

## 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

|                          |  |
|--------------------------|--|
| <input type="checkbox"/> | I treat my password as confidential information and do not divulge it to anyone.   |
| <input type="checkbox"/> | I do not use my UNC Charlotte password for any non-University accounts or systems.   |
| <input type="checkbox"/> | I do not use the "Remember Password" feature in applications or browsers.  |
| <input type="checkbox"/> | I do not store my password information in a file unless I've secured it by applying a strong password on the file.   |
| <input type="checkbox"/> | I follow a clean desk practice by ensuring that confidential and sensitive information located in my work area and at my workstation is secure and out of sight when I leave for the day or when I am gone from my work area for an extended period of time. |
| <input type="checkbox"/> | I lock my computer screen or log off if I am going to be away from my workstation for any period of time.  |
| <input type="checkbox"/> | I understand that using the University's <a href="#">two-factor authentication</a> solution adds an extra layer of protection to my NinerNET account.  |

### Sharing Files and Documents

|                          |  |
|--------------------------|--|
| <input type="checkbox"/> | 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.   |
| <input type="checkbox"/> | 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.                                   |
| <input type="checkbox"/> | If transferring sensitive University information, I first check the restrictions on how the data is to be handled which may be governed by the <a href="#">Guideline for Data Handling</a> , a Data Security Plan, or legal, regulatory or contractual restrictions. |

### Handling Data

|                          |  |
|--------------------------|--|
| <input type="checkbox"/> | I understand the four levels of data classification: Level 0 = public, Level 1 = Internal, Level 2 = Confidential/Sensitive, Level 3 = Highly Restricted.                  |
| <input type="checkbox"/> | I have reviewed the <a href="#">Guideline for Data Handling</a> and understand where data may be stored based on its classification level.                                 |
| <input type="checkbox"/> | I do not store confidential or sensitive University information on non-University cloud services.  |
| <input type="checkbox"/> | I understand that applying a password to a file that contains sensitive University information adds an additional level of security.                                       |
| <input type="checkbox"/> | If sharing a password-protected file with an authorized end user or authorized external entity, I understand that the password should be sent separately.                  |
| <input type="checkbox"/> | 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

|                          |   |
|--------------------------|---|
| <input type="checkbox"/> | 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.  |
| <input type="checkbox"/> | 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.  |
| <input type="checkbox"/> | 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.                                  |
| <input type="checkbox"/> | 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

|                          |  |
|--------------------------|--|
| <input type="checkbox"/> | I have taken the online <a href="#">Security Awareness Training</a> .  |
| <input type="checkbox"/> | I have reviewed the <a href="#">Guideline for reporting information security incidents</a> and understand that it is my responsibility to report anything suspicious to OneIT. |

## Copiers, Printers, Fax Machines

|                          |  |
|--------------------------|--|
| <input type="checkbox"/> | I only use copiers, printers, and fax machines that are located in secure areas if I am transmitting sensitive University information.   |
| <input type="checkbox"/> | If purchasing a copier, printer, or fax machine, I work with OneIT or our <a href="#">Information Security Liaison</a> to ensure the device is configured appropriately to secure University information transmitted via the device. |
| <input type="checkbox"/> | I do not use non-University devices to copy, print, or fax non-public University information.  |

## Hardware Disposal, Reassignment or Surplus

|                          |  |
|--------------------------|--|
| <input type="checkbox"/> | If considering the transfer or surplus of University-owned hardware and/or media, I work with our <a href="#">Information Security Liaison</a> to ensure that data has been properly removed by destroying, purging, or clearing it based on the <a href="#">Guideline for hardware and media disposal</a> . |
| <input type="checkbox"/> | If reassigning University equipment within the department, I ensure that data is erased before transferring the equipment.   |