Document Owner	Group CFO
Document Holder	Group CFO
Approval	Board of directors of Bentley Endovascular Group AB (publ)
Date of Approval	2025-04-29

Information Security Policy

Bentley Endovascular Group AB (publ)

TABLE OF CONTENTS

1. Introduction....3
2. Purpose....3
3. Scope....3
4. Principles....3
5. Roles and responsibilities....4
6. Overall objectives and requirements....5
7. Compliance....7
8. Associated Documents....7

1. INTRODUCTION

Bentley Endovascular Group AB (publ) (hereinafter “Company”; Bentley Endovascular Group AB (publ) as well as its subsidiaries hereinafter “Bentley”, the “Group” or “we”) is an international medical technology company with headquarters in Sweden and global subsidiaries.

Bentley is committed to preserving the Confidentiality, Integrity, and Availability of all the physical and electronic Information Assets throughout the organization. This Policy describes and records Bentley’s approach towards managing information security and supplemented by Group entity level Instructions and SOPs. Information security shall be applied to all of Bentley’s business processes.

2. PURPOSE

The board of directors (the “**Board**”) of Bentley Endovascular Group AB (publ) (has adopted this Policy in relation to the Group’s Information Security (the “**Policy**”).

The purpose of this Policy is to ensure that the management, control and governance of information security, including Confidentiality, Integrity and Availability, is efficient. All Bentley’s Information Assets must be protected from unauthorized use or change and are available for an efficient use throughout their lifecycle. Strategic decisions related to information security shall always be approved by the Group CFO.

3. SCOPE

The Policy applies to all permanent and temporary employees of the Company (including any of its intermediaries, subsidiaries or associated companies). It also applies to any individual or corporate entity associated with the Company or who performs functions in relation to, or for and on behalf of, the Company, including, but not limited to, directors, agency workers, casual workers, contractors, consultants, and suppliers. All employees and associated persons are expected to adhere to the principles set out in this Policy.

4. PRINCIPLES

4.1.1 Bentley’s framework for implementation and management of information security consists of:

- This Policy and the Group Data Privacy Policy
- Group Business Continuity Policy, supplemented by Group and entity level plans and BIA
- IT Access and Change management instructions, at the Group (if applicable) and entity level adhering to Bentley’s policies

- Standard Operating Procedures (SOPs)/IT Handbook detailing the policies and instructions, established at Group and/or Entity level adhering to Bentley's policies.

4.2 Ultimate responsibility for this Policy rests with the Board, but Policy rests with the Group CFO, who is also the Document holder/owner. This Policy shall be reviewed at least annually for any necessary updates. As Bentley's business and regulatory requirements are constantly changing, it is important for the Group CFO to ensure that this Policy as well as instructions under it are regularly updated. The Group CFO is responsible for maintaining appropriate documentation of any changes to the Policy.

4.3 This Policy applies to all employees, consultants, contractors, and other third-party users involved in any way with the application, design, development and support of Bentley's Information Assets. Compliance with this Policy is both an individual and a corporate responsibility. It is the responsibility of the managers to ensure that employees and consultants are made aware of this Policy.

5. ROLES AND RESPONSIBILITIES

Roles	**Responsibilities**
Board	• Approves the Information Security Policy.
Group CEO	• Strategic responsibility and escalation of items from the Group CFO.
Group CFO	• Overall responsibility for the Policy and the supporting instructions (Document Owner). • Responsible for conducting regular assessment to measure the status of implementation and provide guidance to business areas to improve maturity based on the business needs and risk exposures. • Responsible for proposing updates to the Policy and documenting such changes in the policy (as Document Holder). • Approval of Group level guidelines & instructions under this Policy, if required. • Reports to Group CEO & Board.
IT manager/Head of IT	• Operational responsibility for the Policy and the supporting instructions as well as SOPs/IT Handbook

	• Approval of entity level instructions/SOPs/IT Handbook under this Policy. • Overall responsibility for implementing as well as testing SOPs/instructions/ IT Handbook on entity level. • Implement appropriate information security awareness training and education for employees. • Responsible for ensuring that the relevant Information Asset meets relevant and sufficient requirements for Confidentiality, Integrity, and Availability. • Defining the information security requirements for IT Systems based on risk and vulnerability assessments and classifications made by the system owner. This includes the classification of the respective Information Assets and thus the determination of the applicable security level. • Overall responsibility for incident management and IT business continuity in relation to Information Assets. • Report serious or repeated Information security Incidents for the Entity to the local CEO and/or Group CFO. • Responsible for ensuring that IT Systems and Information Assets comply with regulatory requirements relating to information security.
Employees, contractors and external parties	• Each employee and contractor are responsible for complying with this Policy and its supporting instructions and SOPs.

