

# Information Security Policy Statement

Significant advancements in information and communication technology have radically increased the ease with which data may be collected, transmitted, stored and / or disseminated. Such developments – together with an increased awareness of fundamental rights – have led to legislative changes and the emergence of a new data protection regime.

In light of the General Data Protection Regulation’s (“GDPR”) implementation on 25 May 2018, Nomad Digital (“ND”) reinforces its ongoing commitment to privacy and data protection, and to ensuring that its technical and organisational policies, procedures and practices employ a data protection by design and by default approach from the earliest possible opportunity.

ND encourages all staff to ensure that privacy and data protection is a key consideration in the early stages of any project, and throughout its lifecycle. ND regards its privacy by design and by default approach to be integral to minimising privacy risks and building trust.

Information Security is an integral part of ND’s strategy to become a global leader in information and communication technology, by expanding its activities to new markets and geographies. ND regards Information Security as being fundamental to maintaining its position as an industry leader, and it is committed to safeguarding the confidentiality, integrity and availability of all physical and electronic information assets.

## Scope

- To minimise the financial and reputational impact following any Information Security incident, and to safeguard all company assets, including employees, intellectual property, physical equipment and business / customer information from all threats, whether internal / external, deliberate or accidental
- To cover all ND staff –whether an employee, contractor or otherwise – operating on ND’s behalf worldwide
- To integrate with existing ND policies and procedures, and corporate governance to ensure compliance with legal, statutory and corporate obligations

## Policy Statement

All staff must adhere to ND’s Information Security policies and procedures in order to understand the requirements and expectations placed on them as professionals working for ND.

ND strives to ensure the confidentiality, integrity and availability of company, customer and personal data at all times. Confidentiality refers to limiting information access and disclosure to unauthorised users. Integrity refers to the trustworthiness of information resources; namely, that data has not been changed inappropriately.

Availability of information resources is the assurance that the systems responsible for delivering, storing and processing information are accessible when needed and by those who need them. We ensure:

- All regulatory and legislative requirements are met
- All contractual obligations are met
- Security incident response plans are in place, maintained and tested
- Information security training will be available to all ND staff
- Information security breaches, whether actual or suspected, are reported, logged and investigated

- A steering committee will convene on a quarterly basis to review the implementation of ND's Information Security Management System ("ISMS"), discuss security improvement initiatives and compliance, and a formal management review with ND's Executive Group will take place at least annually to make sure that it remains appropriate for the business

## Responsibilities

- **Managing Director** - Overall policy ownership and provision of appropriate resources to mitigate any associated risks
- **Executive Group** - Regularly review the ISMS and its applicability to the business
- **Senior Leadership Team** - Information ownership / accountability within their areas of responsibility
- **Steering Committee** - Lead ND's data protection by design and by default approach, implementation of the ISMS and security initiatives, improve ND's security awareness and compliance across the business
- **Information Security Officer** - Management and continuous improvement of the ISMS and Information Security Compliance
- **In-House Lawyer** - Assisting ND's Information Security Officer in ensuring that all legal, regulatory and contractual obligations are met
- **Staff** - Comply with all Information Security policies and procedures and be aware of potential disciplinary action that may result if they do not. Attend Information Security induction sessions, complete training modules and acknowledge understanding

## Governance

This Policy is fully integrated with the groups Business Management System and is underpinned by specific Information Security policies, procedures and standards. It reflects the current business aspirations and the risk appetite of ND globally, and will be reviewed and updated on a two yearly basis, or following any significant business or regulatory changes.