**2022/08/09**

PCI Compliance & Encryption

Case Study

Submitted to Dr. Mahbub Mishu (PhD)  
D’Artagnan Boocock, Jack Chen, Rhean Propp, Cole Sanheim

Table of Contents

[**PCI Compliance**](#_gt5pfjtnjzmq) **2**

[Does SAIT need to be PCI compliant?](#_gipoyhfd5muk) 2

[**Security**](#_5wjpkjofh5ao) **2**

[What needs to be secure?](#_vojdnoq3zu8p) 2

[Is this just an IT project?](#_dw66hw7m11qr) 2

[Can we do it without outside help?](#_dfrvii6fzj78) 3

[**Domains**](#_3t8udqi30mfw) **3**

[What PCI domains will come into play?](#_31xhvywruqq0) 3

[**Reporting**](#_fn3juahq2gl6) **4**

[What details should be included in your report to your boss?](#_mc923ftz34dj) 4

[How many decisions regarding both mandatory and optional implementation items are in the report?](#_oyb5i9v7a8oc) 5

[**Conclusion**](#_9uusbzd564o7) **5**

[Where do you start?](#_b0tqx0b1zdb8) 5

# PCI Compliance

## Does SAIT need to be PCI compliant?

Yes. SAIT handles credit card information. This information needs to be handled securely.

# Security

## What needs to be secure?

The most vulnerable information includes credit card numbers, name, address, phone number and emails. This additionally includes any miscellaneous account information.

Primary security concerns surround the transaction process and storage of sensitive data. Transactions can include card readers and online payment applications.

Data storage should be kept in an environment that only authorized personnel have access to. Any sensitive data must be encrypted. Only necessary information such as account details, name, emails and phone numbers should be visible to account managers & personnel who oversee payment processing.

## Is this just an IT project?

No. This is a common myth in the industry. PCI DSS compliance is considered more than just a project as it is an ongoing process of assessing, remediating and reporting. A multi-disciplinary team will be in charge of the management of PCI compliance.

## Can we do it without outside help?

Ideally, this project should be handled by the company’s internal staff. This allows the encryption, methods and processes to be left unknown by outside parties.

However, depending on the circumstances of the company and the project, a trusted third party could be brought in as a contractor for this project. It would be incredibly important to ensure that the hired contractor is reputable, trustworthy and any and all information after the project’s completion is controlled by the company and its internal staff.

# Domains

## What PCI domains will come into play?

There are several PCI domains that come into play. This includes building and maintaining a secure network and systems. Requiring a firewall to protect cardholder data and ensure vendor supplied passwords are not used.

Cardholder data needs to be protected. The transmission of this data needs to be encrypted across open networks.

Maintaining a vulnerability management program allows the protection of systems against malware. Regular security patches and antivirus software enables the security of the system and its applications.

Additionally, strong access control needs to be implemented. Restricting access to cardholder data through a need to know basis. Identifying and authenticating access to system components and restricting the physical access to this cardholder data is included in these requirements.

The network needs to be regularly monitored and tested. Systems for monitoring the network include logging and tracking of all data that passes through. The system needs to be regularly tested to ensure there are no issues that have come into play.

Maintaining an information security policy addresses concerns, and provides a systematic process for handling information for all personnel.

# Reporting

## What details should be included in your report to your boss?

Details should include an overview of the project plan. Who will be involved? If there is a third party contractor being hired, who are they, how reputable they are, and how the information will be handled after their job is completed.

After completion of the job, your boss should know what security measures have been put in place. What implementations have been made that change how processes were previously performed in the past, and who is now responsible for this information.

## How many decisions regarding both mandatory and optional implementation items are in the report?

There are several decisions regarding mandatory and optional implementation items on the report. The security program must restrict access to cardholder data on a need to know basis. Additionally, there needs to be a system created for identifying and authenticating access to system components.

Assigning IDs to each person ensures accountability. Through the ID assignment, malicious actions can then be associated with the ID number in question.

# Conclusion

## Where do you start?

The start of the project involves project planning. Who will be taking charge of the project? Who is responsible for its implementation? What are the projected deadlines? Who is on the team? Is outside help needed? If so, who will the company be hiring as a trusted third party? Once the planning phase has concluded, project implementation can begin.