Technology Help Desk
412 624-HELP [4357]
technology.pitt.edu

University of Pittsburgh Security Assessment Questionnaire (v1.5)

Directions and Instructions for completing this assessment

The answers provided must be accurate and representative of the circumstances currently in place. This risk assessment is to be used not only to assess the particulars of the application/system but also the general security infrastructure of your company. This is to meet the University of Pittsburgh security procedures and to ensure that your processes are in conformance with our internal policies, as well as to establish a level of trust with your organizations security infrastructure.

Only the appropriate and knowledgeable personnel responsible for the particular areas and questions should respond to these questions. *Most, if not all, of the questions are likely to be applicable to your organization. If a question is not applicable to your organization please provide the reason why.*

The answers should be descriptive for each question (not just answered with yes or no) and the whole of the response should be included in the space allocated. Supporting documents should not be imbedded in this document but should be provided separately but please refer to an attachment in your answer so that we can document we have received it. Each question should be answered, some cells have multiple questions. Do not refer to different responses when answering each question. (Similar questions may be asking from a different scope or perspective.)

The material requirements and presentations provided via this security assessment review process will be part of and be considered incorporated into related contracts.

If there are questions regarding this form, please contact the University Security Analyst who provided the Questionnaire from the University of Pittsburgh and they will either address the questions or coordinate a response as needed.

Section	Description	Vendor Response
Company Details	a) Identify your company's name and applicable geographic locations. (Corporate Headquarters, Hosting facility locations, etc.) b) Please provide short background on company. (Creation dates, major transitions, any national/global newsworthy events, etc.) c) Provide applicable Web URLs for information regarding your company and services. Provide links to White-papers, FAQs and Privacy Notice.	
Project Details	a) Please provide a description of the services to be provided by this relationship. Include any details in regards to the handling or hosting of University of Pittsburgh data b) Please list all University/customer data that will be collected and stored on the vendor's systems, including personally identifiable information, social security numbers, and financial account numbers.	
Supporting Documentation	Please include the following documentation when submitting this questionnaire to the University of Pittsburgh: a) Security / Architecture diagram b) SSAE 16 SOC 1 or SOC 2 report	
Roles & Responsibilities	a) Has your organization formally appointed a central point of contact for security coordination? b) If so, whom, and what is their position within the organization? c) Are responsibilities clearly documented? i.e. job descriptions, information security policy	
External Parties	a) Do you work with third parties, such as IT service providers, that have access to your sensitive information? (e.g. backup tape storage, maintenance providers, hosting facilities, cleaning staff, etc.) b) Does your organization have Business Associate and / or Non-Disclosure agreements in place with these third parties? c) If not, what controls does your organization have in place to monitor and	

Section	Description	Vendor Response
	assess third parties? (e.g. Logging of VPN connections, Access logs, etc.) d) Would your company share, send, or otherwise provide access to University of Pittsburgh data in any form (personal, anonymous, aggregated) to any parties, including subcontractors or other service providers. Provide relevant details for all such practices	

Section	Description	Vendor Response
Information Security Policy & Procedures	a) Do you have documented information security policies and procedures? b) Do you have a formal information classification procedure? Please describe it. In particular, how would sensitive data be categorized? (e.g. *critical*, *essential*, and *normal.)* c) Have formal acceptable use rules been established for assets? Example assets include data assets, computer equipment, communications equipment, etc. d) Do you have formal processes in place for security policy maintenance and deviation?	
Risk Assessment	Do you have a process that addresses: the identification and measurement of potential risks, mitigating controls (measures taken to reduce risk), and the acceptance or transfer (Insurance policies, warranties for example) of the remaining (residual) risk after mitigation steps have been applied?	
Compliance with Legal Requirements - Identification of applicable legislation	a) Does a process exist to identify new laws and regulations with IT security implications? (e.g., new state breach notification requirements)? b) Please describe status of compliance with any of the following: 1)HIPAA 2)GLBA 3)Sarbanes-Oxley section 404,406 4)FISMA 5) Standards based compliance (ISF, CoBIT, ISO, OCTAVE, FIPS, etc)	

Section	Description	Vendor Response
eCommerce	a) How is credit card data stored, processed, or transmitted? b) Please list your PCI DSS merchant/service level. c) Please provide proof of PCI compliance and results of the most recent quarterly network scan. d) Will a third-party payment gateway used? If yes, please list.	
During Employment – Training, Education & Awareness	a) Have your employees been provided formal information security training? Have policies been communicated to your employees? b) Are periodic security reminders provided (e.g. New employee orientation, annual training, posters in public areas, email reminders, etc.)?	
Background Checks	a) Does your organization perform background checks to examine and assess an employee's or contractor's work and criminal history? b) Are particular sensitive positions subject to periodic follow-up background checks? c) What type of background checks are performed?	
Prior to Employment - Terms and Conditions of Employment	a) Are your employees required to sign a non-disclosure agreement? b) If so, are employees required to sign the non-disclosure agreement annually?	
Termination or Change in Employment	a) Do you have a formal process to manage the termination and or transfer of employees? (e.g. All equipment is returned, user ID's disabled in systems, Windows, badges and/or keys returned.) b) Is existing access reviewed for relevance for transfers?	

