University of Victoria | Accounting Services

What is Payment Card Industry (PCI)?

In an effort to reduce credit card fraud, the ***PCI*** developed a set of security standards called *Data Security Standards* (DSS) or PCI DSS. All organizations which accept *payment cards* (debit or credit) must follow these standards. This is a university wide initiative and requires all departments and offices to be compliant.

In addition to severe fines to the university, a single point of failure could lead to ***withdrawal of card services for the entire university.*** If you ever are in doubt as to a procedure that should be followed in terms of PCI compliance, always check with your supervisor.

PCI Data Security Standards

The standards cover a broad range of requirements including the collection, storage and transmission of *payment card* information:

Goals	PCI DSS Requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect *cardholder* data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect *cardholder* data	3. Protect stored *cardholder* data. 4. *Encrypt transmission* of *cardholder* data across open, public networks.
Maintain a vulnerability management program	5. Use and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement strong access control measures	7. Restrict access to *cardholder* data by business need to know. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to *cardholder* data.
Regularly monitor and test networks	10. Track and monitor all access to network resources and *cardholder* data. 11. Regularly test security systems and processes.
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel.

Goals

Remove sensitive authentication data and limit data retention. This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other cardholder data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it.

Protect the perimeter, internal, and wireless networks. This milestone targets controls for points of access to most compromises – the network or a wireless access point.

Secure payment card applications. This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data.

Monitor and control access to your systems. Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment.

Protect stored cardholder data. For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protection mechanisms for that stored data.

Finalize remaining compliance efforts, and ensure all controls are in place. The intent of Milestone Six is to complete PCI DSS requirements, and to finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.