OUHSC Escalation Process for PCI Non-Compliance

Instances of non-compliance with OUHSC PCI policy and standards will be presented to the PCI Governance Group by the PCI Compliance Coordinator or by the PCI Compliance Officer when their reasonable efforts to remedy the non-compliant situation have not been successful. Examples of instances of non-compliance may include, but are not limited to failure to complete PCI training in a timely manner, failure to complete PCI merchant account assessments, failure to complete Security Assessment Questionnaires, or failure to install, configure, and/or operate IT infrastructure in accordance with PCI.

The PCI Governance Group will review the instance of non-compliance presented and assign a risk level to the situation. The Group will adopt an action plan based upon the risk level to resolve the non-compliance and will give the individual or area responsible for the non-compliance a deadline by which to implement the action plan. The PCI Governance Group will also communicate the instance of non-compliance with the appropriate Dean, Vice President, or manager and will include the action plan for resolution.

If the non-compliance has been deemed a high level of risk and no resolution has been made by the department or college, then the PCI Governance Group and/or other appropriate administrators or governing bodies may take action to remedy the non-compliance, including but not limited to, additional monitoring or assessments, and even suspension or revocation of a merchant account.

If the non-compliance is not resolved to the Group's satisfaction, the Group may present the matter to the Information Security Review Board (ISRB) for resolution.

4/20/2017