INFORMATION SYSTEMS

In November 2011, The University of North Carolina Information Technology Security Council [ITSC] recommended the adoption of ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management [ISO 27002] as the common security framework baseline to be used by the campuses of the University of North Carolina system to develop their individual institutional information technology security policies. The referenced implementation standards are the NC IT Security Manual, the Control Objectives for Information and related Technology (COBIT), and the National Institute of Standards and Technology (NIST). These standards are recognized nationally and within NC by the NC Office of State Auditors and the NC Office of the CIO.

At UNC Charlotte, these standards apply to all software and hardware systems. ITS is accountable for meeting the established standards for software and hardware under ITS control. Departments, colleges and divisions that independently manage software and hardware outside ITS control are accountable to meet the same standards as ITS.

Information Security Liaisons (ISL) have been designated in units throughout the campus and act as an intermediary between their respective unit and ITS, assisting with implementation of information security policy, standards and guidelines.

Applicable external policies or procedures:

- ISO/IEC 27002 Information Technology - Security Techniques

University policies or procedures:

- University Policy 302: Web Communications
- University Policy 304: Electronic Communication Systems
- University Policy 311: Information Security and all supplemental standards, and guidelines
- University Policy 315: Copyright Policy
- University Policy 317: Mobile Communication Devices
- University Policy 601.14: Proprietary Software

Information Security Checklist for Service Owners and System Administrators

The following questions should be used as a starting point to review information security related to the systems and services owned by each unit and/or college. These topic areas are supported by the Standards and Guidelines associated with University Policy 311 Information Security. For a complete list of associated resources, see the IS Checklist located at http://itservices.uncc.edu/home/it-policies-standards/ISChecklist.

Access Control

☐	If not using the centrally managed authentication system, are you following a formal user password management protocol and adhering to the standards for password management?
☐	Are you ensuring that special accounts with elevated privileges (e.g., root, super user, system admin) adhere to the same rigorous password standards plus the additional security measure of regular and frequent audits?
☐	Do you have a formal process for the authorization of user access?
☐	Is access granted to sensitive systems or data based on a need-to-know basis?
☐	Is access to systems terminated when an employee leaves or moves to another department?
☐	Are the access rights of all student workers and/or third party users removed upon termination of employment, contract or agreement?
☐	Do you have a formal process for reviewing user access rights at regular intervals?
☐	Are you requiring unique user IDs?
☐	If the business need requires the use of shared user IDs, is there a process in place and followed to change the password frequently and at a minimum whenever a member of the group leaves or changes jobs?
☐	Have you removed or disabled unnecessary vendor-supplied default accounts?
☐	For required vendor accounts, have you changed the default password following the installation of systems or software?

Communications Security

☐	Before placing a system on the university network, do you ensure that it has been registered with ITS and has adequate security protocols installed and maintained to prohibit unauthorized access?
☐	Before allowing an outside vendor or other third party to connect a system to the university network, do you obtain prior review and approval from ITS?
☐	When transferring sensitive university information, have you ensured that agreements are in place between the university and the external party to appropriately protect the data?
☐	Before transferring sensitive university information, do you check the restrictions on how the data is to be handled which may be governed by: the guideline for data handling, a Data Security Plan, constraints placed by the Data Owner or the Data Security Officer, legal, regulatory or contractual restrictions, and/or export control regulations?

Data Management

☐	Have you identified the data classification level for information stored or transmitted to/from the system or application using the data classification standard?
☐	Have you ensured that the data is being handled appropriately according to its classification as outlined in the guideline for data handling?
☐	Have you obtained review and approval from the University CIO prior to securing a contract with a cloud service provider?
☐	When considering the transfer or surplus of hardware and/or media, have you ensured that data has been properly removed by destroying, purging, or clearing based on the guideline for hardware and media disposal?

Operations Security

☐	Have you implemented and do you follow a formal change management process?
☐	Have you implemented capacity management planning?
☐	Do you keep production, test, and development environments separate?
☐	Have you implemented controls to detect, prevent, and recover from malware?
☐	Have you ensured that backup copies of information, software, and system images are created and do you test them periodically?
☐	Do you maintain event logs and review them as appropriate?
☐	Do you maintain logs of privileged account holders' activity and review as appropriate?
☐	Do you review the vulnerability management scans for your system or application and determine the appropriate measures needed to address the related risks?

