Information Security Policy Statement

Top things to takeaway

Risk Based Security

Protecting information using, risk-based controls

C-I-A

Ensuring information remains secure, accurate and accessible

Security Standards

Certified to ISO 27001 & Cyber Essentials+

Strong Access Controls

Authorised access enforced with strong authentication

Security Monitoring

Detecting incidents and responding through defined processes

Continual Security Improvement

Regularly reviewing and improving security controls

Proprietary Notice

Version control and ownership

Policy owner: Kate Lincoln

Version no	Date	What changed	Changed by	Approver
1.0	09/08/2024	Approved version	Eddie Adams	Kate Lincoln
1.1	12/03/2025	Rebrand	Eddie Adams	Kate Lincoln
1.2	15/04/2026	Rebrand	Eddie Adams	n/a

What is this policy for?

This policy sets out Node4's commitment to protecting information assets and maintaining an effective Information Security Management System (ISMS). It explains how Node4 safeguards information from unauthorised access, tampering, loss, or destruction to support business continuity and reduce the impact of security incidents. The policy also confirms our commitment to meeting applicable regulatory, legislative, and contractual requirements and to maintaining relevant certifications (including ISO 27001, ISO 27017, ISO 27018, Cyber Essentials Plus and PCI DSS), supported by a framework of organisational, people, technical and physical security controls and continual improvement.

Who is this policy for?

This policy applies to Node4 as an organisation and to everyone who works for, or on behalf of, Node4 and may access, handle, or manage Node4 or client information. This includes all employees (including temporary and contract staff) and relevant third parties where applicable. It covers information and supporting systems used to deliver Node4 services within the scope of our ISMS, including the provision of public, private and hybrid cloud solutions, network infrastructure and connectivity solutions, cyber security services, data management solutions and IT Managed Services, and applies across the locations included in the ISMS scope.

Contents

Purpose

Node4 recognises the importance of Information Security, defined as the practice dedicated to safeguarding data from unauthorised access, tampering, or destruction to ensure business continuity and minimise business damage by preventing and reducing the impact of security breaches.

This policy is owned by the Executive Boar to protect Node4's information assets from all threats whether internal or external, deliberate or accidental. It has been written taking into account Node4's strategic plan and the company's attitude to risk. Node4's Information Security Management System is implemented to support this policy and security objectives set.

It is the policy of Node4 to ensure that:

- ISO 27001, 27017 & 27018 is complied with and certification is maintained.
- Cyber Essentials Plus certification is maintained.
- PCI DDS certification is maintained.
- Information is protected against unauthorised access.
- Confidentiality of information is assured.
- Integrity of information is maintained.
- Availability of information is not impacted.
- Regulatory, Legislative and Contractual security requirements are met.
- Information security training is available to staff.
- The Information Security Management System (ISMS) is continuously improved.

As a Cloud Service Provider, Node4's commits to:

- Achieve compliance with applicable PII legislation and contractual terms agreed between the public cloud processor and our clients.
- Establish a baseline of information security requirements applicable to the design and implementation of the cloud service.
- Understand the risks from authorised insiders.
- Maintain multi-tenancy, and cloud service client's isolation, including virtualization.
- Protect access to cloud service client assets.
- Ensure access control procedures, e.g., strong authentication for administrative access to cloud services.
- Ensure communications to cloud service clients during change management.
- Implement virtualization security.
- Ensure access to and protection of cloud service client data.
- Maintain the lifecycle management of cloud service customer accounts.
- Ensure communication of breaches and information sharing guidelines to aid investigations and forensics.

Objectives

Node4's information security objective is to:

- Improve the security of Node4's IT systems along with the information security knowledge and awareness of all users.

In addition to the delivery of our objective plan, Node4 have a number of success indicators for this objective.

Performance to this objective and the objectives plans is reviewed at the quarterly Quality Management Reviews.

Scope

Node4 has committed to maintaining ISO 27001, 27017 and 27018 certification and continually improving the ISMS.

27001

Node4's Information Security Management System (ISMS) covering the provision of public, private and hybrid cloud solutions, network infrastructure and connectivity solutions, cyber security services, data management solutions, and IT Managed Services, in accordance with the ISO 27001:2022 SoA v1.0.

