

Document ControlReference: [ISMS Doc 5.2](#)

Issue No: 1

Issue Date: 28th January 2022

Total Pages: 4

Servebolt Information Security Policy

Purpose

Servebolt AS's strategic purpose is to deliver secure, fast, stable and scalable green internet hosting infrastructure. As our core business depends on the storage and processing of sensitive data, it is our board and management's duty that this information be protected appropriately.

The growing sophistication of data security threats makes necessary a stringent Information Management Security System (ISMS) and the governance it outlines. This ensures our compliance with legal and regulatory obligations; that we meet contractual obligations and the requirements of stakeholders to ensure continued confidence of our customers, employees, partners and suppliers; and to ensure our continued productivity and profitability.

Policy Statement

The Board of Directors and management of Servebolt AS are committed to preserving the confidentiality¹, integrity² and availability³ of our information assets⁴.

¹ Confidentiality is [defined as the] property that information is not made available or disclosed to unauthorized individuals, entities or processes in ISO 27000:2018, Clause 3.10.

² Integrity is [defined as the] property of accuracy and completeness in ISO 27000:2018, Clause 3.36.

³ Availability is [defined as the] property of being accessible and usable upon demand by an authorized entity in ISO 27000:2018, Clause 3.7.

⁴ The complete information asset register of Servebolt can be accessed [here](#).



Our commitment and purpose provide the strategic context for our ISMS, within which our risk management plan is established. The risk management plan provides the framework for identifying, evaluating, analyzing and controlling information security-related risks, through the establishment and maintenance of Servebolt's ISMS.

In particular, the Risk Assessment plan sets a framework for identifying the information assets critical to Servebolt's strategic purpose⁵, and evaluating these, in the context of the security objectives of confidentiality, integrity, and availability, and on the basis of Servebolt's risk acceptance criteria. These criteria are based on Servebolt's customer confidence, critical business drivers, financial security and profitability, technical security, organizational productivity, and legal and regulatory requirements.

The Statement of Applicability and Risk Treatment plan analyze how the evaluated information-related risks are controlled, based on Servebolt's criteria for control. Control objectives are supported by the specific documents and procedures in the Security Policies & Process manual, which is available to all who fall within the scope of the ISMS. All who fall within the scope of the ISMS are given the necessary training and support for implementing our control objectives appropriately.

The procedures resulting from the ISMS ensure that the ISMS itself is subject to continuous, systematic review and improvement in line with the evolution of our objectives.

Policy Requirements and Benefits

The implementation of this policy will require significant financial, people and time resources to implement. It will require significant documentation and the training of both existing and future employees.

Servebolt's resource investment will provide us with a structured way of addressing information security issues which will become part of our product offering itself. It will increase our stability, scalability, security and the quality of our service. This will make our services relevant to a larger market. It will simplify our communication internally and externally with regards to information security, and be a professional driver, increasing competence and the quality of our operations and company culture.

⁵ Other assets falling outside of the scope of critical to purpose are still covered by the Risk Assessment process at this time.



Applicability

Servebolt's information security policy and ISMS applies to the entire organization, our employees and contractors, our data centers globally, and our internal and external IT systems and processes.

In particular, servers and services supporting critical business processes, customer-facing services (production data), customer-facing production applications, non-production data, internal systems and support infrastructure, network and security devices, employee data, internal intellectual property, financial data, physical devices such as laptops and mobile phones, and physical facilities are of special importance to Servebolt's security policy.



Signatures

Ragnar Bø

Ragnar Bø
Chair of the Board

Jan Wan

JAN WAN

Board member

Erlend Eide

Erlend Eide

Board member and CEO