UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Vice Chancellor for Information Technology

Responsible Office
Information Technology Services

POLICY ON FACULTY, STAFF AND AFFILIATE TERMS OF USE FOR UNC-CHAPEL HILL ADMINISTRATIVE SYSTEMS

Policy Statement

UNC-Chapel Hill (the "University") requires its faculty, staff and affiliates to access and use its ConnectCarolina System, InfoPorte System, and associated reporting tools ("Administrative Systems") in a responsible manner and for legitimate business purposes only.

Audience

The audience for this Policy is faculty, staff and authorized affiliates who are users of the University's Administrative Systems. The Policy excludes faculty, staff or affiliate use of the "self-service" components of the ConnectCarolina System in order to access information or transact business regarding themselves (e.g., employee paystub access, student registration, viewing/modifying personal UNC Directory entry, etc.).

Policy Details

In accordance with the Institutional Data Governance Policy, all users who access institutional data in performance of their assigned duties, including reading, entering, downloading, copying, querying, or updating data or information must adhere to the following tenets:

Confidentiality: Respecting the confidentiality and privacy rights of individuals whose records they may access.

Ethics: Observing the ethical restrictions that apply to data to which they have access.

Policy Adherence: Abiding by applicable laws and University policies with respect to access, use, protection, proper disposal, and disclosure of data.

Responsible Access: Accessing and using institutional data only as required in their conduct of University business. Reporting any breaches of University Information in a timely manner according to procedures defined in the Incident Management Policy.

Specifically, for Administrative Systems, the following requirements apply:

Information access and sharing

Users are granted access to Administrative Systems based on their individual job responsibilities and University business need, and this access must be approved by the appropriate Major Organizational Unit or School/Division authority.

Users will only access information in Administrative Systems that that they are authorized to use, and which is specifically necessary to perform their assigned duties, even if the system

does not explicitly prevent it. Likewise, users will neither share their access to Administrative Systems, nor information retrieved from these systems, with others who do not have authority to view this information. Sharing information retrieved from Administrative Systems is only authorized when the receiver has both the appropriate access authorization and a demonstrated business need for the information. This includes sharing passwords or allowing an individual to use Administrative Systems while signed on as someone else.

Information accessed with appropriate authorization from an Administrative System may only be downloaded for authorized business use, and the downloader must have the appropriate authorization for use. Care must be taken to appropriately secure downloaded information, to include any printed or written information.

Confidentiality

Federal and state laws require the University to protect records and information contained within the University's Administrative Systems. Administrative Systems users are also required to comply with the provisions of the University's policies at all times in their use of these systems including but not limited to confidentiality of personnel information and student records.

Sharing or distribution of information contained within Administrative Systems is forbidden other than for University business purposes by authorized individuals for appropriate and authorized purposes. Users sharing such information must ensure that they adhere to all applicable requirements for securing the information in transit, and for communicating the information only to authorized recipients who need the information for University business purposes.

Information Security

When not connected directly to the University network, users must only access Administrative Systems using the University's virtual private network (VPN) functionality. Using remote access to connect to a machine that is connected to Administrative Systems without connecting first to the University's approved VPN is prohibited. The only exception is when a user is accessing his/her own information through "self-service" functions in ConnectCarolina.

Users must not access Administrative Systems in a location that might permit University data to be compromised or viewed by unauthorized individuals. Specific care and sound judgment must be exercised at all times in using devices to access Administrative Systems in public locations.

Users must not access Administrative Systems on any unsecure wireless ("Wi-Fi") network. Users may only use secure wireless networks that require authentication to the network by a password. The University provides a secure wireless network that is acceptable for connecting to Administrative Systems.

Violations

Users are required to report any known or suspected violations of this policy immediately to the Information Technology Services (ITS) Information Security Office by calling the UNC ITS Helpdesk (919-962-HELP).

All use of Administrative Systems is subject to random audit at any time by ITS or the responsible University office to confirm that any individual use is in accord with this and other University policies. Users are expected to cooperate fully with any such audit as a condition of use of the Administrative Systems.

