SPIA for Vendors

This document is intended to help guide vendor responses about existing or planned security controls protecting hosted data and/or systems. Responses are used to evaluate existing security posture and whether it meets Penn's current recommendations and guidelines.

1. Briefly summarize the service offering, identifying the location of data being stored, the type of data being stored, transmission details (how frequently, through what mechanisms), and any aspects of the service that use subcontractors or are outsourced. Please specify if any sensitive, confidential, or other protected data is planned to be stored.

2. Do you have a third party security assessment and certification of your information security controls? How recently was the review performed? How regularly are reviews performed? Can you supply a copy?

3. Do you have an established Information Security Program, including an Incident Response process?

   Your response should refer where applicable to the title of the employee in charge of the program, the number of employees in the program, any credentials or special skills, the organizations incident response program, any security policies or procedures.

4. Do you have any certifications for any compliance frameworks such as FISMA, HIPAA, PCI, etc.? If custom application developed, describe any security frameworks (e.g. OWASP) used or formal processes (e.g., SDLC) in place:

5. Please describe controls to address the threat of information being compromised by an external hacker or malicious software.

   Your response should refer where applicable to safeguards such as intrusion detection, anti-virus, firewalls, vulnerability scanning, penetration testing, encryption, authentication and authorization protections and policies, including those involving system hardening, such as passwords, removal of unnecessary network services, limiting of administrative access, code review, logging, employee training and other relevant safeguards.

6. Please describe controls to address the threat of information being intercepted in transit by unauthorized persons.

   Your response should refer where applicable to safeguards such as encryption during transmission, availability and/or encryption of wireless traffic, physically securing devices in transit, network traffic segregation, and other relevant safeguards, and include descriptions of encryption protocols and algorithms used.

7. Please describe controls to address the threat of information being mistakenly disclosed to unauthorized persons.

   Your response should refer where applicable to issues of awareness and training, removal of unnecessary data (electronic and paper), use of screen savers and lockouts, limiting storage of confidential data on remote devices, verification of identity of individuals requesting access, and other relevant safeguards that enforce “need to know”.

8. Please describe controls to address the threat of information knowingly being misused by your workforce and contractors.

   Your responses should refer where applicable to issues of strong sanctions policy and practice, background checks, role-based access to information, oversight of data authorization by supervisor, terminating access to data for terminated employees and employees changing job functions, prohibition on sharing passwords, and other relevant safeguards.

9. Please describe controls to address the threat of physical theft or loss of data.

   Your responses should refer where applicable to policies on the storage of confidential data on laptops, PDAs, USB drives and other portable devices, encryption of data on portable devices, two factor authentication, removal of unnecessary information, physical protection of desktops and servers, and other relevant safeguards.

10. Please describe controls to address community concerns regarding privacy practices.

    Your responses should refer where applicable to privacy statements, opt-in or opt-out consents, compliance with applicable privacy rules, and other relevant safeguards.

11. Please describe controls to address the use, handling, protection and sharing of confidential data shared with subcontractors.

    Your responses should state any relevant relationships that may induce additional risk to the safe storage of sensitive data (such as outsourcing of key services, use of sub-contractors or cloud services for hosting, etc.) and refer where applicable to contractual safeguards and reviews of security programs / practices.

12. Please describe controls to address threats to the availability of data based on inadequate business continuity procedures.

Your responses should refer to business continuity and disaster recovery plans and procedures, regular testing, routine data backups and offsite storage.

