nordic
entertainment group

Information Security Approach

Document owner	Information Security Officer
Approval	Head of IT & Information Security
Date last approved	17 June 2021
Effective from date	17 June 2021
Date of next review	Q2 2022
Access level	Public information

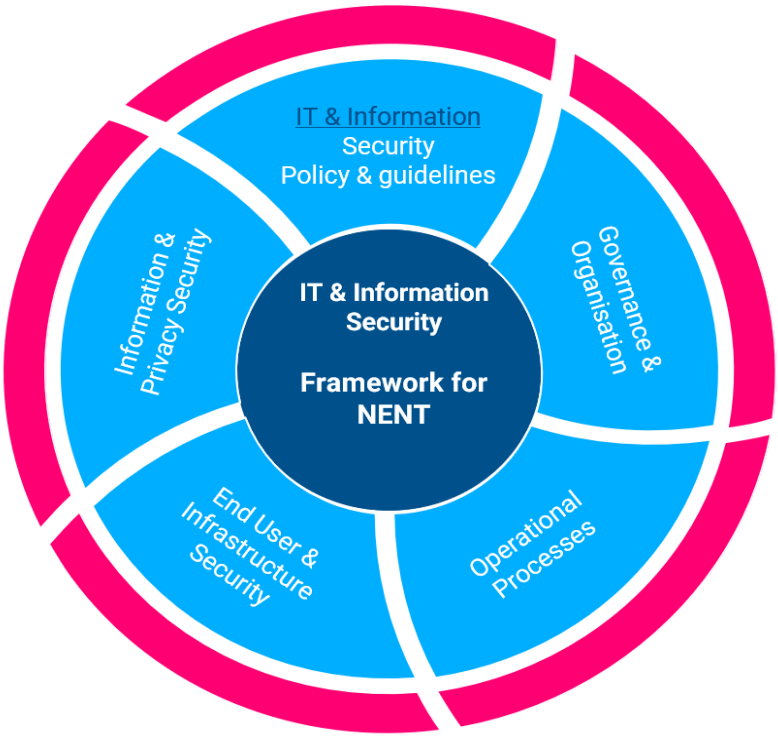
Information Security Management System - ISMS

The NENT Group information security management system, ISMS, is a governance and Audit model that combines the organisations specific information security prerequisites with the formal controls and audit areas.

This includes identifying information and assets - whether defined by law or in agreements or by NENT group - in addition to the consequences of an information security incident and suitable security controls to reduce risk.

1. Areas

The NENT ISMS, information security management system is divided into areas. Each area has corresponding guideline documents and instructions that sets out more detailed requirements:



- IT & Information Security Policy & Guidelines
- Governance & Organization
- Operational Processes
- End User & Infrastructure
- Information & Privacy Security

2. IT & Information Security Statement

We protect the organization's IT & Information Assets for our Customers, Business, and Employees according to applicable legislation. It is necessary to do so, to achieve the business goals and for customers, partners and employees to feel confident in us. We work actively with information security to secure all our information is accessible to those who are to access it, secured from malicious access and reliable for all who uses it.

We have chosen a common and structured way of working with information security that is based on the Industry Standard; ISO 27000 and underlying components. The framework is documented and accessible to all needing it, it is our IT & Information Management System, ISMS, this includes Internal Security Rules and Guidelines to secure our IT and Information Assets at all time.

With the support of our ISMS we get the right level of both IT & Information security in connections to our Customers Agreements, our Business Processes and the information in relations to our employees.

The Management of the ISMS is delegated to our Information Security Officer, whose mission is to make sure our work with IT & Information security is long-term and continuous, covering all parts of our business and its IT & information assets.

The Continuous work is manage this through our IT & Information Security Program were we assess our security Controls and risks, and document and mitigate gaps. The staff receives awareness training to understand the ISMS impact on their role.

Everyone has a responsibility to ensure that IT & Information is securely managed according to our Policy & Guidelines. Anyone who discovers deficiencies in applications or infrastructure shall report this as an Incident according to our established processes. All employees must also report incidents that could expose our information assets to risks.