Public Information

Official public information requests for University information stored in Administrative Systems must be referred to and handled by the Office of University Counsel or the relevant University central office. Individual users outside of these offices are not permitted on their own to extract and provide information from Administrative Systems in response to public information requests, unless specifically directed to do so by one of these offices in writing.

For more information about public information requests, refer to the University's Public Records Policy.

Acknowledgement

Every Administrative System user is required to read this Policy. ITS requires users to acknowledge receipt of this policy, either by written signature or by electronic signature. All users must attest in writing that they have read and understood this policy before receiving access to Administrative Systems.

Compliance

Failure to adhere to this policy may have disciplinary consequences for employees, up to and including termination of employment. Students who fail to adhere to this policy may be referred to the UNC-Chapel Hill Office of Student Conduct. Contractors and vendors who fail to adhere to this policy may face termination of their business relationships with UNC-Chapel Hill.

Violation of this policy may also carry the risk of civil or criminal penalties.

Roles and Responsibilities

Information Technology Services: receives reports of potential policy violations; conducts audits of system use; maintains records of user receipt of this policy

Major Organizational Unit/School/Division Authority: approves access for designated users

Office of University Counsel: receives referrals of public information requests

University central offices: receives reports of potential policy violations; conducts audits of system use; responds to public information requests

User: accesses information in accordance with this policy and as needed to perform their job responsibilities

Definitions

ConnectCarolina System: the integrated administrative portal for University business processes related to student services, human resources, payroll and finance.

InfoPorte System: InfoPorte provides a consolidated view of financial information from various enterprise University systems. The purpose of InfoPorte is to allow a variety of users a simplified way to access the information they need to perform their job functions on a day-to-day basis.

University central office: an administrative office of the University whose information is accessible through ConnectCarolina (e.g., Office of Human Resources, Finance Division, Office of the University Registrar, etc.).

User: any faculty, staff or other affiliate granted access to the ConnectCarolina system.

Virtual Private Network (VPN): Virtual Private Network (VPN): A virtual network, built on top of existing physical networks, which provides a secure communications tunnel for data and other information transmitted between networks.

Wi-Fi: technology allowing wireless access to a private or public network.

Related Documents

Privacy Policy

Information Security Policy

Incident Management Policy

Password Policy for General Users

Policy on the Transmission of Personal Health Information and Personally Identifying Information

Policies and Procedures Under the Family Educational Rights and Privacy Act of 1974

Access to Student Records

Personnel Records and Confidentiality of Personnel Information

Public Records Policy

Transmission of Protected Health Information and Personal Identifying Information Policy

Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 C.F.R. § 99.1 *et seq.*

North Carolina Identity Theft Protection Act of 2005, N.C. G.S. § 75-60 *et seq.*

Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.*; 16 C.F.R. § 313.1 *et. seq.* (privacy), 16 C.F.R § 314.1 *et seq.* (safeguarding)

Red Flags Rule, based on Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. § 1601 *et seq.* and 15 U.S.C. § 1681 *et seq.*

North Carolina Public Records Act, N.C.G.S. Chapter 132

North Carolina State Personnel Act, N.C.G.S. Chapter 126

Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d *et seq.*; 45 C.F.R. § 160 *et seq.* (general administrative requirements), 45 C.F.R. § 162 (administrative requirements), 45 C.F.R. § 164 *et seq.* (security and privacy)

Contacts

Subject	Contact	Telephone	Email
Technical questions	ITS Help Desk	919-962-HELP (4357)	
Reporting an information security incident or violation	ITS HELP Desk (Ask that your Remedy ticket be marked “critical” for the Information Security Office (ISO) and do not provide detail on the incident until called back by an ISO incident handler)	919-962-HELP (4357)	

Use of Administrative System Human Resources data	Senior Director, Human Resources Information Management, Office of Human Resources	919-843-2300	hr@unc.edu
Use of Administrative System Finance data	Director, Finance Business Analysis, Finance Division	919-962-7242	avcfinance@unc.edu
Use of Administrative System student data	University Registrar	919-962-3594	registrationservices@unc.edu
Public Information requests	Refer to the University's Public Records policy		publicrecords@unc.edu

Document History

- Effective Date: 10/1/2014
- Last Revised Date: 03/25/2015