Section	Description	Vendor Response
Secure Areas	a) Do you have effective physical access controls (e.g., door locks, badge / electronic key ID and access controls) in place that prevent unauthorized access to facilities? b) Are there plans in place to handle/manage contingent events or circumstances (e.g. what if the person with the key to the server room is sick)? b) Is there a facility security plan? c) How are physical access controls authorized (who is responsible for managing and ensuring that only appropriate persons have keys or codes to the facility and to locations within the facility with secure data)?	
Application and Information Access Control - Sensitive System Isolation	a) Describe your network configuration. b) Are systems and networks that host, process and or transfer sensitive information 'protected' (isolated or separated) from other systems and or networks? c) Are internal and external networks separated by firewalls with access policies and rules? c) Is there a standard approach for protecting network devices to prevent *unauthorized* access/ network related attacks and data-theft?	
Encryption	a) Describe how encryption is used to protect data at rest and data in transit. (Include protocols, algorithms and bit strengths). b) Describe how your private keys are protected and who has access to them.	
Vulnerability Assessment and Remediation	a) How often do you perform periodic vulnerability scans on your information technology systems, networks and supporting security systems? b) Has any in-house written application undergone a source code security review?	

Section	Description	Vendor Response
	c) Are those scans performed internally or by an independent third-party? d) What is the security patch management criteria used to prioritize vulnerability remediation? e) What is the frequency for routine patch deployment?	

Section	Description	Vendor Response
Network Monitoring	a) Are connections to your network monitored and reviewed to confirm only authorized access and appropriate usage? (This includes internal and external connections) b) How long are those logs retained? c) How frequently are the logs reviewed?	
Access Management	a) Do you have a formal access authorization process based on 'least privilege' (employees are granted the least amount of access possible in order to perform their assigned duties) and need to know (access permissions are granted based upon the legitimate business need of the user to access the information) ? b) How are systems and applications configured to restrict access only to authorized individuals? c) Minimum password length? Complexity? History? Lockout? Password change? d) Is there a list maintained of authorized users with access (administrative access) to operating systems? e) Does a list of 'accepted mobile devices' (e.g., smart phones, cell phones) exist based on testing? f) Is sensitive information (customer information, PII, financial data) removed from, or encrypted within, documents and or websites before it is distributed? g) Is software installation restricted for desktops, laptops and servers? h) Is there an automatic logoff of workstations, VPN, servers? g) Is access to source application code restricted? If so, how? Is a list of authorized users maintained?	

Section	Description	Vendor Response
Identity Management	a) Please describe your centralized authentication mechanism for internal and external users? b) Any shared accounts or local accounts used? c) Do you have a process to review user accounts and related access?	
Antivirus	a) Has antivirus software been deployed and installed on your computers and supporting systems (e.g., desktops, servers and gateways)? b) Product installed? Centrally managed? Updated daily? c) Reviewed for being current?	
Network defense and Host intrusion prevention systems.	a) Is any host-based or network –based IPS deployed? b) Any next generation firewall or web application firewall? c) Any web security gateway? d) Do these systems perform dynamic responses to suspicious activity? e) How are these systems updated to adapt to emerging threats?	
Security Monitoring	How are systems and networks monitored for security events?	
Media Handling	a) Do procedures exist to protect documents, computer media (e.g., tapes, disks, CD-ROMs, etc.), from unauthorized disclosure, modification, removal, and destruction? b) Is sensitive data encrypted when stored on laptop, desktop and server hard drives, flash drives, backup tapes, etc.? c) Is data encrypted on the server? Backups? Mobile devices? SD Cards?	

Section	Description	Vendor Response
Secure Disposal	Are there security procedures for the decommissioning (replacement) of IT equipment and IT storage devices which contain or process sensitive information?	
Segregation of Computing Environment	a) Are development, test and production environments separated from operational IT environments to protect production (actively used) applications from inadvertent changes or disruption? b) Is production data used in development environments?	
Segregation of Duties	Are duties separated, where appropriate, to reduce the opportunity for unauthorized modification, unintentional modification or misuse of the organization's IT assets?	
Change Management	Do formal change management procedures exist for networks, systems, desktops, software releases, deployments, and software vulnerability (e.g., Virus or Spyware) patching activities?	
Process & Procedures	a) How do you identify, respond to and mitigate suspected or known security incidents? b) During the investigation of a security incident, is evidence properly collected and maintained using forensic procedures? c) Are incidents identified, investigated, and reported according to applicable legal requirements? c) How are incidents escalated and communicated to customers?	

Section	Description	Vendor Response
Disaster Recovery Plan & Backups	a) Do you have a mechanism to back up critical IT systems and sensitive data? b) Have you had to restore files after a systems outage? c) Does a Disaster Recovery plan exist for the organization and does it consider interruption to, or failure of, critical IT systems? d) Are disaster recovery plans updated at least annually? e) Is source code escrowing in place?	
Software Development Lifecycle	Describe how security best practices are implemented during the lifecycle?	
Federated Identity Management and Web Services Integration	a) Describe your SSO and Federated Identity Enablement integration options (e.g. Support for Standards like SAML v2 and OAuth 2.0) b) Describe your web services and data import / export options.	
Contact Information	a) Whom do we contact if we identify a security issue or breach involving or impacting your product? Please provide an email address and/or full contact information. b) What is their expected SLA to respond to initial contact?	

Section	Description	Vendor Response
Additional Information	Please provide any additional information that may be relevant to the review of the security of your organization.	