NetFoundry Alignment to PCI-DSS 4.0.1 Requirements

The 12 Requirements of PCI DSS v4.0.1

The requirements set forth by the PCI SSC are both operational and technical, and the core focus of these rules is to protect account data at all times.

These standards apply not just to merchants and ISVs but to anyone that stores, processes, transmits, or otherwise affects the security of account data. Service providers whose products or services can affect the security of cardholder data are also responsible for compliance with applicable requirements.

The 12 requirements are grouped under six control objectives:

Build and Maintain a Secure Network and Systems

1. Install and Maintain Network Security Controls
2. Apply Secure Configurations to All System Components

Protect Account Data

3. Protect Stored Account Data
4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Maintain a Vulnerability Management Program

5. Protect All Systems and Networks from Malicious Software
6. Develop and Maintain Secure Systems and Software

Implement Strong Access Control Measures

7. Restrict Access to System Components and Cardholder Data by Business Need to Know
8. Identify Users and Authenticate Access to System Components
9. Restrict Physical Access to Cardholder Data

Regularly Monitor and Test Networks

10. Log and Monitor All Access to System Components and Cardholder Data
11. Test Security of Systems and Networks Regularly

Maintain an Information Security Policy

12. Support Information Security with Organizational Policies and Programs

Note on this revision: This page has been updated from the earlier PCI DSS v3.2.1-based version to reflect PCI DSS v4.0.1. Several requirement titles and numbers changed between v3.2.1 and v4.0, and two requirements that were previously "best practice" — MFA for all access into the CDE (8.4.2) and automated protection for public-facing web applications (6.4.2) — became fully enforced as of March 31, 2025. Both are called out below because they materially affect how NetFoundry's capabilities map to the standard.

Requirement 1: Install and Maintain Network Security Controls

Network security controls (NSCs) — such as firewalls and other network security technologies — are network policy enforcement points that control traffic between logical or physical network segments based on pre-defined rules. NSCs examine ingress and egress traffic and decide, based on policy, whether it is allowed to pass. Traditionally this function was provided by physical firewalls; v4.0.1 explicitly broadens the definition to include virtual devices, cloud access controls, virtualization/container systems, and other software-defined networking technology.

1.1 Establish and implement NSC configuration standards, including documentation of all connections between the CDE and other networks, diagrams of cardholder data flows, and a review of rule sets at least every six months.

1.2 NSCs are configured and maintained, restricting inbound and outbound traffic to only that which is necessary for the CDE, with a "deny all" default.

1.3 Network access to and from the CDE is restricted, including prohibiting direct public access between the Internet and any CDE system component.

1.4 Connections between trusted and untrusted networks are controlled, including at network security devices between the entity's networks and the CDE.

1.5 Risks to the CDE from computing devices that can connect to both untrusted networks and the CDE (e.g., employee laptops) are mitigated, for example with personal firewall or equivalent controls.

NetFoundry alignment: NetFoundry provides control of packets and access as a network security control, though not in the traditional form of a perimeter firewall — a distinction v4.0.1's broadened NSC definition now explicitly recognizes. The NetFoundry Network allows only previously authenticated and authorized traffic into a software-defined data plane, and depending on configuration, the physical or virtualized system interface can be

configured to reject all traffic that is not part of the NetFoundry Network instance. This zero-trust, identity-based access model helps customers meet 1.2 through 1.5 of the requirement; 1.1 (documented policies, diagrams, and periodic rule-set review) is an administrative control the customer must implement within their own organization, informed by their NetFoundry Network design.

Requirement 2: Apply Secure Configurations to All System Components

Malicious individuals, both external and internal, often use default passwords and other vendor-default settings to compromise systems. Applying secure configurations reduces the attack surface by changing defaults, removing unnecessary accounts and services, and hardening system components consistently.

2.1 Processes for applying secure configurations are documented and understood.

2.2 System components are configured and managed securely, including changing all vendor-supplied defaults, removing/disabling unnecessary functionality, and encrypting all non-console administrative access using strong cryptography.

