Besitzer des Dokuments	Group CFO
Dokumentenhalter	Group CFO
Genehmigung	Verwaltungsrat der Bentley Endovascular Group AB (publ)
Datum der Genehmigung	2025-04-29

Information Security Policy

Bentley Endovascular Group AB (publ)

(Richtlinie zur Informationssicherheit)

INHALT

1. Einleitung 3
2. Zweck 3
3. Anwendungsbereich 3
4. Grundsätze 3
5. Rollen und Verantwortungsbereiche 4
6. Ziele und Anforderungen 5
7. Compliance 7
8. Verknüpfte Dokumente 7

1. EINLEITUNG

Die Bentley Endovascular Group AB (publ) (nachfolgend das „**Unternehmen**"; gemeinsam mit ihren Tochtergesellschaften nachfolgend auch „**Bentley**“, die „**Gruppe**" oder „**wir**") ist ein international tätiges Medizintechnikunternehmen mit Hauptsitz in Schweden und weltweiten Tochtergesellschaften.

Bentley hat sich verpflichtet, die Vertraulichkeit, Integrität und Verfügbarkeit aller physischen und elektronischen Informationswerte im gesamten Unternehmen zu wahren. Diese Richtlinie beschreibt und dokumentiert Bentleys Ansatz zum Management der Informationssicherheit und wird durch Anweisungen und SOPs auf Ebene der Tochtergesellschaften ergänzt. Die Informationssicherheit wird auf alle Geschäftsprozesse von Bentley angewendet.

2. ZWECK

Der Verwaltungsrat der Bentley Endovascular Group AB (publ) (im Folgenden das „**Board**“) hat diese Information Security Policy (im Folgenden „**Richtlinie**“) angenommen.

Mit dieser Richtlinie soll sichergestellt werden, dass die Verwaltung, Kontrolle und Steuerung der Informationssicherheit, einschließlich Vertraulichkeit, Integrität und Verfügbarkeit, effizient ist. Alle Informationswerte von Bentley müssen vor unbefugter Nutzung oder Veränderung geschützt werden und während ihres gesamten Lebenszyklus für eine effiziente Nutzung verfügbar sein. Strategische Entscheidungen im Zusammenhang mit der Informationssicherheit müssen stets vom Group CFO genehmigt werden.

3. ANWENDUNGSBEREICH

Diese Richtlinie gilt für alle unbefristet oder befristet beschäftigten Mitarbeitenden des Unternehmens (einschließlich etwaiger Vermittler, Tochtergesellschaften oder verbundenen Unternehmen). Sie gilt ebenso für jede natürliche oder juristische Person, die mit dem Unternehmen in Verbindung steht oder Funktionen im Zusammenhang mit dem Unternehmen oder in dessen Namen bzw. Auftrag ausübt. Dazu zählen unter anderem Mitglieder des Boards, Zeitarbeitskräfte, Aushilfen, Auftragnehmer, Berater und Lieferanten. Alle Mitarbeitenden und verbundenen Personen haben die in dieser Richtlinie dargelegten Grundsätze zu befolgen.

4. GRUNDSÄTZE

4.1 Bentleys Rahmen für die Implementierung und Verwaltung der Informationssicherheit besteht aus folgenden Elementen:

- Diese Richtlinie und die Data Privacy Policy.
- Business Continuity Policy, ergänzt durch Pläne auf Unternehmensebene und der Ebene der Tochtergesellschaften und BIA.
- Anweisungen für die IT-Zugangs- und Änderungsverwaltung auf Unternehmensebene (falls zutreffend) und Ebene der Tochtergesellschaften unter Einhaltung der Bentley Policies.
- Standardarbeitsanweisungen (SOPs)/IT-Handbuch mit detaillierten Richtlinien und Anweisungen, die auf Unternehmensebene und der Ebene der Tochtergesellschaften unter Einhaltung der Bentley Policies eingeführt wurden.

4.2 Die letztliche Verantwortung für diese Richtlinie liegt beim Board, die operative Zuständigkeit wird aber vom Group CFO wahrgenommen, der auch Dokumentenhalter ist. Die Richtlinie ist mindestens einmal jährlich auf notwendige Aktualisierungen zu überprüfen. Da sich Bentleys Geschäftstätigkeit und die regulatorischen Anforderungen laufend verändern, ist es von zentraler Bedeutung, dass der Group CFO sicherstellt, dass diese Richtlinie sowie die dazugehörigen Anweisungen regelmäßig aktualisiert werden. Der Group CFO ist für die ordnungsgemäße Dokumentation sämtlicher Änderungen dieser Richtlinie verantwortlich.