The following ISO 27001 Annex A clause is excluded from Node4's ISO 27001 certification as per our Statement of Applicability:

- A.8.30 – Outsourced development

27017

Node4's Information Security Management System (ISMS) includes the implementation and management of cloud service provider controls as specified in ISO 27017. This applies to our Infrastructure as a Service (IaaS) cloud service offering, 'Virtual Data Centre (VDC)'.

27018

Node4's Information Security Management System (ISMS) includes the protection of Personally Identifiable Information (PII) as specified in ISO 27018. This applies to our Infrastructure as a Service (IaaS) cloud service offering, 'Virtual Data Centre (VDC)'.

Locations

The scope of Node ISMS 27001 covers the following locations:

- **Newbury Office** - Beacon House. Harts Lane, Newbury, RG20 9LJ
- **Derby Office and Data Centre (DC1)** - Node4, Millenium Way, Derby, DE24 8HZ
- **Derby Office and Data Centre (DC2)** - Node4, Millenium Way, Derby, DE24 8HZ
- **Wakefield Office and Data Centre (DC3)** - Unit 1 Normandy Park, Pope Street, Normanton, Wakefield, WF6 2TA
- **Northampton Office and Data Centre (DC4)** - Lower Farm Road, Northampton, NN3 6XF
- **Stafford Offices** – Unit 15 Parker Court, Staffordshire Technology Park, Stafford, ST18 0WP

Security Controls

Organisational

- **Policies** – a suite of Information Security policies are in place and available to all employees via the Intranet site. All policies are reviewed annually or when a change occurs. Employees are required to read key policies as part of their induction.
- **Roles and responsibilities** – roles and responsibilities have been defined and are in place to effectively maintain the Information Security Management System (ISMS) and the confidentiality, integrity and availability of Node4's company and client information.
- **Asset management** – all employees are issued with a company device which is configured and managed via Microsoft Intune, making use of device compliance policies and conditional access. An Acceptable Use Policy is in place which includes guidance the use and misuse of assets as well as working on the move.
- **Information classification** – a classification scheme is in place to ensure our information assets receive protection in line with its classification. Our scheme is enforced on emails and Microsoft documentation to ensure they receive a label.
- **Joiners, movers, leavers (JML)** – a JML process is in place which is triggered by our HR team, ensuring that access is provisioned with appropriate levels of access for employed staff only, access is amended to reflect any role changes and access is revoked upon termination of employment. Access is provisioned in line with the employees' job role and department following the Role Based Access Control principle.
- **Access control** – all employees receive a unique logon and password. We enforce our password policy technically to ensure quality, which is configured in line with NCSC's guidance. Multi-factor authentication is enforced for all accounts.
- **Incidents** – an Incident Response Procedure is in place which defines the activities that should be considered when detecting, analysing, and remediating an incident, along with identifying the key stakeholders who may be required to undertake these specific activities.
- **Business continuity** – A Business Continuity Management System BCMS is in place in line with our ISO 22301 certification. For each planned for disaster scenario, the likely effects on information security have been considered and mitigations built into our Disaster Recovery Plans.

People

- **Screening** – Node4 conduct comprehensive screening of all employees. Screening checks include background checks, credit checks, qualification verifications, previous employment history, and criminal records. All employees undergo a DBS check, while NPPV3 & SC is required for specific roles only.
- **Terms and conditions of employment** – all employees have signed contracts of employment in place which include clauses around information security and confidentiality which last post employment. A Disciplinary procedure in place, which can be invoked as a result of an information security breach.
- **Information security awareness** – all employees complete information security training as part of their induction and receive refresher training annually.
- **Remote working** – An Acceptable Use Policy is in place which provides guidance to all employees on the additionally precautions to be taken when working remotely,

outside of technical controls enforced on end user devices. Additionally, training is also provided on working remotely as part of our training programme.

- **Information security event reporting** – procedures are in place at Node4 to allow for staff to report issues in a timely manner. Training is provided to all employees on how and to whom to report an incident. Incidents are handled by the Compliance team and any other relevant teams that need to be involved.

