Teleworking is an option that must be approved by Human Resources. Employees who have an approved Teleworking Agreement on file with HR must adhere to KSC IT Security Standards for Teleworking and submit this signed agreement, along with a copy of the New Appointment Confirmation from HR to the IT Security Manager.

**KSC IT Security Standards for Teleworking**

Please read the following procedures to ensure you understand the Keene State College’s IT Security Standards, then sign to indicate that you have read, understand and will adhere to these standards.

1. I will follow good information security practices as described at [http://www.keene.edu/office/itg/stay-secure](http://www.keene.edu/office/itg/stay-secure).
2. I will only use KSC-issued equipment (i.e. KSC laptops).
3. It is my responsibility to ensure that the equipment I use for teleworking meets all KSC IT security requirements to include:
   a) Enable all security features on equipment (i.e. passwords, screen locks, remote wipe).
   b) Enable all automatic critical/security operating system and application security updates
   c) Run an approved Antivirus/antimalware product and enable automatic updates
   d) Enable the host firewall
   e) Ensure KSC configured security options are not modified, (i.e. auto lock after 15 minutes inactivity)

4. If I am unable to accomplish these KSC IT security requirements independently, KSC IT Group can assist me. (Visit [http://www.keene.edu/office/itg/stay-secure](http://www.keene.edu/office/itg/stay-secure) call 603 358 2532)
5. I will not share KSC-issued equipment (i.e. with other family members).
6. I will protect equipment from theft when not in use.
7. I will protect all printed material from unauthorized access.
8. I will log into the KSC VPN prior to remotely accessing any KSC resources.
9. I will store all KSC information on KSC servers whenever possible. If not possible, temporary storage of non-restricted data on password protected and encrypted mobile devices (i.e. laptop, jump drive) are permissible with prior supervisor approval. Storage of restricted data on computers, external media and mobile devices must be approved in advance by IT Security to ensure appropriate protections will be implemented.
10. I will not use public machines to log into access KSC resources that contain restricted information (i.e. Colleague) or public networks, and will not use passwords used for restricted environments on public machines or for other purposes.
11. I will review the KSC Computer and Network User Policy [http://www.keene.edu/administration/policy/detail/cnup](http://www.keene.edu/administration/policy/detail/cnup) and other appropriate departmental policies depending on my work assignment.
13. I will annually review the KSC Computer and Network User Policy [http://www.keene.edu/administration/policy/detail/cnup/](http://www.keene.edu/administration/policy/detail/cnup/) and other appropriate KSC policies at least annually.
14. HelpDesk and I will verify my equipment’s configuration is secure to current KSC IT standards at least annually.

__________________________
<table>
<thead>
<tr>
<th>Employee Signature</th>
<th>Date Click here to enter a date.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department Click here to enter text.</td>
<td></td>
</tr>
<tr>
<td>Supervisor Name (PRINT) Click here to enter text.</td>
<td></td>
</tr>
</tbody>
</table>

(PLEASE PRINT DOCUMENT, SIGN AND SEND VIA EMAIL TO securitymanager@keene.edu AND ATTACH THE EMPLOYEE’S NEW APPOINTMENT CONFIRMATION FROM HR/PAYROLL)