Node4 Public Information Security Policy Statement ISO27001

PUBLIC

NODE4 LIMITED

08/11/2017

SECURITY POLICY STATEMENT

Node4 operates an Information Security Management System (ISMS) which conforms to ISO27001 at Node4's premises located at

- Pride Park in Derby (Office and Data Centre)
- Normanton in Wakefield (Office and Data Centre)
- Moulton Park in Northampton (Office and Data Centre)
- Imperial Way in Reading (Office)
- New Broad Street in London EC2 (Office)
- Bottle Lane in Nottingham (Office)
- Castle Boulevard in Nottingham (Office)

and is in accordance with the Statement of Applicability v5.n stored on the Node4 Intranet.

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

The Managing Director has approved the information security policy.

This policy and its sub-policies apply to all people, processes, services, Onomi database services, technology and assets detailed in the ISMS Scope. It also applies to all employees or subcontractors of Information Security Critical Suppliers who access or process any of the company's Information Assets.

The Information Security Objectives of Node4 are to:

- Protect information against unauthorised access
- Assure the confidentiality of information
- Maintain the integrity of 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
- Continually review and improve the ISMS
- Ensure controls are implemented that provide protection for information assets and are proportionate to their values and the threats that they are exposed to

All breaches of information security, actual or suspected, will be reported to, and investigated by the Information Security Manager.

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, vulnerability management and business continuity.

The Information Security Manager has direct responsibility for maintaining the policy and providing advice and guidance on its implementation.

Node4 is committed to achieving the objectives detailed in the policy through the following means:

- The implementation and maintenance of an Information Security Management System (ISMS) that is independently certified as compliant with ISO 27001:2013
- The systematic identification of security threats and the application of a risk assessment procedure that will identify and implement appropriate control measures
- Regular monitoring of security threats and the testing/auditing of the effectiveness of control measures
- The maintenance of a risk treatment plan that is focussed on eliminating or reducing security threats
- The maintenance and regular testing of a Business Continuity Plan
- The clear definition of responsibilities for implementing the ISMS
- The provision of appropriate information, instruction and training so that all employees are aware of their responsibilities and legal duties and can support the implementation of the ISMS
- The implementation and maintenance of the sub-policies detailed in this policy

The appropriateness and effectiveness of this policy and the means identified within it for delivering the company's commitments will be regularly reviewed by Top Management.

The implementation of this Information Security Policy and the supporting policies and procedures is fundamental to the success of the business and must be supported by all employees as an integral part of their daily work and all suppliers who have an impact on them. These include, but are not limited to, physical and logical access controls, network security, malware controls, vulnerability management and business continuity.

All breaches of information security, actual or suspected, will be reported to, and investigated by the Compliance Manager.

The Compliance Manager 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 areas, and for adherence by their staff.

It is the responsibility of each member of staff to adhere to the policy.

Andrew Gilbert	Vicky Withey
CEO	Compliance Manager
08/11/2017	08/11/2017