Contents

1. INTRODUCTORY STATEMENT

Netsight Internet Solutions Limited is committed to preserving the confidentiality, integrity and availability of all information assets, both physical and electronic. Our company recognises that an Information Technology / Information System (ISMS) aligned with our company goals is an enabling mechanism that plays a major role in our business activities.

We expect that the data in our possession, and the infrastructure that handles it, must be kept secure. A breakdown in security could have serious effects on our business. Any breach could result in a direct financial loss, a loss of confidence, or a breach of legal and/or regulatory requirements. For these reasons, the Board of Directors has approved the production and company-wide implementation of our Information Security Policy and programme.

Our company's Policy, as outlined below, establishes standards that represent the minimum-security requirements that apply to all our information systems and the processes that support them. It also gives important responsibilities to managers, who must ensure compliance within their areas of control. This will ensure that there is a correct balance between the objectives of creating and maintaining an open, trusting environment in which information, with limited exceptions, is made freely available to all employees, while protecting our data from accidental or deliberate loss, alteration, or disclosure.

It is essential that this Policy is fully implemented and that all employees are aware of their responsibilities regarding the protection of data and systems against unauthorised access or disclosure. All employees are therefore required to comply with this policy and with the Information Security Management System (ISMS) that supports this policy. The Board of Directors therefore asks that each employee reads this document and directs any questions to a line manager.

Signed: (Ben Ackland, Projects Director)

For and on behalf of the Netsight Board of Directors

2. POLICY

The principal focus of Netsight's Information Security Policy is to provide the following:

- **Confidentiality**: maintaining the restriction of access to information by authorised persons, entities and processes at authorised times and in an authorised manner;
- **Integrity**: safeguarding the accuracy and completeness of information and information processing systems; and
- **Availability**: ensuring that authorised users have access to information and associated assets when required.

The purpose of this Policy is to protect the organization's information assets[1] from all threats, whether internal or external, deliberate or accidental.

The Board of Directors has approved this policy and delegated the responsibility for writing, managing and implementing any related policies to the Information Security Management Group (ISMG).

It is the Policy of our company to ensure that:

- Information should be made available with minimal disruption to staff and the public as required by the business process.[2]
- The integrity of this information will be maintained.[3]
- Confidentiality of information not limited to research, third parties, personal and electronic communications data will be assured.[4]
- Regulatory and legislative requirements will be met.[5]
- A Business Continuity Framework shall be made available and Business Continuity plans will be produced to counteract interruptions to business activities and to protect critical

---

[1] Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, stored on tapes, USB, or spoken in conversation and over the telephone.

[2] This policy element will ensure that information and vital services are available to users when and where they need them.

[3] Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.

[4] The protection of valuable or sensitive information from unauthorised disclosure or unavoidable interruptions.

[5] This policy element will ensure that the company remains compliant to relevant business, national and international laws and it include meeting the requirements stated in legislations such as the Companies Act and the Data Protection Act.

business processes from the effects of major failures or disasters. Business continuity plans are to be maintained and tested.[6]

- Information security education, awareness and training will be made available to staff.[7]
- All breaches of information security, actual or suspected, will be reported to and investigated by the relevant authorities not limited to System Administration and Incident Response team.[8]
- Appropriate access control will be maintained and information protected against unauthorised access.

The Board of Directors has direct accountability for maintaining the ISMS Policy and has appointed the Information Security Management Group (ISMG) to write and manage relevant policies, procedures and guidelines to support the ISMS policy.

All Directors are directly responsible for implementing the ISMS Policy within their areas of the business, and for adherence by their staff. For sample purposes only, some Policies, Procedures and Guidelines not limited to Information Security will be made available online to support the ISMS Policy.

It is the responsibility of each member of staff to adhere to the ISMS Policy.

Information security is managed through the company's Risk Management framework.

The availability of information and information systems will be met as required by the core and supporting business operations.

Internal Audit shall assess compliance with this ISMS policy and system (Internal Audit is outsourced to a third party).

---

[6] Business Continuity Management should be implemented effectively to ensure continuity of business operations in the event of a crisis or disaster.

[7] This policy element will ensure that relevant and effective trainings are provided to staff.

[8] This policy element will ensure that all employees understand their roles and responsibilities in handling incidents and have a comprehensive and well-tested incident response plan ready.

3. Document History

Revisions:				
Version	Status:	Date:	Author:	Comments
0.01	Draft	21 July 2014	Thom Bunting, Jason Parker-Smith	For review by the Board of Directors
1.0	Approved	22 July 2014	Thom Bunting	Includes minor adjustments requested during Netsight Board of Directors meeting on 22 July 2014.
1.01	Approved	26 September 2014	Thom Bunting	Minor formatting changes, for consistency with other documentation.