NODE4

# PCI-DSS Charter and Scope

07/05/2025 Node4 Limited PUBLIC

| Version | Status | Date | Author | Reviewer | Changes |
|---|---|---|---|---|---|
| 1.0 | Approved | 21/01/2019 | Vicky Withey | Andrew Gilbert | Original release |
| 1.1 | Approved | 03/06/2021 | Vicky Withey | Ian Thomas | Annual review |
| 1.2 | Approved | 20/02/2023 | Vicky Withey | Ian Thomas | Annual review |
| 1.3 | Approved | 03/06/2024 | Eddie Adams | Kate Lincoln | Aligned to V4.0 of the PCI standard |
| 1.4 | Approved | 07/05/2025 | Eddie Adams | Kate Lincoln | Scope review frequency updated. Scope reviewed – no change. |

# Contents

# Purpose

Payment Card Industry Data Security Standard (PCI-DSS) is a comprehensive standard designed to enhance the security of payment card transactions. It establishes guidelines and requirements for organizations that handle cardholder data.

By adhering to these standards, Node4 help protect sensitive information, prevent data breaches, and ensure the safety of financial transactions.

By maintaining compliance to this standard, Node4 provide the following:

- **Independent Assurance and Compliance**: providing independent assurance that the physical security controls and management at Node4 Data Centres align with PCI requirements.
- **Universal Benefit**: All Node 4 clients benefit from using these physically secure environments, regardless of whether they specifically need to comply with PCI-DSS. The independently assessed security measures contributes to overall information security programs.

Additionally, our PCI-DSS compliance program complements Node4's existing Information Security Management System (ISMS), which manages controls for ISO 27001 certification and provides an extra layer of assurance regarding physical security. The independent assessment process ensures transparency and confidence in the security practices.

# Objectives & Scope

Node4 is audited against section 9 and 12 of the PCI-DSS as we offer hosted infrastructure in our data centres. The sections below outline the requirements from Node4 data centres to ensure compliance with the PCI-DSS.

The scope includes:

- Derby (DC 1 & 2)
- Leeds (DC 3)
- Northampton (DC 4)

This scope will be reviewed every six months or after any significant event or change.

## Section 9: Restrict Physical Access to Cardholder Data

Any physical access to cardholder data or systems that store, process, or transmit cardholder data provides the opportunity for individuals to access and/or remove systems or hardcopies containing cardholder data. Therefore, Node4 appropriately restrict physical access.

Node4 apply controls to meet the below PCI-DSS requirements:

- **9.1** Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

- **9.2** Physical access controls manage entry into facilities and systems containing cardholder data.
- **9.3** Physical access for personnel and visitors is authorised and managed.
- **9.4** Media with cardholder data is securely stored, accessed, distributed, and destroyed.
- **9.5** Point of interaction (POI) devices are protected from tampering and unauthorized substitution.

### Section 12: Support Security with Organisational Policies

Node4's overall information security policy sets the tone for the whole entity and informs personnel what is expected of them. All relevant personnel are aware of the sensitivity of cardholder data and their responsibilities for protecting it. "Personnel" refers to full-time and part-time employees, temporary employees, contractors, and consultants with security responsibilities for protecting account data or that can impact the security of account data.

Node4 apply controls to meet the below PCI-DSS requirements:

- **12.1** A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.
- **12.2** Acceptable use policies for end-user technologies are defined and implemented.
- **12.3** Risks to the cardholder data environment are formally identified, evaluated, and managed.
- **12.4** PCI-DSS compliance is managed.
- **12.5** PCI-DSS scope is documented and validated.
- **12.6** Security awareness education is an ongoing activity.
- **12.7** Personnel are screened to reduce risks from insider threats.
- **12.8** Risk to information assets associated with third-party service provider (TPSP) relationships is managed.
- **12.9** Third-party service providers (TPSPs) support their customers' PCI-DSS compliance.
- **12.10** Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

## Independent Assessment

Annually, Node4 engages an independent Qualified Security Assessor (QSA) to evaluate the company's compliance with the Payment Card Industry Data Security Standards (PCI-DSS).

Upon successful completion of the assessment, the Qualified Security Assessor Company (QSAC) issues a Report on Compliance (RoC) and an Attestation of Compliance (AoC).

Interested parties, including our customers, can access the completed Attestation of Compliance, which assures that Node 4's PCI-DSS assessment aligns with the requirements of the standard from the resource page on our website.

# Roles and Responsibilities

## Executive Board

Node4 Executive Board demonstrate leadership and commitment to PCI compliance by:

- Taking responsibility for the effectiveness of the PCI-DSS compliance efforts in line and included within the Node4 ISMS.
- Ensuring this PCI-DSS charter and scope aligns with Node4's strategic direction and context.
- Ensuring that the necessary resources for PCI-DSS compliance are readily available.
- Promoting continual enhancement of security measures through Information Security management reviews.

## Quality and Compliance Team

Node4's Quality and Compliance team are responsible for:

- Undertaking internal audits in relation to the ISMS, PCI-DSS requirements and physical security controls.
- Facilitate external auditors to complete external audits to ensure we are conforming to ISO 27001 and PCI-DSS requirements.
- Managing any non-conformities which may arise.
- Providing sufficient information security training to all employees, which is refresher annually.
- Managing risks and opportunities for improvement.
- Understanding the needs and expectations of interested parties.
- Preparing a response and action plan to any potential incidents or emergency situations which may arise.

## Data Centre Operations

Node4's Data Centre Operations team are responsible for:

- Maintaining physical security of the data centres in line with our access control policies.
- Keeping up to date with maintenance of the data centres.
- Identifying any risks in conjunction with the Quality and Compliance team.
- Identifying any opportunities for improvement in conjunction with the Quality and Compliance team.
- Ensuring that Data Centres comply with all relevant laws and regulations.

# Communication

Node4 maintains an open and proactive communication approach, ensuring that stakeholders are well-informed about security measures, compliance, and their collective role in safeguarding sensitive data.

- **Stakeholder Engagement** - Node4 actively engages with interested parties, emphasizing the importance of information security through training, code of conduct and due diligence. We communicate the organisation's commitment to ISO 27001 and PCI-DSS compliance.
- **Policy Dissemination** - Node4 establishes clear policies related to information security, including ISO 27001 and PCI-DSS. These policies are communicated across the organisation, ensuring everyone understands their roles and responsibilities.
- **Training and Awareness** - Node4 information security training to interested parties. These sessions cover security practices, compliance requirements, and the impact of their actions on data protection.
- **Reporting and Metrics** - Node4 generates regular reports on security performance, incidents, and compliance status.
- **Incident Communication** - In case of security incidents, Node4 promptly communicates with affected parties. Transparency during incidents ensures stakeholders are informed and can take necessary actions.
- **External Audits** - Node4 facilitates external audits by independent assessors (e.g., Qualified Security Assessors for PCI-DSS and external ISO auditors). Audit results are shared with interested parties, demonstrating compliance efforts.
- **Continuous Improvement** - Node4 communicates its commitment to ongoing improvement in security practices. Interested parties are informed about enhancements, risk mitigation, and lessons learned.