PCI Roles – Segregation of Duties

The roles and responsibilities outlined within this document will be reviewed at least annually or sooner if significant changes take place within PCI compliance, new departments joining the PCI environment or staffing changes in regards to anyone performing duties related to PCI.

**PCI Administrative Roles**
The following roles specific to PCI have been defined for the purpose of this document in order to make clear a segregation of duties between groups in order to be compliant with PCI. All administrative roles are responsible for reviewing scan reports, addressing vulnerabilities, and reporting medium/high risk vulnerabilities to the appropriate support area.

**PCI Compliance Officer** (Primary: Bob Wagner, Secondary: TBD) – Responsible for scheduling internal and external scans and PEN testing and routing them to appropriate administrator if non-compliant.

**Information Security** (Primary: Mike Grypp, Secondary: Shane Stimac) – Responsible for performing the annual risk assessment.

**Network Administration** (Primary: Peter Hachmeister, Secondary: Matt Baran) – The network administrators are responsible for all network devices that are PCI in-scope. This is limited to the Firewall/Router in the EMS DC as well as the two end of row switches in the EMS DC. The Network administrators will create and set the firewall rules as well as make changes to logical networks and the IDS/IDP as necessary. All actions will be logged to the central logging server. Network Administrators do not have admin access to the logging environment. Analyzes, designs, and implements network infrastructure to support the PCI environment. Including (but not limited to) firewalls, switches, routers, VLAN design, DMZs, and IDS/IDP.

**Infrastructure Administrator** (Primary: Ben Seefeldt, Secondary: Steve Penn) – Physical hardware, manages VM environment, VPN hardware, storage hardware and network design and configuration in consultation with UITS Network Operations. Manages storage arrays and physical servers.

**Server OS Administrator** (Primary: Alex Hardy, Secondary: Christopher Cook) – Handle the installation and updating of the server operating system and file integrity monitoring software. Manage SCCM.

**AD Environment Administrator** (Primary: Christopher Cook, Secondary: Alex Hardy) – Handle the administration and operation of the PCI AD environment. These administrators will set up and administer all access accounts to the PCI environment.

**Application Administration** - The application administrators are responsible for managing the server software and the registers. OS level patching and updates are the responsibility of the Server OS Administrator but the Application administrators need to work with them to schedule and define the update process.

All server and application logs are to be sent to the central logging server. Application administrators cannot be administrators in the logging server environment.
Micros Server Admin and Cash Register Hardware – (Primary Craig Heser, Secondary: Kurt Witzlsteiner)
MBS Server Admin – (Primary: Craig Heser Secondary: Paul Gunderson)
Coldfusion & IIS Application Support – (Primary: Titus Curtain Secondary: Chris Rizio)

Application Developers/Reviewers – (Ricky Kaja, Tamara Edmond and Mike Duschak) – makes changes to the ePayment code base. Perform code reviews of any changes made to the ePayment code base. NOTE – the individuals who developed the code change cannot perform the review of the code change.

ePayment Release Administrators – (Primary: Titus Curtain Secondary: Chris Rizio) – Move the current ePayment release into the production environment.

Change Requester – Submits change requests to the PCI-CAB. Following is a list of individuals who can submit requests and the type of request they can submit.

  - OS Patches – Alex Hardy, Ben Seefeldt, Craig Heser, Christopher Cook, and Steve Penn.
  - ePayment Code Changes – Mark Jacobson, Ricky Kaja, Tamara Edmond, and Mike Duschak
  - Network Changes – Ben Seefeldt, Mark Jacobson, Ricky Kaja, Peter Hachmeister, Steve Penn, and Matt Baran.
  - Coldfusion & IIS Application Patches – Titus Curtain and Chris Rizio
  - Infrastructure – Ben Seefeldt and Steve Penn

PCI-Change Advisory Board-PCI (PCI-CAB) – (Ben Seefeldt, Craig Heser, Ryan McNallie, Christopher Cook, Bob Meyer, Mark Jacobson, and Matt Preston) - Review and approve changes before they are moved into production. Two different individuals must approve every change before it is moved into production. NOTE: Members of the PCI-CAB cannot approve a change which they developed or requested.

Backup Server Administration (Primary: Ben Seefeldt, Secondary: Steve Penn) – Runs backups specific to the PCI environment

Firewall and Router rule set Reviewer (Primary: Ryan McNallie, Alan Williams) – Reviews firewall and router rule sets. This person is also responsible for vetting the business justification for all services, protocols and ports open in the environment.

Log Server Administrator/Log Analyst (Primary: Ryan McNallie, Alan Williams) – Administrator for the logging environment and automated logging tool. The log server administrator is responsible for building and configuring the logging environment outside of the PCI in-scope row in the DC. The log server administrator will install and configure the automated logging tool (e.g. SIEM) and hand out all access as needed to view logs, generate reports, etc. This group reviews the output of the logging tool for activity performed by the other administrators to make sure they have not performed any inappropriate activity.

The Log Server Administrator will not have access to the PCI in-scope environment.
Log Review
Any anomalies discovered by the logging tool (i.e. SIEM) will be reviewed first by the log server administrator and then routed to the proper area listed below:

**Network Log Reviewer** (UITS - NOC) – The network log reviewers are responsible for researching and fixing any items discovered by the automated logging tool or log server administrator that fall outside of “normal” as determined in the logging rules during initial log server setup. These duties will be performed by UITS via a .5 FTE SLA with Student Affairs. Reviews and responds to log anomalies discovered by the automated logging tool or the log server administrator - per the "Log Review Procedure," reviews logs (firewall, switch, router, & SIEM) daily for suspicious and/or anomalous activities and escalates through the "Incident Management Procedure."

**Environment Log Reviewer** (PCI Infrastructure, AD and/or OS Server Administrators) - The environment log reviewers are responsible for researching and fixing any items discovered by the automated logging tool or log server administrator that fall outside of “normal” as determined in the logging rules during initial log server setup. Reviews and responds to log anomalies discovered by the automated logging tool or the log server.

**Application Log Reviewer** (Application Administrator) - The application log reviewers are responsible for researching and fixing any items discovered by the automated logging tool or log server administrator that fall outside of “normal” as determined in the logging rules during initial log server setup. Reviews and responds to log anomalies discovered by the automated logging tool or the log server administrator.