Employee 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.
☐	I use the university's two-factor authentication solution to add an extra layer of protection to my NinerNET account.

Sharing Files and Documents

☐	If 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.
☐	If transferring sensitive university information to an external entity, I confirm with the appropriate responsible party that agreements are in place between the university and the external entity to properly protect the data.
☐	If transferring sensitive university information, I first 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, 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 university information adds an additional level of security.
☐	If 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 university 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.
☐	I understand that using the university's secure VPN service can add an extra layer of protection when accessing university resources from a remote location.
☐	If planning to travel to other countries with a university-owned laptop or other mobile device, I contact the Export Control department in the Research and Economic Development Office.
☐	If 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.
☐	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 only use copiers, printers, and fax machines that are located in secure areas if I am transmitting sensitive university information.
☐	If 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 university 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

☐	If considering the transfer or surplus of university-owned 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.
☐	If reassigning university equipment within the department, I ensure that data is erased before transferring the equipment.