21. Database Access & Configuration Settings Policy

Overview
In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, UIT-PCI Compliance Services has established a formal policy and supporting procedures concerning database access & configuration settings. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding UIT-PCI Compliance Services’ needs and goals.

Policy
UIT-PCI Compliance Services will ensure that the Database Access & Configuration settings policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that all users are authenticated prior to access.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that user direct access to or queries of databases are restricted to database administrators.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that application IDs can only be used by the applications (and not by individual users or other processes).

Responsibility for Policy Maintenance
UIT [PCI Compliance Services](mailto:pci-compliance@stanford.edu) is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.