PCI DSS v4.0 Toolkit – Payment Card Industry Data Security Standard

Level 1 - Policies	
1.	Operational Security Policy Statement
2.	Information Security Policy
3.	Firewall and Router Policy
4.	System Configuration Policy
5.	Data Retention and Disposal Policy
6.	Cryptographic Key Management Policy
7.	Cardholder Data Policy Statement
8.	Anti-Malware Policy
9.	Vulnerability Management Policy
10.	Application and System Development Software Policy
11.	Change Management Policy
12.	Access Control Policy
13.	Physical Security Policy Statement
14.	Card Reader Policy
15.	Systems Monitoring Policy
16.	Testing Systems and Processes Policy
17.	Information Security Responsibilities Policy Statement
18.	Policy Statement Technology Usage
19.	Internet Acceptable Use Policy
20.	Network Access Control Policy
21.	Password Policy Statement
Level 2 - Procedures and Processes	
Procedures	
1.	Inventory and Ownership of Assets Procedure
2.	User Access Management Procedure
3.	Managing Service Providers Procedure
4.	Responding to Information Security Incidents Procedure
5.	Document Control Procedure
6.	Control of Records Procedure
7.	Disposal of Media Procedure
8.	Data Centre Access Procedure

Processes	
1.	PCI DSS Charter
2.	PCI DSS Compliance Programmer
3.	Staff Training Programmer
4.	PCI DSS Operational Security Programmer
5.	Pen Testing Methodology
6.	Username Administration
7.	Targeted Risk Analysis
8.	Customized Approach Matrix
9.	Customized Approach Targeted Risk Analysis
10.	Rules for Use of Email
11.	Information Security Classification Guidelines
Level 3 - SOPs	
1.	Handling of Virus Attacks
2.	Personal Security
3.	Warehouse Security
4.	Information Security Incident Management
Level 4 - Formats and Templates	
Formats	
1.	Change Request Form
2.	Inventory Template
3.	Cryptographic Key Custodian Acceptance Form
4.	Individual User Agreement
5.	Pen Test Log Sheet
6.	Pen Test Report Evaluation Checklist
7.	Risk Treatment Plan
8.	List of Service Providers
9.	Shared Responsibility Matrix
10.	Credit Card Receipt
11.	Master List of Records
12.	Master List of Document Approval
13.	Security Incident and Investigation Form
14.	Outsourced Service Details
15.	Customer Complaint Report
16.	Continual Improvement Monitoring Log

17.	Security Incident Report
Templates	
1.	Meeting Agenda Template
2.	Meeting Minutes Template
3.	Service Level Agreement Template
4.	Work Instruction Template
Guidelines for Implementation Methodology	
1.	Documentation Analysis Tool
2.	Encryption Key Management Guidance
3.	Gap Analysis Tool
4.	Roles and Responsibilities Matrix
5.	Scoping Guidance

Contents

1 Scope 4

2 Responsibility 4

3 Procedure 4

3.1 Data Centre Access Principles 4

3.2 Requesting Access to the Data Centre 4

3.3 Visitor Guidelines 5

3.4 Equipment Deliveries 6

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

Scope

The purpose of this document is to provide customers, third parties, visitors, and other persons with clear instructions on how to request access and what is expected from the Organization Name data Centre.

Responsibility

The IT Managers or Asset Owners are responsible for granting permitted access to employees, including customers, suppliers, and other third parties.

Procedure

Data Centre Access Principles

There are several principles that govern access to data Centre's at Organization Name:

- The data centre should be accessible only to authorized staff of Organization Name;
- There should be specific authorizations for all access;
- Visitor registration and dispersion are required at the data center;
- Visitor identification badges must always be worn by all visitors.

Requesting Access to the Data Centre

Reach us at +xx xxx xxx xxxx or send us an email at access@[Company Name].com to request access to an Organization Name data Centre.

It will typically be necessary to give 24 hours' notice. Access is often only permitted during regular work hours, which are Monday through Friday from 9 am to 5:30 pm, excluding holidays.

Visitor Guidelines

The following regulations shall apply to all clients, third parties, and other visitors granted access to Organization Name's data center:

- The data centre does not permit the use of food or beverages;
- Smoking is not permitted anywhere on the site;
- Organization Name's health and safety policies must be observed at all time

Contents

1 Scope 4

2 Responsibility 4

3 Compliance Programmed 4

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

1 Scope

The PCI DSS Compliance Program applies to employees within Organization Name that are involved in maintaining Organization Name's compliance with the Payment Card Industry Data Security Standard (PCI DSS) in line PCI DSS Charter.

