Data Protection Checklist

If you are purchasing software, services, or IT/medical/scientific products, you must complete this form.

Instructions: Determine if your request involves sensitive information, complete the appropriate section below, obtain signatures, and attach this form, along with any required approvals, to your purchase requisition.

No Sensitive Information

☐ The product/service will not receive, store, transmit, or have access to sensitive information, including FERPA. No approvals are required, proceed to the Signatures section.

Sensitive Information Checklist

☐ The product/service will receive, store, transmit, or have access to sensitive information. Complete this checklist to determine which approvals you must obtain.

Core Requirements - for all types of sensitive information

All requests that involve sensitive information have two core requirements that you must complete.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Contact</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Risk Assessment</td>
<td>Information Security Office, <a href="mailto:security@unc.edu">security@unc.edu</a></td>
<td></td>
</tr>
<tr>
<td>2. Data Steward Approval</td>
<td>View the list of Data Stewards at safecomputing.unc.edu; must receive approval from all impacted stewards.</td>
<td></td>
</tr>
</tbody>
</table>

Additional Requirements - for specific types of sensitive information

Some types of sensitive information have additional requirements. If your request involves the types of information below, you must complete the associated requirement(s) in addition to the core requirements. In the first column, enter Y or N to indicate whether each data type is involved in this request.

<table>
<thead>
<tr>
<th>Y/N</th>
<th>Data Type</th>
<th>Requirement</th>
<th>When</th>
<th>Contact</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>SSN (4 or more digits)</td>
<td>University Committee for the Protection of Personal Data (UCPPD) Approval</td>
<td>After data steward approval</td>
<td>Privacy Office, <a href="mailto:privacy@unc.edu">privacy@unc.edu</a>; see UCPPD site for mtg dates</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Credit Card</td>
<td>CERTIFI Committee Approval</td>
<td>As early as possible</td>
<td>CERTIFI committee, <a href="mailto:certifi@unc.edu">certifi@unc.edu</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protected Health Info (PHI)</td>
<td>Business Associate Agreement (BAA) with vendor</td>
<td>Once vendor is selected</td>
<td>Your unit’s Privacy Liaison or Purchasing.*</td>
<td></td>
</tr>
</tbody>
</table>

*If your unit does not have a Privacy Liaison, contact the Privacy Office at privacy@unc.edu.

Digital Accessibility

Digital accessibility is a practice ensuring that content, resources, and technology communicated electronically can be used regardless of ability, disability, or assistive technology. For purchases/renewals over $5,000 and user base greater than 100 people, a Voluntary Product Accessibility Template (VPAT) is required.

☐ A VPAT is required for my purchase/renewal/request

☐ A VPAT is not required for my purchase/renewal/request

Signatures

☐ I attest that I have provided complete and correct information on this form to the best of my knowledge.

Responsible Party Signature ___________________________ Date ___________ School/Dept/Division IT Director Signature ___________________________ Date ___________

Title ___________________________ Title ___________________________

For more info on this form, visit: http://go.unc.edu/DataProtectionChecklist

Version 3.0, Updated 8/24/2020