



Empowering business to do more

# Node4 Public Information Security Policy

Integrated Management System

**Policy**

Public

29/03/2022

## Information Security Policy Statement

Node4 operates an Information Security Management System (ISMS) which conforms to ISO27001, 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)
- Imperial Way in Reading (Office)
- Nottingham Bottle Lane (Office, Database Management Services, SOC)

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

The Information Security Objectives of Node4 are to:

- Protect information against unauthorised access
- Assure the confidentiality of information
- Maintain the integrity of the information
- Ensure the availability of information as required by the business processes
- Meet all regulatory and legislative requirements
- Implement, maintain and test DR / BC 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 Limited and uphold its ethical and legal responsibilities
- Respect customer rights, including how to react to enquiries and complaints about non-compliance

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

Additional policies and procedures exist to support the Information Security Policy. These include, but are not limited to, physical and logical access controls, network security, malware controls, change management, vulnerability management and business continuity.

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

All department managers are directly responsible for implementing the policy within their business area. It is the responsibility of all employees to adhere to the policy.



Andrew Gilbert  
CEO  
29/03/2022



Ian Thomas  
COO  
29/03/2022