2.3 Wireless environments connected to or transmitting into the CDE are configured and managed securely (e.g., changed defaults, strong encryption for authentication/transmission).

NetFoundry alignment: NetFoundry does not ship default passwords, so this is natively aligned with the intent of 2.2. Where NetFoundry-provided images are used (AWS AMI, Azure image, etc.), the image is hardened using a CIS Benchmark baseline. Customers remain responsible for maintaining that security posture once a gateway is deployed into their own environment, since NetFoundry has no access to those gateways post-deployment. All administrative access to NetFoundry-managed components uses strong cryptography by design, and the configuration model makes it straightforward to inventory in-scope system components accessed via the NetFoundry Network.

Requirement 3: Protect Stored Account Data

Protection methods such as encryption, truncation, masking, and hashing are critical components of account data protection. Sensitive authentication data must never be stored after authorization, and primary account numbers (PAN) must be rendered unreadable wherever stored, with documented key-management processes covering the full cryptographic key lifecycle (3.6, 3.7).

NetFoundry alignment: NetFoundry does not handle, process, or store customer account data at rest — it provides network-layer connectivity and access control, not a data storage service. Requirement 3 is therefore not applicable to the NetFoundry solution itself.

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

The use of strong cryptography provides assurance of data confidentiality, integrity, and non-repudiation during transmission. PAN must be encrypted during transmission over networks that are easily accessed by malicious individuals, including untrusted and public networks; misconfigured wireless networks and legacy encryption/authentication protocols remain common attack targets.

4.1 Processes for protecting PAN in transit are documented and understood.

4.2 PAN is protected with strong cryptography during transmission, and only trusted keys/certificates are accepted; where SSL/early TLS was historically used, it must not be introduced or continue in use as a security control (subject to the narrow POI terminal exception in Appendix A2).

NetFoundry alignment: Strong encryption for all transmissions is a fundamental characteristic of the NetFoundry Network — it is not an optional add-on but part of how the overlay establishes and maintains connections. Deploying a NetFoundry Network therefore inherently supports Requirement 4's transmission-security objective.

Requirement 5: Protect All Systems and Networks from Malicious Software

Malicious software (malware) — viruses, worms, trojans, spyware, ransomware, keyloggers, rootkits, malicious scripts and links — can enter a network through everyday business activity such as email and web/internet use. v4.0.1 broadened this requirement's scope from the older "anti-virus on commonly affected systems" framing: entities must now protect all systems and networks from malware, and any system component excluded from anti-malware protection must be justified by a documented, periodic (targeted) risk analysis (5.2.3, 5.2.3.1) rather than an assumed exemption. v4.0.1 also adds an explicit anti-phishing requirement (5.4).

NetFoundry alignment: NetFoundry provides images and other methods for deploying its software. Once gateways or clients are running in the customer's environment, the customer is responsible for maintaining the anti-malware and anti-phishing posture of those systems per their own standards and practices — including performing and

documenting the periodic risk evaluations now expected under 5.2.3.1 for any components not running traditional anti-malware tooling.

Requirement 6: Develop and Maintain Secure Systems and Software

Security vulnerabilities in systems and software can allow attackers to gain privileged access to account data. Vendor-provided patches must be applied, and bespoke/custom software should follow a secure software lifecycle (SLC) and secure coding practices. Requirement 6.4 (protection of public-facing web applications) changed materially in v4.0.1: the older "vulnerability assessment *or* automated technical solution" either/or choice (formerly 6.6) is being replaced. As of **March 31, 2025**, an automated technical solution — a web application firewall (WAF), Runtime Application Self-Protection (RASP), or equivalent — that continually detects and prevents web-based attacks is now a **mandatory** control in front of public-facing web applications (6.4.2), not an optional alternative to periodic scanning.