Technical

- **Systems** – information security requirements for any potential new system or solutions are captured and managed. This ensures that information security is considered before introducing any change that could affect information security.
- **End points** – all Node4 issued mobile computing devices are protected using BitLocker Encryption. If a device is lost or stolen the information contained with the locally cached user policy is encrypted and not readily accessible. All corporate-issued mobile devices within Node4 operate on the Windows platform. To ensure these devices remain up-to-date and secure, a policy for updates has been implemented.
- **Privileged access** – only those who require an administrator account, typically those in technical roles (which are pre-approved by line managers), are granted one. A record is kept of all individuals who have been granted an administrator account. This record, including admin account access, is audited internally by our Quality and Compliance team. All users, including those with admin accounts, have their own unique identity and password to ensure usage can be tracked.
- **Role based access** – access to systems is strictly controlled by Azure Active Directory and based on the principles of least privilege and role-based access. This means that each user is only granted the minimum levels of access necessary to perform their job functions. If a user requires additional permissions for their job role, a request must be made to managed services or the system owner. This ensures that all access is properly authorised and recorded.
- **Secure authentication** – our password management policy is enforced to all users by Azure Active Directory and Microsoft Intune, which is set in line with NCSC guidance. Multi-Factor Authentication (MFA) is enforced through conditional access, and Single Sign-On (SSO) is also configured for added convenience and security.
- **Malware** – Node4 utilises antivirus software, offering robust protection against various online threats. The solution continuously monitors system activities and potential threats, logging all significant events. It alerts users with real-time notifications upon detecting any threat. The solution ensures up-to-date protection by updating its antivirus signatures and database every hour, keeping Node4's systems consistently safeguarded against the newest threats.
- **Firewall** – A software based firewalls is enabled on all end user devices.
- **Vulnerability Management** – Node4 has a comprehensive Vulnerability Management Policy in place which outlines the responsibilities of various teams in monitoring vulnerability trends, performing vulnerability scans, and analysing and remediating the scan results.

- **Incident Management** – we utilise Microsoft Sentinel as a cloud-based Security Information and Event Management (SIEM) solution. This tool allows us to detect, investigate, and respond to security events and incidents in real-time.
- **Backup** – our Backup Policy is in place to identify critical data to be backed up to prevent data loss, specify the backup frequency, detail where backups are stored, how they're tested and responsibilities.
- **Networks** – Node4 has implemented robust firewall systems at our offices to add a line of defence against external threats to the on-premises network. In addition, Node4 utilises a VPN for all remote workers.
- **Encryption** – all internally developed applications at Node4 align with industry best practices, including the use of the latest supported TLS encryption technology. For applications where Node4 utilise third-party services, we strive to ensure that they employ the highest or most appropriate level of encryption based on the work they provide.

Physical

- **Physical security permitters** – all buildings are protected by physical entry controls to ensure only authorised personnel are allowed access. Electronic magnets are installed on external doors and internal doors into offices and data centres which will only release upon presenting a valid key fob. Node4 use Net2 Access Control to manage the door entry system with key cards proximity passes.
- **Physical entry** – all employees are issued with an individually assigned access card. Access levels within Node4 are defined based on staff roles and responsibilities, limiting who requires access to sensitive areas and Data Centres. Additional access levels are in place providing granular access for specific roles.
- **Intruder Alarm** – an intruder alarm system is installed across all Node4 offices and is activated as per close-down routines. Alarm systems are serviced regularly by an approved supplier, ensuring their effectiveness and reliability.
- **CCTV** – all Node4 offices and Data Centres are equipped with CCTV. The purpose of the CCTV system is to ensure a safe and secure environment for our employees, visitors, and customers. CCTV is continuously recording in real-time, 24 hours a day, 7 days a week. CCTV is monitored by the Data Centre Operations, Service Desk, and Reception teams during working hours. Outside of these hours, CCTV alerts are monitored by Security Guards.
- **Security Guards** – outside of normal working hours, security guards are stationed on-site at our Data Centres to monitor CCTV and control site access.
- **Working in secure areas** – all visitor requests must be approved in advance. Visitors are required to sign in upon arrival, wear a visitor lanyard pass, and be escorted by a Node4 staff member at all times. To book a visitor request to Node4 offices a Node4 staff member must make the booking at the relevant office with the receptionist. All visitors are required to sign out at the end of their visit to ensure an accurate record of individuals present is maintained.
- **Clear desk and clear screen** – a policy is in place to ensure that devices are always locked when unattended and workstations are left clear from confidential information.
- **Maintenance** – offices and Data centres have planned maintenance schedules for the year, covering power, cooling, and fire systems. These schedules ensure that all

equipment is maintained to the highest possible standards, preventing damage and mitigating any risks to health and safety. Regular maintenance not only helps to prolong the lifespan of our equipment, but also ensures the reliability and efficiency of our data centres.