4.3 Diese Richtlinie gilt für alle Mitarbeitenden, Berater, Auftragnehmer und andere Drittnutzer, die in irgendeiner Weise mit der Anwendung, dem Entwurf, der Entwicklung und der Unterstützung der Informationswerte von Bentley zu tun haben. Die Einhaltung dieser Richtlinie liegt sowohl in der Verantwortung des Einzelnen als auch in der des Unternehmens. Es liegt in der Verantwortung der Führungskräfte, dafür zu sorgen, dass Mitarbeitende und Berater mit dieser Richtlinie vertraut gemacht werden.

5. ROLLEN UND VERANTWORTUNGSBEREICHE

Rolle	Verantwortungsbereich
Board	• Genehmigt die Information Security Policy.
Group CEO	• Trägt die Verantwortung für die Strategie und eskalierten Anliegen des Group CFO.
Group CFO	• Gesamtverantwortung für die Richtlinie und die zugehörigen Anweisungen (Dokumentenhalter) • Führt regelmäßige Bewertungen zur Umsetzung durch und unterstützt Unternehmensbereiche bei der Entwicklung basierend auf Geschäftsanforderungen und Risiken. • Verantwortlich für die Aktualisierung der Richtlinie und deren Dokumentation (als Dokumentenhalter). • Genehmigt gruppenweite Richtlinien und Anweisungen gemäß dieser Richtlinie, falls notwendig. • Berichtet an Group CEO und Board.
IT Manager/Head of IT	• Operative Verantwortung für die Richtlinie und die unterstützenden Anweisungen sowie SOPs/IT-Handbuch. • Genehmigung von Anweisungen/SOPs/IT-Handbuch der Tochtergesellschaften gemäß dieser Richtlinie.

	• Gesamtverantwortung für die Umsetzung und das Testen von SOPs/Anweisungen/IT-Handbüchern der Tochtergesellschaften. • Durchführung geeigneter Schulungen für die Informationssicherheit und Aufklärung der Mitarbeitenden. • Verantwortlich für die Sicherstellung, dass der betreffende Informationswert die relevanten und ausreichenden Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit erfüllt. • Festlegung der Informationssicherheitsanforderungen für IT-Systeme auf der Grundlage von Risiko- und Schwachstellenbewertungen und Klassifizierungen durch den Systemeigentümer. Dazu gehört auch die Klassifizierung der jeweiligen Informationswerte und damit die Festlegung der anwendbaren Sicherheitsstufe. • Gesamtverantwortung für das Störungsmanagement und die IT-Geschäftskontinuität in Bezug auf Informationswerte. • Meldung schwerwiegender oder wiederholter Vorfälle im Bereich der Informationssicherheit für die Tochtergesellschaft an den local CEO und/oder den Group CFO. • Verantwortlich für die Sicherstellung, dass die IT-Systeme und Informationswerte den gesetzlichen Anforderungen an die Informationssicherheit entsprechen.
Mitarbeitende, Vertragspartner und externe Parteien	• Alle Mitarbeitenden und jeder Auftragnehmer sind für die Einhaltung dieser Richtlinie und der zugehörigen Anweisungen und SOPs verantwortlich.

6. ZIELE UND ANFORDERUNGEN

6.1 Allgemein

Die in diesem Rahmen durchgeführten Maßnahmen zur Informationssicherheit werden einer ständigen Risiko- und Schwachstellenbewertung unterzogen.

Diese Richtlinie verlangt, dass Ziele, Grundsätze und Prozesse zur Informationssicherheit bei der Konzeption, Entwicklung und dem Betrieb der Geschäftsabläufe, IT-Systeme und Informationswerte von Bentley einheitlich definiert und angewendet werden. Bentley stellt außerdem sicher, dass Maßnahmen zur Informationssicherheit zum Schutz der Privatsphäre von Personen gemäß den Datenschutzgesetzen und den weiteren Ausführungen in der

Datenschutzrichtlinie von Bentley umgesetzt werden.

6.2 Management und Klassifizierung von Informationswerten

Alle Informationswerte sind nach einer Risiko- und Schwachstellenanalyse entsprechend der erforderlichen Sicherheit und geschäftlichen Bedeutung zu kategorisieren. Informationswerte sind mit einem angemessenen Schutzniveau zu versehen, wobei auch die einschlägigen Rechtsvorschriften, wie z.B. die Datenschutzbestimmungen (vorbehaltlich der Datenschutzrichtlinie der Gruppe), zu berücksichtigen sind. Diese Bewertung erfolgt in Form einer Risiko- und Schwachstellenanalyse.