NetFoundry alignment: While Requirement 6 is primarily binding on the entity that develops and operates applications processing cardholder data, NetFoundry applies equivalent practices within its own software development lifecycle. NetFoundry's engineering teams follow an Agile SDLC and uses tools and automation for functional and security testing, supported by annual third-party penetration testing and ongoing vulnerability/web-posture scanning. Separately, because NetFoundry's zero-trust model can remove public-facing exposure of an application entirely — replacing an internet-routable endpoint with private, identity-based access — it is directly relevant to how customers satisfy 6.4.1/6.4.2: an application that is never exposed to the public internet reduces the attack surface the WAF/RASP requirement is designed to address, and can be a complementary or, in some architectures, alternative control worth discussing with a QSA.

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

Access control rules must ensure that critical data can only be accessed by authorized personnel, based on need-to-know and job responsibility. v4.0.1 clarifies that access rights (what a user can reach) and privileges (what a user can do once there) are distinct concepts, and that access control systems must default to "deny all" unless explicitly allowed. These requirements apply to employees, contractors, consultants, and third parties, and (in relevant parts) to service accounts; they do not apply to consumers/cardholders.

NetFoundry alignment: NetFoundry can assist directly with Requirement 7. Where systems holding cardholder data are NetFoundry-enabled, access to those systems can be centrally controlled — down to individual identities and least-privilege network paths — via the web console or programmatically, with a default-deny posture. Access changes can be audited at any time, and logs retrieved and retained to support long-term auditability of changes that may have affected user access.

Requirement 8: Identify Users and Authenticate Access to System Components

Assigning a unique ID to each person with access ensures that actions on critical systems can be traced to known, authorized individuals. v4.0.1 significantly expanded the multi-factor authentication (MFA) requirements compared with v3.2.1:

- **8.4.1** — MFA is required for all non-console *administrative* access into the CDE (carried over from the prior standard).
- **8.4.2** — **new/broadened in v4.0.1:** MFA is required for **all** non-console access into the CDE, for any user, not administrators alone. This became fully enforced (no longer "best practice") as of **March 31, 2025**.
- **8.4.3** — MFA is required for all remote access originating from outside the entity's network that could access or impact the CDE.

MFA can be applied at the network level or the system/application level — it does not need to be applied at both — and applies across cloud, hosted, and on-premises systems alike.

NetFoundry alignment: Requirement 8 applies to application and network access generally. NetFoundry can serve as one of the factors in an MFA scheme: because a device is enrolled in the NetFoundry Network and carries an identity established via its installed X.509 certificate and local configuration data, it constitutes "something you have." Combined with an application credential ("something you know") or biometric factor ("something you are"), this can help satisfy MFA requirements. With v4.0.1's expansion of 8.4.2 to cover *all* access into the CDE — not only administrative access — this NetFoundry-based factor is now relevant to a broader population of users than under the prior standard, making it a stronger fit for the current requirement. See Application Specific Networking as a factor in MFA for more detail. More traditional MFA capabilities, such as one time token (OTT) options, are also available, depending on the needs and the assessment findings. Existing OIDC systems may also be integrated to use assets and procedures already in place within the environment.

Requirement 9: Restrict Physical Access to Cardholder Data

Any physical access to cardholder data, systems, or media provides an opportunity for unauthorized removal or exposure of that data, and must be appropriately restricted, monitored, and logged for onsite personnel, visitors, and media alike.

NetFoundry alignment: NetFoundry does not implement anything in the physical space; Requirement 9 remains not applicable to the NetFoundry solution.

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

Logging mechanisms and the ability to track user activity are critical to detecting, and performing forensic analysis of, a compromise. Audit trails must link access to individual users, be protected from tampering, reviewed regularly, retained (at least 12 months, with 3 months immediately available), and synchronized to a consistent time source. v4.0.1 also requires timely detection, reporting, and response to failures of critical security control systems (10.7).

NetFoundry alignment: NetFoundry provides several types of logs and configuration data via its API and console. These can identify who had access via a NetFoundry Network instance to which nodes and systems, when devices were online, and what changes were made to network configuration — information that can be fed into a customer's own logging/SIEM pipeline to support the auditability and time-correlated analysis Requirement 10 calls for.

