

**Personal Information Protection Questionnaire/Checklist (PPIQ) for Vendors**

The following information is intended to provide reasonable assurances that Personal Information (PI) that is handled by vendors and providers of services to Salem State University (SSU), for the University to fulfill its mission, is protected from unauthorized access and/or illicit use.

**I - Vendor Contact Information:**

Vendor Name: \_\_\_\_\_

Address One: \_\_\_\_\_

Address Two: \_\_\_\_\_

City/Town: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

Contact Person: \_\_\_\_\_ Title: \_\_\_\_\_

Tel. (Office): \_\_\_\_\_ Tel. (Cell): \_\_\_\_\_ E-mail: \_\_\_\_\_

**II – Services and Data Required**

Services provided to or being proposed to be provided to Salem State University requiring the need for Personal Information (PI): \_\_\_\_\_

What PI is acquired, transmitted, processed and/or otherwise handled via your process/system? (Please attach any additional clarifying information)

- Name  Address  Tel  SSN  Credit/Debit Card  Bank Acct.  Date of Birth  Other Birth Data
- Driver's License #  Motor Vehicle Data  Passport  Visa  Other Demographic  Biometric
- E-mail

Please specify other PI and/or descriptions for above: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**III - PCI Certification**

If your business processes payment card information or you have a relationship with a third party who will be processing such information on behalf of Salem State University, your company must certify that copies of the Payment Card Industry (PCI) Security Standards Council, Self-Assessment Questionnaire(s), Attestation(s) of Compliance relevant to your /both organization(s), have been completed within the last year, are on file and meet all PCI standards.

- Yes  No

**IV – Confirmation of Security Measures to Protect PI**

1.  Do you have a comprehensive, Written Information Security Program (“WISP”) applicable to all records containing personal information?

2.  Does the WISP include administrative, technical, and physical safeguards for protection? Please explain.  
\_\_\_\_\_  
\_\_\_\_\_
3.  Have you designated one or more employees to maintain and supervise WISP implementation and performance?  
\_\_\_\_\_  
\_\_\_\_\_
4.  What procedural measures/internal controls do you have in place to protect PI that is acquired via your system (e.g. restriction of system access, documented policies & procedures, segregation of duties, system security monitoring & reviews)? Attach any additional clarifying information.  
\_\_\_\_\_  
\_\_\_\_\_
5. Has your company or organization ever been cited by any oversight, standards setting organization, regulatory body, or audit for deficiencies with regard to protecting PI?  
 Yes  No If 'Yes' please explain in detail below. Attach any additional detailed explanation.  
\_\_\_\_\_  
\_\_\_\_\_
6. Have you read and understand Commonwealth of Massachusetts Executive Order 504 Regarding the Security and Confidentiality of Personal Information?  
<http://www.mass.gov/governor/legislationexecorder/executiveorder/executive-order-no-504.html>  
 Yes  No Attach any additional detailed explanation?
7. Have you read and understand Commonwealth of Massachusetts data protection regulation 201 CMR 17?  
<http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf>  
 Yes  No Attach any additional detailed explanation?
8. Have you read and understand Commonwealth of Massachusetts General Law 93H Requirements for Security Breach Notifications?  
<http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93h> Notifications?  
 Yes  No Attach any additional detailed explanation?
9. Have you read and understand read Federal Trade Commission Red Flag Rules and established polices consistent with these rules? <http://www.ftc.gov/bcp/edu/microsites/redflagrule/index.shtml>  
 Yes  No Attach any additional detailed explanation?
10. Has your company ever experienced a breach of confidential information? If 'Yes', please explain in detail including the resolution and the current status. Please attach additional sheets if necessary.  
 Yes  No

**Authorized Vendor Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_  
(Signature indicates compliance with statutes, regulation and standards regarding the protection of Personal Information and/or PCI Standards)

**Title:** \_\_\_\_\_