ARCTIC WOLF Layer 7 Data Solutions

BRIEF

PCI DSS Security Compliance Checklist

AWN™ CyberSOC

Goals of PCI DSS:

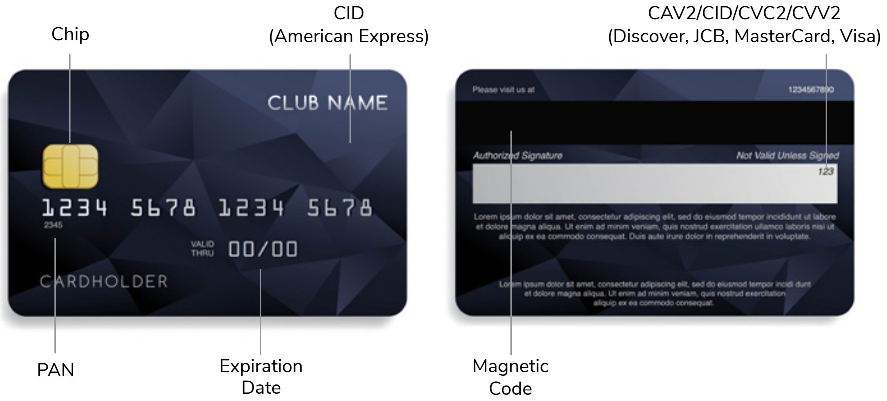
- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards set by the PCI Security Standards Council to protect cardholder data. The PCI DSS applies to all entities that store, process, and/or transmit cardholder data.

Security Controls and Processes for PCI DSS Requirements

The security controls and processes required by PCI DSS are vital for protecting cardholder account data, including the PAN – the primary account number printed on the front of a payment card. Merchants and any other service providers involved with payment card processing must never store sensitive authentication data after authorization. This includes sensitive data that is printed on a card, or stored on a card's magnetic stripe or chip – and personal identification numbers entered by the cardholder. This document presents the objectives of PCI DSS and related 12 requirements.

Types of data on payment card



PCI DSS compliance monitoring with the AWN CyberSOC solution:

- Monitor configuration changes
- Monitor systems that store PAN
- Monitor systems for data leaks
- External vulnerability scans
- Web traffic monitoring
- User behavior analysis
- Log management & analysis
- Log storage for 90 days & beyond
- Forensic analysis
- Intrusion detection system
- Security incident response

PCI DSS Security Checklist

PCI DSS is best achieved in two phases. Phase one is setting the controls, where your organization plans and commits to becoming compliant. This phase typically involves planning, leadership commitment, and setting up of basic infrastructure such as Firewall, Anti-virus, password management, data storage & encryption, identity management and more. Phase two is monitoring those controls to include vulnerability scanning, monitoring for configuration changes, intrusion detection, user behavior monitoring, and incident response. Arctic Wolf helps you with the second phase by providing a SOC-as-a-Service delivering managed detection and response.

PCI #	PCI Requirement	Phase One	Phase Two through AWN™ CyberSOC PCI monitoring
1	Install and maintain a firewall configuration to protect cardholder data	Setup Firewall and zoning	Monitor the Firewall configuration for unauthorized changes
2	Do not use vendor-supplied defaults for system passwords and other security parameters	Change default passwords	Monitor the configuration for critical infrastructure
3	Protect stored cardholder data	Data storage	Monitor systems for attacks and data leaks
4	Encrypt transmission of cardholder data across open, public network	Encrypt PAN	Security monitoring of systems that contain PAN
5	Use and regularly update anti-virus software or programs	Setup Anti-Virus	Security monitoring of Anti-Virus systems
6	Develop and maintain secure systems and applications	Build/ deploy secure apps	External vulnerability scans Application log monitoring
7	Restrict access to cardholder data by business need to know	Identity management	Monitor user logon activity through integrations with Active Directory
8	Assign a unique ID to each person with computer access	Identity management	Monitoring user behavior based on identifiers
9	Restrict physical access to cardholder data	Identity management	*NA*
10	Track and monitor all access to network resources and cardholder data	Identity management	Log management and SIEM for auditing & forensics
11	Track and monitor all access to network resources and cardholder data	*NA*	External vulnerability scans Intrusion Detection System Continuous security monitoring
12	Maintain a policy that addresses information security for all personnel	Create an IR team	Security incident response Managed Security Training for users

✓ PCI compliance and AWN CyberSOC

AWN CyberSOC provides continuous monitoring of your critical infrastructure for threat detection and management. The service starts by evaluating your security configurations, performing vulnerability scans and related patching recommendations, logging all your security events for analysis & forensic investigation, monitoring network activity to detect known and zero-day attacks, and implementing incident response principles. All of these activities are an important part of a success PCI DSS compliance initiative.

✓ Arctic Wolf redefines the economics of security

Arctic Wolf Networks is redefining the economics of security through an affordable, turnkey SOC-as-a-Service solution that deploys in less than 60 minutes. With a designated Concierge Security Engineer™, a proprietary cloud-based SIEM, 24x7 monitoring, incident response, vulnerability scans, and a tailored escalation & ticketing process, AWN CyberSOC provides an end-to-end security monitoring at a fraction of a cost of a security engineer.

ARCTIC WOLF Layer 7 Data Solutions

Contact us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com