Physical and Environmental Security

☐	Are all servers kept in a secure area using appropriate entry controls to ensure only authorized personnel are allowed access?
☐	Do you periodically review the access lists and remove access for those individuals who no longer need it?

System Acquisition, Development, and Maintenance

☐	If using production data containing sensitive or confidential information for testing purposes, have you applied equivalent access controls and other securities to the test system as exist in the production environment?
☐	When considering the development of a new system or an enhancement to an existing information system, are you considering the information security requirements and discussing with ITS as appropriate?
☐	When considering the acquisition of a new system, are you carefully reviewing the security requirements and data protection language in the contract and discussing with ITS prior to purchase?
☐	When considering the acquisition of an application that involves credit/debit card payment transactions, have you included the University Controller's eCommerce Office for assurance of compliance with PCI-DSS and the university's Payment (Credit/Debit) Card Processing Standard?

Vendors and External Parties

☐	When providing vendors and other external parties with the ability to access university information, do you document each party's rules for acceptable use and responsibility for implementing and managing access control?
☐	Do you obtain the vendor's or external party's documented commitment to employ industry best practices for the protection of sensitive university information?
☐	Have you stipulated the details for handling data upon termination of the contract or agreement?

End User Checklist for Information Security

Every member of the university community handling information resources is responsible for ensuring the protection of that information. The following checklist acts as a guide to assist individuals in safeguarding these resources in an appropriate manner. More detailed information may be found in the Standards and Guidelines associated with University Policy 311 Information Security.

Passwords and Access

☐	I treat my password as confidential information and do not divulge it to anyone.
☐	I do not use my UNC Charlotte password for any non-University accounts or systems.
☐	I do not use the "Remember Password" feature in applications or browsers.
☐	I do not store my password information in a file unless I've secured it by applying a strong password on the file.
☐	I protect confidential and sensitive information located in my work area and at my workstation.
☐	I lock my computer screen or log off if I am going to be away from my workstation for any period of time.

Sharing Files and Documents

☐	When sharing files with others within the university, I limit access to those individuals who have a need to know and are authorized to view the data.
☐	I do not access, copy or transmit information that belongs to another end user without obtaining his/her authorization.
☐	When transferring sensitive university information to an external entity, I make sure that agreements are in place between the university and the external entity to appropriately protect the data.
☐	Before transferring sensitive university information, I check the restrictions on how the data is to be handled which may be governed by: the Guideline for Data Handling, a Data Security Plan, constraints placed by the Data Owner or the Data Security Officer, export control regulations, or legal, regulatory or contractual restrictions.

Handling Data

☐	I understand the four levels of data classification: Level 0 = public, Level 1 = Internal, Level 2 = Confidential/Sensitive, Level 3 = Highly Restricted.
☐	I have reviewed the Guideline for Data Handling and understand where data may be stored based on its classification level.
☐	I do not store confidential or sensitive university information on non-University cloud services.
☐	I understand that applying a password to a file that contains sensitive information adds an additional level of security.
☐	When sharing a password-protected file with an authorized end user or authorized external entity, I understand that the password should be sent separately.
☐	I delete files in the Downloads folder and empty the Recycle Bin frequently to ensure that sensitive/confidential information is not stored in these locations.

Mobile Devices, Remote Access

☐	If using a mobile device to access university resources including email, I understand that I am responsible for setting a password, PIN, or swipe pattern on the device.
☐	When using a public WiFi network, I use the University's secure VPN service to connect to university information resources.
☐	When planning to travel to other countries with a laptop or other mobile device, I contact the Export Control department in the Research and Economic Development Office.
☐	When I elect to use a personally-owned device to access university information resources, I adhere to the policies governing information security and acceptable use as well as the corresponding standards and guidelines.

Security Awareness and Incident Reporting

☐	I have taken the online Security Awareness Training in Moodle.
☐	I have reviewed the Guideline for reporting information security incidents and understand that it is my responsibility to report anything suspicious to ITS.

