THE UNIVERSITY *of* NORTH CAROLINA *at* CHAPEL HILL

Responsible Party Name(s): ________________________________

Department: Kenan-Flagler Business School Date______________

Vendor: ________________________Product:_____________________

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 approvals, and attach this form, along with any needed documentation, to your purchase requisition.

No Sensitive (Tier 2 or 3) Information

□ The product/service will not receive, store, transmit, or have access to sensitive information, including FERPA.

Sensitive Information Checklist (skip the next two items if no SI)

□ 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 Tier 2 or 3 information have two core requirements that you must complete.

Requirement	Information	**ServiceNow or other Reference**	Completed Date
1. Risk Assessment	safecomputing.unc.edu		
2. Data Governance Review	datagov.unc.edu		

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.

Y/N	Data Type	Requirement	When	Contact	Completed
	Credit Card	CERTIFI Committee Approval	As early as possible	CERTIFI committee, certifi@unc.edu	
	Protected Health Info (PHI)	Business Associate Agreement (BAA) with vendor	Once vendor is selected	Your unit's Privacy Liaison or Purchasing.*	

*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 from the vendor. (A VPAT is always strongly recommended.)*

☐ I have received and reviewed a VPAT from the vendor ☐ I was not able to obtain a VPAT

*For assistance or training regarding review of VPAT, or if the product/service does not meet all accessibility requirements, contact the Digital Accessibility Office.

Attestations

RESPONSIBLE PARTY: □ I attest that I have provided complete and correct information on this form to the best of my knowledge. I understand that my unit is financially and otherwise responsible if procured products or services do not meet accessibility, security, or other requirements. This may include ceasing use of a product or service if accessibility or security issues cannot be resolved.

IT DIRECTOR: □ I attest that to the best of my knowledge this procurement has all required technical support to ensure security requirements are met, that the responsible party has needed processes for access control, vendor management, and other technical policy requirements in place such that the product or service can operate in compliance with IT and Digital Accessibility policies.

________________________________ ______________________________________

Responsible Party Name and Title School/Dept/Division IT Director name and Title

Information Tiers

Instructions: Please review the website linked below and indicate what Tier of information is involved in your use of the product. Then, complete the rest of the form and attach it (along with any other needed documentation) to your purchase request.

Information Tiers: https://go.unc.edu/InfoTiers

□ Tier 0: Public Information

□ Tier 1: Business Information

□ Tier 2: Confidential Information

□ Tier 3: Restricted Information

* Please contact Kelly Farrell if you unsure of the Tier after reviewing the documentation

University Security Standards

□ As the responsible party, I will ensure that the technology meets and maintains all relevant University security standards.

Responsible Party Name:

Responsible Party Signature: **Date:**

Signature

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

Vendor Name:

Product Name:

Owner, Administrator, or Contact:
(if different than Responsible Party)

Kenan-Flagler Area /
Department /Group:

UNC Information Security Office

August 1, 2023

To: Georgia Allen, Associate Dean Information Technology at Keenan-Flagler School of Business
From: Paul Rivers, AVC and Chief Information Security Officer for UNC Chapel Hill
Re: Clarification of security responsibilities and the Data Protection Checklist

Under the authority delegated to me by the UNC Chapel Hill Chancellor to oversee the UNC security program and sign documents necessary for the management of this program, I am writing to you to clarify the meaning of security responsibility with respect to the Data Protection Checklist.

At UNC Chapel Hill, the cabinet member is **accountable** for the cybersecurity posture within that unit. For Keenan-Flagler, this accountable person is the Dean. The accountable person must set overall unit priorities and allocate resources within the unit to manage the cyber risks of that unit consistent with UNC security policies and standards.

At UNC Chapel Hill, a person is **responsible** for cybersecurity if and only if that person has direct operational control of the technology, inclusive of control of a vendor relationship for a vendor providing a technology service to UNC. Security responsibility may not be separated from control. The meaning of responsibility for cybersecurity is the person who must perform the operational actions required to maintain the UNC security standards, which includes managing the vendor relationship for third party IT services. Every technology and IT service, whether operated at UNC or provided by a third party, must have a UNC faculty or staff member who is responsible in this sense.

The current procurement process at UNC requires a signature on Data Protection Checklist (DPC) from KFSB. When you sign the DPC, there are two cases. In case one, you (or the teams reporting to you) have direct operational control, and thus you are responsible for the security of the technology or IT service. In the second case, you do not have this control, and thus you are not responsible for the operations and hence security of the technology or IT service.

What your signature indicates in this second case is that you have performed a basic triage function on behalf of the Dean to identify cases where a deeper look by your team on behalf of the accountable person (i.e. – the KFSB Dean) may be warranted to ensure UNC standards are maintained. This triage process is a due diligence check; you are not providing a guarantee that the standards are met and maintained, nor are you assuming responsibility for the security of the technology or service in question. Responsibility remains with the individual who has the requisite operational control of the technology or vendor in every case.

Regards,

Paul Rivers

Chief Information Security Officer
UNC Chapel Hill