6. OVERALL OBJECTIVES AND REQUIREMENTS

6.1 General

The information security measures implemented hereunder shall be subjected to ongoing risk and vulnerability assessments.

This Policy requires that information security control objectives, principles and processes are consistently defined and applied in the design, development, and operation of Bentley's business, IT Systems and Information Assets. Bentley shall also ensure that information security measures are implemented to protect the privacy of individuals as required by personal data laws and further elaborated in Bentley's Data Privacy Policy.

6.2 Asset management and information classification

All Information Assets shall be categorized based on the required security and business criticality following a risk and vulnerability assessment. Information Assets shall be protected with an appropriate level of protection, including consideration of relevant legislation, such as data privacy protection regulations (subject to the Group Data Privacy Policy). Such evaluation shall be done in the form of a risk and vulnerability assessment.

6.3 Human resources

Appropriate functions shall be in place to ensure that the information security roles of employees, consultants, contractors and other third-party users are clearly defined and monitored.

Ongoing training shall be provided to all relevant resources to ensure appropriate information security practices and controls prior to granting access to Information Assets and for the performance of high-risk tasks.

6.4 Physical and environmental security

The IT Systems used by Bentley, together with all other relevant infrastructure and facilities, shall be adequately protected against both external and internal threats. IT Systems, infrastructure and facilities shall be well-maintained and serviced throughout their useful life.

Appropriate access control measures, shall be implemented to protect IT systems, including infrastructure and facilities.

6.5 Communications and operations

Appropriate safety measures shall be implemented based on the risk, including but not limited to encryption, logs, firewalls and backups of data and other Information Assets. All Information Assets and data of Bentley shall thus be backed up with frequency and security as required depending on the sensitivity of the Information Assets/data. Data shall be stored and subject to back-up during a period as required by business needs and as required by regulatory requirements.

6.6 Access control

Refer to IT Policy

6.7 Life Cycle Management

Information security shall be an integral part of the Life cycle of Information Assets. Applications and IT Systems shall be continuously tested for potential risks from internal and external threats.

6.8 Incident management

Refer to IT Policy

7. COMPLIANCE

To fulfil this Policy, Bentley intends to comply with all relevant legislation relating to, for example information security, data protection, protection of intellectual property rights etc.

Functions shall be in place to monitor Bentley’s compliance on an ongoing basis and to identify new and changing requirements due to e.g. changes in legislation, new case law and decisions from public authorities/regulatory decisions.

8. ASSOCIATED DOCUMENTS

- Data Privacy Policy
- IT Policy

* * * *

APPENDIX DEFINITIONS

Availability

means that the Information Assets and IT Systems are available to authorized users at relevant times and to the extent the Information Assets or IT Systems are needed.

Confidentiality

means that Information Assets that are stored, processed, transported and/or communicated shall be protected from unauthorized users and disclosure.

Information Asset

means all data which has value to the organization. Information Assets refer to and include data found or used in Bentley's business environment. These assets may include information technology, systems & infrastructure, people & processes, customer & employee personal information, and/or business critical information.

Integrity

means that Information Assets and IT Systems shall be protected from manipulation and unauthorized change.

IT System

means hardware, software and firmware of computers, telecommunications and network equipment or other electronic information handling systems and associated equipment.

Life cycle

All times in a life of an IT System. From the initial requirements to its final shutdown and dissembling. Other points in life of an IT System are for example design, specification, programming, testing, installation, operation and maintenance.

SOP

Standard Operating Procedure, providing details and checklists for IT Systems and Information Assets.