Copiers, Printers, Fax Machines

☐	I ensure that copiers, printers, and fax machines used to copy, print, or transmit sensitive information are located in a secure area.
☐	When purchasing a copier, printer, or fax machine, I work with ITS or our Information Security Liaison to ensure the device is configured appropriately to secure information transmitted via the device.
☐	I do not use non-university devices to copy, print, or fax non-public university information.

Hardware Disposal, Reassignment or Surplus

☐	When considering the transfer or surplus of hardware and/or media, I work with our Information Security Liaison to ensure that data has been properly removed by destroying, purging, or clearing it based on the Guideline for hardware and media disposal.
☐	I ensure that data is erased from equipment that is reassigned within the department.

End User Checklist for Information Security

Every member of the university community handling information resources is responsible for ensuring the protection of that information. The following checklist acts as a guide to assist individuals in safeguarding these resources in an appropriate manner. More detailed information may be found in the Standards and Guidelines associated with University Policy 311 Information Security.

Passwords and Access

☐	I treat my password as confidential information and do not divulge it to anyone.
☐	I do not use my UNC Charlotte password for any non-University accounts or systems.
☐	I do not use the "Remember Password" feature in applications or browsers.
☐	I do not store my password information in a file unless I've secured it by applying a strong password on the file.
☐	I protect confidential and sensitive information located in my work area and at my workstation.
☐	I lock my computer screen or log off if I am going to be away from my workstation for any period of time.

Sharing Files and Documents

☐	When sharing files with others within the university, I limit access to those individuals who have a need to know and are authorized to view the data.
☐	I do not access, copy or transmit information that belongs to another end user without obtaining his/her authorization.
☐	When transferring sensitive university information to an external entity, I make sure that agreements are in place between the university and the external entity to appropriately protect the data.
☐	Before transferring sensitive university information, I check the restrictions on how the data is to be handled which may be governed by: the Guideline for Data Handling, a Data Security Plan, constraints placed by the Data Owner or the Data Security Officer, export control regulations, or legal, regulatory or contractual restrictions.

Handling Data

☐	I understand the four levels of data classification: Level 0 = public, Level 1 = Internal, Level 2 = Confidential/Sensitive, Level 3 = Highly Restricted.
☐	I have reviewed the Guideline for Data Handling and understand where data may be stored based on its classification level.
☐	I do not store confidential or sensitive university information on non-University cloud services.
☐	I understand that applying a password to a file that contains sensitive information adds an additional level of security.
☐	When sharing a password-protected file with an authorized end user or authorized external entity, I understand that the password should be sent separately.
☐	I delete files in the Downloads folder and empty the Recycle Bin frequently to ensure that sensitive/confidential information is not stored in these locations.

Mobile Devices, Remote Access

☐	If using a mobile device to access university resources including email, I understand that I am responsible for setting a password, PIN, or swipe pattern on the device.
☐	When using a public WiFi network, I use the University's secure VPN service to connect to university information resources.
☐	When planning to travel to other countries with a laptop or other mobile device, I contact the Export Control department in the Research and Economic Development Office.
☐	When I elect to use a personally-owned device to access university information resources, I adhere to the policies governing information security and acceptable use as well as the corresponding standards and guidelines.

Security Awareness and Incident Reporting

☐	I have taken the online Security Awareness Training in Moodle.
☐	I have reviewed the Guideline for reporting information security incidents and understand that it is my responsibility to report anything suspicious to ITS.

Copiers, Printers, Fax Machines

☐	I ensure that copiers, printers, and fax machines used to copy, print, or transmit sensitive information are located in a secure area.
☐	When purchasing a copier, printer, or fax machine, I work with ITS or our Information Security Liaison to ensure the device is configured appropriately to secure information transmitted via the device.
☐	I do not use non-university devices to copy, print, or fax non-public university information.

Hardware Disposal, Reassignment or Surplus

☐	When considering the transfer or surplus of hardware and/or media, I work with our Information Security Liaison to ensure that data has been properly removed by destroying, purging, or clearing it based on the Guideline for hardware and media disposal.
☐	I ensure that data is erased from equipment that is reassigned within the department.