Document Review Log

Date Reviewed	Description of Changes
8/17/2023	Initial Draft approved by Senior Leadership Team

otherwise, to the extent expressly required by applicable law, in which case, Service Provider shall (i) use best efforts to notify Customer before such disclosure or as soon thereafter as reasonably possible]; (ii) be responsible for and remain liable to Customer for the actions and omissions of such Unauthorized Third Party concerning the treatment of such Customer Information as if they were Service Provider's own actions and omissions.

(c) Service Provider agrees to implement and maintain appropriate information technology security controls in the following areas, as outlined in APU Policy 9.4000, IT Security for 3rd Party Partners and providers, and NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (incorporated by reference).

d) If the Service Provider is hosting data on a multi-tenant system, these controls must include controls to prevent the unauthorized access of APU data to other tenants.

i) Access Control
ii) Awareness and Training
iii) Audit and Accountability
iv) Configuration Management
v) Identification and Authentication
vi) Incident Response
vii) Maintenance
viii) Media Protection
ix) Personnel Security
x) Physical Protection
xi) Risk Assessment
xii) Security Assessment
xiii) System and Communications Protection
xiv) System and Information Integrity

e) [required only if the service provider will be handling confidential payment card data] The service provider must Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:

- Firewalls