Requirement 11: Test Security of Systems and Networks Regularly

Vulnerabilities are discovered continually, so systems, processes, and software must be tested frequently. Compared with v3.2.1, v4.0.1 tightens several testing expectations:

- **11.3.1.2** — internal vulnerability scans must generally be performed using **authenticated scanning** (new requirement).
- **11.4.5** — *all* entities relying on segmentation to reduce PCI DSS scope must penetration-test their segmentation controls at least **every 12 months** and after any change to those controls — this obligation is now explicit for all entities, not just service providers.
- **11.4.6** — service providers specifically must continue penetration-testing segmentation controls at least **every 6 months** (unchanged from the prior standard's equivalent requirement).

Quarterly external scans still require an Approved Scanning Vendor (ASV); annual (or more frequent, for service providers using segmentation) penetration testing is still required.

NetFoundry alignment: As with Requirements 6 and 12, this requirement is primarily binding on the holder/processor of cardholder data, but NetFoundry applies equivalent internal practices: automated vulnerability scans are performed weekly with mitigation as needed, and annual penetration tests are performed by competent external testers. Within NetFoundry-controlled production network environments, host-based intrusion detection (HIDS) monitors for unauthorized filesystem changes, including malware installation. Separately, NetFoundry's network segmentation capabilities (see below) are directly relevant to how customers satisfy 11.4.5/11.4.6's segmentation-testing requirements, since the scope and boundaries being tested are often defined by how the NetFoundry overlay segments the environment.

Requirement 12: Support Information Security with Organizational Policies and Programs

The organization's overall information security policy sets the tone for the entity and informs personnel of what is expected of them. This requirement covers policy governance, acceptable use, risk assessment, PCI DSS scope validation, security awareness training, personnel screening, and incident response. v4.0.1 adds an explicit sub-requirement (12.9, including 12.9.2) requiring third-party service providers (TPSPs) to support their customers' PCI DSS compliance — including providing specific information customers need for their own scoping and assessments upon request.

NetFoundry alignment: Requirement 12 is a collection of administrative controls required of the holder or processor of cardholder data and is not directly applicable to NetFoundry Networks. However, NetFoundry maintains a SOC 2 report evidencing that equivalent organizational controls are in place and effective, even though they are not directly assessed against PCI DSS. Under the new TPSP-support expectations in 12.9, NetFoundry is positioned to provide customers with relevant technical and configuration information about the NetFoundry Network to support their own PCI DSS scoping and assessment activities upon request.

Network Segmentation

Excerpted from PCI SSC scoping and segmentation guidance.

Network segmentation — isolating the cardholder data environment (CDE) from the remainder of an entity's network — is not itself a PCI DSS requirement. However, it is strongly recommended as a method that may reduce:

- the scope of the PCI DSS assessment;
- the cost of the PCI DSS assessment;
- the cost and difficulty of implementing and maintaining PCI DSS controls; and
- the risk to an organization, by consolidating cardholder data into fewer, more controlled locations.

Without adequate network segmentation (sometimes called a "flat network"), the entire network is in scope for the PCI DSS assessment.

Given the above, it's clear why organizations under PCI DSS want to segment their networks as much as possible — though doing so introduces cost and operational complexity. NetFoundry can be used to segment networks in an overlay fashion, significantly reducing the need for traditional network reconfiguration. With endpoints enrolled in a NetFoundry Network and configured (via NetFoundry or other methods) to reject all other network traffic, systems can be effectively segmented even while residing on a shared underlying network. As noted under Requirement 11 above, where segmentation is used to reduce assessment scope, v4.0.1 now requires penetration testing of those segmentation controls at least annually for all entities (11.4.5) and at least every six months for service providers (11.4.6) — testing that should be scoped to explicitly cover the NetFoundry-based segmentation boundaries in use.