**Definitions and Payment Card Industry (PCI) links**

AoC, Attestation of Compliance **–** A report prepared by a QSA in which the QSA and merchant attest to the entity’s compliance status.

Cardholder Data **–** 16-digit PAN (primary account number), Cardholder Name, and Expiration date

CVV Card Verification Value Code (a.k.a CVV2) - This is a three (3) digit number on the back of a credit card. In the case of American Express, this is a four (4) digit code on the front of the credit card.

DSS (Data Security Standards**) –** The credit or debit card data security standards are established by the PCI Council. Merchants at the University must refer to the current and applicable provisions of the DSS. <https://www.pcisecuritystandards.org/security_standards/documents.php>

IP Address – Internet Protocol Address is a unique number used to represent every computer in a network. The format of an IP Address is four sets of numbers separated by dots (e.g. 198.123.123.7)

Merchant - A merchant is a department, entity, or affiliate that accepts cardholder payments using the University’s merchant processor(s). A University merchant is assigned a merchant account number by the Office of the Treasurer.

P2PE – P2PE stands for Point 2 Point Encryption. A validated P2PE solution has been vetted and approved by the council and if installed using the vendor supplied PIM (P2PE Instruction Manual). The following link provides a complete list of validated P2PE solutions. <https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions>

PCI Software - PCI software or PA-DSS software (Payment Application Data Security Standard) is installed on a University computer and determined by the credit card industry to follow the industry’s best practices for securing credit card information. All PA-DSS validated payment applications must be installed per the vendor supplied PA-DSS installation guide. The following link provides a complete list of PCI approved Payment applications. <https://listings.pcisecuritystandards.org/assessors_and_solutions/payment_applications>

PAN (Primary Account Number) – The 16 digit card number.

PED (Pin Entry Device) – Terminal that allows entry of a customer’s Personal Identification Number.

PIN (Personal Identification Number) – Personal number used in debit card transactions.

PCI Council (Payment Card Industry) – Visa, MasterCard, American Express, and Discover, have formed a council to establish Data Security Standards (DSS) for the industry. Please see the following link for their website. <https://www.pcisecuritystandards.org/>

Payment Gateway – A payment gateway is a type of service provider that transmits, processes, or stores credit cardholder data as part of a payment transaction. They facilitate payment transactions such as authorizations and settlement between merchants or processors, also called endpoints. Merchants may send transactions directly to an endpoint or indirectly using a payment gateway.

RoC, Report of Compliance – PCI Report prepared by a Qualified Security Assessor to verify a merchant’s compliance with the PCI DSS, Data Security Standards.

QSA, Qualified Security Assessor – A PCI assessor certified and listed on the PCI Council’s list of QSA companies.

Sensitive Authentication Data - refers to the three (3) or four (4) digit validation code, CVV2, on the front or back of a card and PIN number, personal identification numbers. PCI does not permit this data to be stored even if it is protected according to the PCI Data Security Standards.

Service Provider - A vendor that provides access to the Internet and to applications to facilitate the transfer and/or storage of credit card information. The following link provides a complete list of PCI Compliant Service Providers. (Please note, this list is maintained on Visa’s website.) <http://www.visa.com/splisting/searchGrsp.do>

**Contacts**

|  |  |  |  |
| --- | --- | --- | --- |
| **Subject** | **Office** | **Telephone** | **E-mail** |
| PCI Compliance | Office of the Treasurer | 573-882-3318 | laymanj@umsystem.edu  |
| Data Security – MU, UM, HOSP, & UP | Information Security & Access Management | 573-882-5000 | isam@missouri.edu  |
| Data Security – UMSL  | UMSL IT Security | 314-516-4859 | monroem@umsl.edu  |
| Data Security – MO S&T | MO S&T IT Security | 573-341-6398 | koobp@mst.edu  |
| Data Security – UMKC  | UMKC IT Security | 816-235-5294 | malynj@umkc.edu  |
| Columbia Business PCI Policy | MU Cashiers | 573-882-8227 | carrmm@missouri.edu  |
| UMKC Business PCI Policy | UMKC Cashiers and Collections | 816-235-1366 | SchwartzPN@umkc.edu  |
| MO S&T Business PCI Policy | S&T Cashiers Office | 573-341-7691 | kelleykm@mst.edu  |
| UMSL Business PCI Policy | UMSL Cashiers | 314-516-6608 | hessmr@umsl.edu  |
| UP Business PCI Policy | UP Finance | 573-882-0427 | mckinzier@health.missouri.edu  |
| Hospital Business PCI Policy | Hospital Patient Revenue | 573-882-8874 | smithleann@health.missouri.edu  |
|  | Pharmacies | 573-884-6139 | danaharman@health.missouri.edu  |
|  | Cafeterias & Gift Shops | 573-884-7759 | gebhardtc@health.missouri.edu  |