NODE4

PUBLIC INFORMATION SECURITY POLICY

Document Classification: Public

Date: 15/08/2023

Node4 Group Integrated Management System

INFORMATION SECURITY POLICY SCOPE

Node4 operates an integrated Information Security Management System (ISMS). The scope of the ISMS includes all Node4 employees to conform to ISO 27001 and ISO 27017 in accordance with the Statement of Applicability (SOA) located at:

- Pride Park in Derby (Office and Data Centre)
- Stadium Court in Derby (Finance and HR Office)
- Normanton in Wakefield (Office and Data Centre)
- Moulton Park in Northampton (Office and Data Centre and Tisski Ltd)
- Beacon House in Newbury (Office and Consultancy Practice)
- Bottle Lane in Nottingham (Office, Database Management Services, Security)

PURPOSE

The purpose of the integrated ISMS is to assess and manage risk and protect the organisation's information security assets from all threats, whether internal or external, deliberate, or accidental.

The ISO 27001 information security objectives of Node4 are to:

- Protect information against unauthorised access.
- Assure the confidentiality of information.
- Maintain the Intergrity of the information.
- Ensure the availability of information as required by the business processes.
- Meet all regulatory and legislative requirements.
- Implement, maintain, and test disaster recovery and business continuity plans in line with the security policy.
- Train all staff on information security on a regular basis.
- Continually review and improve the ISMS.
- Monitor and communicate to interested parties any information received on cyber threats.
- Ensure data is correctly classified.
- Maintain the reputation of Node4 and uphold its ethical and legal responsibilities.
- Respect client's rights, including how to react to enquiries and complaints about non-compliance.

The ISO 27017 and ISO 27018 information security objectives of Node4 as a Cloud provider are to:

- Support for and commitment to achieving compliance with applicable PII legislation and contractual terms agreed between the public cloud processor and its 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 by staff of the cloud service provider.
- 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.

DATA BREACHES

All breaches of information security, actual or suspected, will be reported to and investigated by the Compliance and Security Team, and where applicable, notified to Node4's external Data Protection Officer (DPO). You can contact the DPO at DPO@node4.co.uk

ADDITIONAL POLICIES

Additonal policies and procedures exist to support this Information Security Policy Statement. These include but are not limited to, Node4 Data Protection Policy, Information Security Employee Handbook, physical and logical access controls, network security, malware controls, change, incident, and problem management, vulnerability management, and Disaster Recovery and Business Continuity.

RESPONSIBILITIES

Compliance has direct responsibility for maintaining this policy and providing advice and guidance on its implementation.

A.Gilbert

Andrew Gilbert – CEO

15/08/2023

VERSION CONTROL AND OWNERSHIP

Version No.	Date	What Changed	Changed by
1.1	August 2023	Updated policy to include the integration of Tisski Ltd and extend security controls in accordance with ISO 27017 (Cloud) and ISO 27018 (PII data).	V.Withey