Procedures for Safeguarding Personal Information (PI)
Handled by Third Party Vendors and Providers of Services to Salem State University

The following procedures are intended to provide reasonable assurances that Personal Information (PI) that is provided to 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. Procedures set forth here are intended to comply with:

a) Commonwealth of Massachusetts statutes and regulations regarding the protection of Personal Information (PI).
b) Payment Card Industry Data Security Standards (PCI-DSS) for the protection and confidentiality of electronic payment transaction data.

Personal Information (PI)

1) Per Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation Data Protection *Regulation 201 CMR 17.00* and *Executive Order 504* personal information (PI) is defined as first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident
   a) Social Security number
   b) Driver's license number or state-issued identification card number or,
   c) Financial account number, credit or debit card number
   with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

2) **Prospective vendor/providers** whether in response to an RFP or Sole Source acquisition must complete a ***Personal Information (PI)Protection Questionnaire/Checklist (PIPQ)*** and specifically certify, as is stated in E.O. 504 Sec. 9, not merely by reference to the Standard Contract form, that they have read, understand and are in compliance with laws and regulations pertaining to protecting PI including but not limited to:
   a) Executive Order 504 Regarding the Security and Confidentiality of Personal Information. http://www.mass.gov/governor/legislationeexecorder/executiveorder/executive-order-no-504.html
   b) Data Protection Regulation 201 CMR 17 per the Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf
   c) Security Breach Notifications per Commonwealth of Massachusetts General Law 93H http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93h
   d) Federal Trade Commission 'Red Flag ' Procedures http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml
   e) Other applicable laws and regulation both state and federal
   f) Agree to immediately inform principals of SSU of any Breach or compromise of data security

3) **Existing vendors** who handle, accept, process protected data must submit a ***Personal Information Protection Questionnaire (PIPQ).*** This will be requested annually as part of the confirmation procedures of the independent financial audit. Vendors must certify they have read, understand and are in compliance with laws and regulations pertaining to PI including but not limited to:
   a) Executive Order 504 Regarding the Security and Confidentiality of Personal Information.
   b) Data Protection Regulation 201 CMR 17.00 per the Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation
   c) Security Breach Notifications per Commonwealth of Massachusetts General Law 93H including immediately informing principals of SSU of any Breach or compromise of data security
   d) Federal Trade Commission 'Red Flag ' Procedures

e) Other applicable laws and regulation both state and federal

4) As part of the university's annual Risk Assessment and Internal Control Process, internal departments of the University that handle PI or payment card data will be requested to include in their Risk Assessment documentation mitigation procedures for assuring the protection and security ***of PI***.

Payment Card Industry - Data Security Standards (PCI-DSS)

1) The ***Payment Card Industry (PCI***) has formulated ***Data Security Standards (DSS)*** and tools to assist in the protection of Personal Information (PI) related to payment card data processing to which Salem State University continually endeavors to comply. Per statutes and regulations cited above, credit and debit card account information is a specific form of sensitive PI information that requires protection.

2) Per the PCI Security Standards Council Guidelines, PCI Data Security Standards (DSS) as well as Provider Application Security Standards (PA-DSS) along with their supporting documents represent a common set of security standards and measurements to help assure the safe handling of sensitive information.

3) ***Prospective vendors/providers***, whether in response to an RFP or Sole Source acquisition, who acquire PI related data, must provide certification that an organization wide risk assessment has been conducted in accordance with PCI Data Security Standards (DSS) Risk Assessment Guidelines established by the PCI Security Standards Council, by an independent third party. Risk Levels must meet or exceed compliance standards set by PCI-DSS.

4) ***Prospective vendors/providers***, whether in response to an RFP or Sole Source acquisition who acquire PI related data must provide certification that a PCI–DSS Self-Assessment Questionnaire(s) and Attestation(s) of Compliance are on file indicating their compliance with PCI-DSS industry standards. They must also certify the remediation of any significant risk areas. Risk Levels must meet or exceed compliance standards set by PCI-DSS.

5) ***Existing vendors*** who handle, accept, process protected data will be requested to submit a ***Personal Information (PI) Protection Questionnaire (PIPQ)*** as part of the confirmation procedures of the annual independent financial audit.

6) Information referenced above as well as additional information is attainable from the Payment Card Industry Council web site @ https://www.pcisecuritystandards.org/

Management of Procedures

1) Management of these procedures and the PIPQ will rest with Financial Services and be maintained within the Salem State University web site, Purchasing Department pages @ http://www.salemstate.edu/3471.php