NYU PCI-DSS Policy Supplement

Appendix D: Roles and Responsibilities

Last Revised: 2018

Process	Task	Responsible office			
		Bursar	FSM	IT-OTSS	OIS
ANNUALLY					
Merchant ID Deactivation	Run revenue reports to identify merchant IDs with no revenue in last 2 fiscal years	X			
	Correspond with merchants to confirm deactivation of merchant IDs	X			
	Provide FSM with list of merchant IDs to deactivate	X			
	Maintained to monitor service providers' PCI DSS compliance status at least annually	X			
Webform Deactivation	Run webform revenue reports to identify webforms with no activity in 3 years	X			
	Correspond with merchants to confirm deactivation of inactive webforms	X			
	Provide FSM with list of webforms to deactivate	X			
Self-Assessment Questionnaire (SAQ)	Help PCI Manager to prepare SAQ		X	X	X
	Compile annual corporate SAQ submission for PCI Manager sign-off	X			
PoS	Media inventory review		X		
Network	Penatration testing				X
PCI DSS Policy	Security policy review	X			
Risk Assessment	Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually	X	X	X	X
Training	Educate and train personnel about PCI cardholder data security policy and procedures	X			
Incident Response	Review and test inident response plan including all elements listed in Requirement 12.10.1	X			X
Website Vulernability Check	Review public-facing web applications via manual or automated application vulnerability security assessment tools or methods at least annually				X
SEMI-ANNUALLY					
Equipment Inspection	Run Bank of America front-end Device Support		X		
	Conduct on-site physical device inspections for selected merchants		X		
Firewall review	Review configuration standard and rule sets of PCI related firewall and routers				X
QUARTERLY					
Vendor Management	Review Attestations of Compliance (AoC) and ensure current AoC's on file complie quarterly PCI Scorecard	X			
Reporting, Documentation, & Merchant Support	Compile quarterly PCI Scorecard	X			
Internal and External network Vunerability Scans	Examine scan reports and supporting documentation to verify that internal and external vulnerability scans are performed				X
	Perform internal vulnerability scans and resolve all high risk vulnerabilities				X
	Perform external vulnerability scans and resolve all high risk vulnerabilities		X		X
User Account Management	Change user passwords/passphrases at least once every 90 days	X	X		X
Network Diagram	Network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks				X
	Diagram that shows all cardholder data flows across systems and networks				X
MONTHLY					
Patch Management	Install critical patch within one month of relase		X		
WEEKLY					
File Intergrity Monitoring	Configure change-detection mechanism to alert personnel to unauthorized modification of critical system files, configuration files or content files, and do the tools perform critical file comparisons at least weekly				X
DAILY					
Log Review	Reviewing the PCI related security log at least daily, either manually or via log tools:				X
ON-GOING TASKS					
Equipment Requests	Coordinate with IT to ensure computers used to initiate credit card transactions are regularly updated for anti-virus and malware definitions		X		
Self-Assessment Questionnaire (SAQ)	Monitor and ensure merchants submit SAQs	X			
	Assist merchants as needed to complete SAQ	X			
Security Awareness Education (SAE)	Correspond with merchants to maintain current SAE enrollments	X			
	Enroll/de-enroll in Trustwave as needed	X			
	Send periodic email reminders on SAE completion	X			

	Distribute reports (quarterly, at minimum) to Merchant Managers on SAE completion status	X			
Reporting,Documentation & Merchant Support	Maintain Master Merchant Detail File and documentation	X			
	Respond to ServiceLink PCI inquiries	X	X		
Website Vulurnability	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis				X
Device List	Documented inventory of PCI System component		X		X
AS NEEDED TASKS					
Merchant Onboarding	Register merchant for SAQ	X			
	Register merchant for SAE	X	X		
	Set-up merchant in eCommerce Portal		X		
Equpment Requests	Support PCI Manager to review requests for equipment not on NYU approved device list		X		
	Support PCI Manager in migrating merchants to more secure devices (ie. EMV pin-chip)		X		
	Address questions related to middleware		X		
Vendor Management	Support PCI Manager in evaluating PCI compliance implications for new vendor requests		X		
Reporting, Documentation &Merchant Support	Compile Merchant Card Processing Snapshots (summary reports)		X		
	Participate as needed in PCI-Related meetings	X	X	X	X
Enhancement of eCommerce portal	Modification and enhancement of eCommerce portal as required			X	
Risk Assessment	Review risk-assessment documentation to verify that the risk-assessment process is performed upon significant changes to the environment	X	X	X	X
Training	Educate and train personnel about PCI cardholder data security policy and procedures upon hire	X	X	X	
Network Vulnerability Scan	Internal and external vulnerability scans and rescans after significant change				X

Legend:

Symbol	Office	email
BURSAR	Office of the University Bursar	pci.compliance@nyu.edu
FSM	Financial System Management	ecommerce.help@nyu.edu or askfinancelink@nyu.edu
IT- OTSS	Information Technology - Operations Technology and Support Services	its-ecoms-bpa-group@nyu.edu or it-bpa-group@nyu.edu
OIS	Office of Information Security	security@nyu.edu