Cal Poly Third-Party Vendor Security Questionnaire

Contact for information: Campus Information Security Office Phone: 805-756-5595 email: infosec@calpoly.edu

**Supporting Documentation May be Requested*

	Policies and Procedures	**Answer (Y,N,NA)**	**Clarifying/Supporting Comments**
1	Has the security policy document(s) been published and enforced in your organization?		
2	Are you compliant with the following State, Federal, and Industry Standards? *(If you are not collecting medical information, conducting credit card transactions or collecting personal identifiable information (PII), then please indicate N/A)*		
	Health Insurance Portability Accountability Act (HIPAA)		
	Payment Card Industry Data Security Standards (PCI-DSS)		
	California Security Breach Information Act (SB-1386) - collecting personal Identifiable Information (PII)		
	Educational Records (as defined by FERPA)		
3	Can you provide a recent SSAE16 or other industry recognized audit report?		
4	Do you have policies and procedures covering the following practices?		
	Authorized/acceptable use of Networked Services		
	Access Control Policy (policy for granting, creating or motifying access to employees or contractors)		
	Password Management		
	Software/Hardware Acquisition		
	Change Management		
	Encryption Policy and Standards		
	Security related incidence response/handling		
	Data Handling Policy (to include data use, storage and destruction of sensitive data)		
5	Is there a process for annually reviewing, updating, and revising these policies?		
6	Are the consequences of non-compliance to the policies clearly documented?		
7	Is a senior corporate official directly responsible for the implementation of your organizational security policy?		
8	Is the advice of an information security specialist obtained where appropriate?		
9	Are security roles and responsibilities as defined in the organization's information security policy documented?		
10	Do all employees and third party receive appropriate Information Security training in organizational policies and procedures?		
11	Are procedures in place for users, to report security weakness in, or threat to, systems or services?		

Patch Management

12	Do you apply security patches on a monthly basis or as they are available?		
13	Do you have an automated patch management solution deployed?		
14	Do you have vendor agreements in place for timely availability and application of software updates?		
15	Are all your networking devices at the latest patch level?		
16	Do you have a process to validate your patch management procedures?		

Physical Security

17	What kind of perimeter control(s) is applied to data center location?		
	Token/Cards		
	Key Pad Controls		
	Man Trap		
	Biometric Controls		
	Guards		
18	Are controls in place to allow only authorized personnel into various areas within organization?		
19	Do you monitor/log all access to data center?		
20	Do you monitor the security/policy violations and application/ networked services availability?		
21	Do you employ UPS (Uninterrupted Power Supply), Battery Banks, Generators etc?		
22	Do you employ fire/flood detection and suppression systems?		
23	Do you monitor and escort visitors through critical parts of your company?		
24	Do you maintain visitor logs?		
25	Is access to security logs strictly controlled (Firewall logs, etc)		
26	Is an inventory or register maintained with the important assets and the identified owners?		
27	Is a list of contacts maintained to ensure that appropriate action can be taken and advice obtained, in the event of a security incident?		

Network Infrastructure

28	Do you maintain up-to-date network infrastructure and administration procedures?		
29	Do you limit administrator level access on network and systems infrastructure?		
30	Are all your routers configured with access control lists to allow only specific traffic to pass through?		
31	Do you allow access to your routers via its console port only?		
32	Are all your networking devices at the latest patch level?		
33	Do you ensure default passwords are changed on networking devices?		
34	Do you control the change frequency and distribution of admin access to network infrastructure?		

35	Is equipment identification used to authenticate connections from specific locations and equipment?		
36	Do you employ an intrusion prevention/detection system?		
37	Do you outsource any security management functionality?		
38	Is there is a management authorization process for any new information facility including networks, hardware and software?		
39	Where business partner's and/or third parties need access to information system is the network segregated using perimeter security mechanisms such as firewalls?		

Remote Access

40	Is there an authentication mechanism used to control access by remote users?		

Accounts Management & Access Control

41	Do employees having access to computer systems have an established need for this access?		
42	Is there a formal user registration and de-registration procedure for granting access to all information systems and services?		
43	Is there a formal management process for issuing and resetting passwords?		
44	Is there a process to review user access rights at regular intervals?		

Audit Trail

45	Do you collect/review log information from the following sources?		
	Application logs and services that can potentially identify what transactions have been performed, at what time, by whom, and on what, such as web, database and authentication can provide detailed information about those activities.		
	System logs for operating systems.		
	Network devices, such as firewalls, routers and switches are generally capable of logging information.		
	Change management logs that document changes in the business environment.		

Disaster Recovery and Business Continuity

46	Do you have a written business continuity plan for the systems supporting your key services?		
47	Are disaster recovery exercises conducted?		
48	Do disaster recovery plans include documented test and results?		
49	Are manual backup/restore procedures documented and practiced in case of automatic backup failure?		
50	Can you meet recovery time objective(s) (RTO) and recovery point objective(s) (RPO) for all products and services ?		

I hereby certify that the above statements are true and correct to the best of my knowledge. I understand that a false statement may result in termination of our contarct with Cal Poly.

Questionnaire completed by: _____ Date: _____

Contact Information:

Questionnaire approved by: _____ Date: _____

Title: _____