and related activity in connection with computers"

North Carolina:

N.C.G.S. § 14-454. "Accessing computers."
N.C.G.S. § 14-454.1. "Accessing government computers"
N.C.G.S. § 14-455. "Damaging computers, computer systems, computer networks, and resources."
N.C.G.S. § 14-456.1. "Denial of government computer services to an authorized user"
N.C.G.S. § 14-458. "Computer trespass; penalty."
N.C.G.S. §114-15.1. "Misuse of state property."
N.C.G.S. §126-1, et seq. "State Personnel System"
N.C.G.S. §132-1, et seq. "North Carolina Public Records Law"

[3] This is not an exhaustive list of applicable statutes.

N.C.G.S. §132-1.10. "Social security numbers and other personal identifying information"

STATEWIDE SECURITY STANDARDS RELATING TO AUTHENTICATION AND AUTHORIZATION SERVICE[4]

020112	Controlling Remote User Access
060105	Defending Against Opportunistic Cyber Crime Attacks
030103	Accessing Your Network Remotely

Approved by State CIO: October 17, 2007
Effective Date: October 23, 2007

[4] Agencies are required to comply with all security standards established by the State Chief Information Officer. The standards are found at http://www.scio.state.nc.us/sitPolicies.asp