INFORMATION SECURITY POLICY

Nomadix is committed to maintaining our reputation for deploying stable, robust, scalable, and future-proofed internet and in-room entertainment solutions. We work together to ensure that our software, services and solutions, and operational processes minimize risks to the confidentiality, integrity, and availability of our customers' and Nomadix's information and IT systems.

To identify and manage these risks, and provide assurance that we are following best practices for information security, we are implementing a combination of technical and operational security initiatives. These include establishing an Information Security Management System (ISMS), based on international best practises for information security (IS027001).

The Nomadix ISMS has been designed, implemented, and operated to achieve the following objectives:

- Demonstrate senior management commitment to protecting our customers' and Nomadix's information, by aiming for a full accredited certification to IS027001:2013 by 2023.
- Comply with legislative requirements for information protection.
- Deliver stable solutions which minimize cyber security and operational risks.
- Comply with customer requirements for information security.
- Identify and minimize risks in our supply chain.
- Protect customer and Nomadix information from unnecessary access, modification or loss by identifying and managing risks through the use of policies, processes, and controls that are regularly audited.
- Provide information security training to all our staff on an ongoing basis.
- Implement scalable systemized processes that support Nomadix's growth strategy.
- Continually review and improve our security.

All staff, and where appropriate suppliers, are required to comply with the Nomadix ISMS and supporting policies. Non-compliance may lead to disciplinary action or the termination of supplier contracts.

Information Security Responsibilities

- The Group Chief Information Security Officer (GCISO) is responsible for the implementation and management of the ISMS, including reporting upon its effectiveness to the Global Management Team (GMT).
- The Information Security Team oversees the implementation and management of security controls.
- Information asset / risk owners are responsible for identifying and classifying their information and addressing risks. Managers at all levels are responsible for complying with our information security controls and ensuring their team's adherence.
- All staff including temporary workers contractors, and where appropriate, third parties are responsible for complying with our information security policies
- Compliance with our ISMS and information security controls will be regularly assessed by qualified third-party practitioners.

Cyber Essentials

In addition Nomadix has undertaken a commitment to hold a full Cyber Essentials certification as backed by the UK Government. Covering five main security control groups: firewalls and routers, software updates and patching, malware protection, access control, and secure configuration.

Security Management

- Information assets will be identified, assessed for risk and appropriately protected.
- Risk escalation processes will be implemented.
- Security policies covering IT systems, personnel security, facilities, supply chain assurance, business continuity and the collection, use sharing, retention and disposal of information will be implemented and adhered to.
- Information security training will be available to all staff, including temporary workers and contractors.
- All actual or suspected breaches of information security will be reported to and investigated by the Group Chief Information Security Officer.
- Compliance to our ISMS and information security controls will be regularly assessed.

For further Information on this policy please contact the Group Chief Information Security Officer Dr Chris Spencer (D.Sc.).

Signed: C. Spencer

Dated: 7th FEB 2022