2 Responsibility

Within this compliance programmed, the following responsibilities are in charge of the assigned areas:

1. The Insert Role is responsible with overseeing the day-to-day business activities related to PCI DSS compliance.
2. The Insert Role is responsible for overseeing the ongoing validation of PCI DSS requirements.
3. The Insert Role is responsible for overseeing the business-impact study to assess potential PCI DSS impact on strategic business decisions.

3 Compliance programmer

3.1 To maintain PCI DSS compliance, the following activities must be carried out.

Activity Name	Description	PCI DSS Requirement	Interval/Frequency	Responsible Business Unit/Team

3.2 Organization Name's evaluation technique will be used to monitor above compliance actions and to continuously validate requirements. [Describe/insert your approach here; examples include PDCA, ISO 27001, COBIT, DMAIC, and Six Sigma].

3.2 The procedure for performing the yearly PCI DSS assessment is [Describe the process here, or include a reference to an assessment process document].

Contents

1 Scope 4
2 Responsibility 4
3 Requirements 4

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

1 Scope

Organization Name regulates access to data and networked services in accordance with business and security requirements, including the Payment Card Industry Data Security Standard (PCI DSS).

2 Responsibility

1. Access controls for Organization Name must be set up and maintained by the System Administrator.
2. Changes to the configuration of access control mechanisms must be approved by the Information Security Manager.

3 Requirements

3.1 Access control rules and user rights for applications, services, and devices are clearly defined in standard user profiles. These profiles, along with the corresponding business requirements fulfilled by the controls, can be found in [add reference to where they can be accessed].

3.2 A risk assessment that identifies all information relevant to the application, service, or device and the threats to that information determines the security requirements of each business application, service, or device.

3.3 The information processed within the application, service, and device is classified into different levels, and it is essential to maintain consistency between the classification levels and the access control requirements across the systems and network(s).

3.4 Compliance with data protection and privacy legislation, Organization Name's statutory objectives, and contractual commitments (including the PCI DSS) governs access to data, including cardholder data, and services.

3.5 The guiding principle of "everything is generally forbidden unless expressly permitted" is enforced, with a default setting of "deny all".

3.6 Rules must be consistently enforced and differentiated from guidelines, which may not always be enforced.

3.7 Access rights are systematically and consistently managed throughout the network(s).

INCIDENT IDENTIFICATION INFORMATION	
Incident Detector's Information:	
Name:	Date/Time Detected:
Job Title:	Location:
Phone/Contact No:	System/Application:

INCIDENT SUMMARY		
Type of Incident Detected:		
Denial of Service	Malware/Ransom Ware	☐ Unauthorized Use/Disclosure
Loss/Theft	Unplanned Downtime	☐ Inadvertent Site Security
Unauthorized Access	Phishing	☐ Other
Description of Incident:		
Names of Others Involved:		
1.	2.	3.
4.	5.	6.

INCIDENT NOTIFICATION		
☐ PCI DSS Leadership	☐ System/Application Owner	☐ Legal Counsel
☐ Security Incident Team	☐ System/Application Vendor	☐ Human Resources
☐ Administration	☐ Public Affairs	☐ Other

ACTIONS (INCLUDE START & STOP TIMES)
(Phase I) Identification Measures (Incident Verified, Assessed, Options Evaluated):
(Phase II) Containment Measures:

Evidence Collected (Systems Logs, etc.):
(Phase III) Eradication Measures:
(Phase IV) Recovery Measures:
EVALUATION
How well did the workforce members respond?
Were the documented procedures followed? Were they adequate?
What information was needed sooner?
Were any steps or actions taken that might have inhibited the recovery?
What could the workforce members do differently the next time an incident occurs?

What corrective actions can prevent similar incidents in the future?
What additional resources are needed to detect, analyze, and mitigate future incidents?
Other conclusions/recommendations:
FOLLOW-UP
Review by (Organization to determine):

Security Official	Concerned Department/Team
Insert Name	Insert Name

Recommended Actions Carried Out:

Initial Report Completed By	Follow-Up Completed By
Insert Name	Insert Name
Insert Date	Insert Date