6.3 Human Resources

Es müssen geeignete Funktionen vorhanden sein, die sicherstellen, dass die Rollen der Mitarbeitenden, Berater, Auftragnehmer und anderer Drittnutzer im Bereich der Informationssicherheit klar definiert und überwacht werden.

Alle relevanten Ressourcen werden fortlaufend geschult, um angemessene Informationssicherheitspraktiken und -kontrollen zu gewährleisten, bevor Mitarbeitenden der Zugang zu Informationswerten und die Durchführung von Aufgaben mit hohem Risiko gewährt werden.

6.4 Physische und umgebungsbezogene Sicherheit

Die von Bentley genutzten IT-Systeme sowie alle anderen relevanten Infrastrukturen und Einrichtungen müssen angemessen gegen externe und interne Bedrohungen geschützt sein. IT-Systeme, Infrastruktur und Einrichtungen müssen während ihrer gesamten Nutzungsdauer gut gewartet und instandgehalten werden.

Zum Schutz der IT-Systeme, einschließlich der Infrastruktur und der Einrichtungen, sind geeignete Zugangskontrollmaßnahmen zu ergreifen.

6.5 Kommunikation und Betrieb

Je nach Risiko sind geeignete Sicherheitsmaßnahmen zu ergreifen, einschließlich, aber nicht beschränkt auf Verschlüsselung, Protokolle, Firewalls und Backups von Daten und anderen Informationswerten. Alle Informationswerte und Daten von Bentley müssen daher mit der erforderlichen Häufigkeit und Sicherheit gesichert werden, die von der Sensibilität der Informationswerte/Daten abhängt. Die Daten werden so lange gespeichert und gesichert, wie es die geschäftlichen Erfordernisse und die gesetzlichen Vorschriften verlangen.

6.6 Zugangskontrolle

Siehe IT-Policy

6.7 Lebenszyklus-Management

Die Informationssicherheit muss ein integraler Bestandteil des Lebenszyklus von Informationswerten sein. Anwendungen und IT-Systeme sind kontinuierlich auf potenzielle Risiken durch interne und externe Bedrohungen zu testen.

6.8 Management von Zwischenfällen

Siehe IT-Policy

7. COMPLIANCE

Um diese Richtlinie zu erfüllen, beabsichtigt Bentley, alle einschlägigen Rechtsvorschriften einzuhalten, die sich beispielsweise auf die Informationssicherheit, den Datenschutz, den Schutz der Rechte an geistigem Eigentum usw. beziehen.

Es müssen Funktionen vorhanden sein, um die Einhaltung der Vorschriften durch Bentley kontinuierlich zu überwachen und neue und sich ändernde Anforderungen zu identifizieren, die sich beispielsweise aus Gesetzesänderungen, neuer Rechtsprechung und Entscheidungen von Behörden/Aufsichtsbehörden ergeben.

8. VERKNÜPFTE DOKUMENTE

- Data Privacy Policy
- IT-Policy

* * * *

ANHANG DEFINITIONEN

Verfügbarkeit	bedeutet, dass die Informationswerte und IT-Systeme den berechtigten Benutzern zu den relevanten Zeiten und in dem Umfang zur Verfügung stehen, in dem die Informationswerte oder IT-Systeme benötigt werden.
Vertraulichkeit	bedeutet, dass Informationswerte, die gespeichert, verarbeitet, transportiert und/oder übermittelt werden, vor unbefugten Benutzern und Offenlegung geschützt werden müssen.
Informationswert	bezeichnet alle Daten, die für das Unternehmen von Wert sind. Informationswerte beziehen sich auf Daten, die in der Geschäftsumgebung von Bentley vorhanden sind oder verwendet werden. Diese Werte können Informationstechnologie, Systeme und Infrastruktur, Menschen und Prozesse, persönliche Daten von Kunden und Mitarbeitenden und/oder geschäftskritische Daten umfassen.
Integrität	bedeutet, dass Informationswerte und IT-Systeme vor Manipulation und unbefugter Veränderung geschützt werden müssen.
IT-System	bezeichnet die Hardware, Software und Firmware von Computern, Telekommunikations- und Netzwerkausrüstungen oder anderen elektronischen Informationsverarbeitungssystemen und zugehörigen Geräten.
Lebenszyklus	Alle Phasen im Leben eines IT-Systems. Von den anfänglichen Anforderungen bis zu seiner endgültigen Abschaltung und Demontage. Andere Punkte im Leben eines IT-Systems sind zum Beispiel Entwurf, Spezifikation, Programmierung, Test, Installation, Betrieb und Wartung.
SOP	Standardarbeitsanweisung, die Einzelheiten und Checklisten für IT-Systeme und Informationswerte enthält.