

**Leitlinie zur Informationssicherheit
für das
Deutsche Institut für Bautechnik (DIBt)
– Kurzfassung –**

Berlin, den 17.10.2011

Inhaltsverzeichnis

1	VERPFLICHTUNG UND VERANTWORTUNG	2
2	GELTUNGSBEREICH	2
3	GESETZLICHE GRUNDLAGEN	3
4	GRUNDSÄTZE DER INFORMATIONSSICHERHEIT	3
5	SICHERHEITSZIELE	4
5.1	Institutsweite Schwerpunkte	4
5.2	Schwerpunkte in Teilbereichen	4
6	VERANTWORTLICHKEITEN	4
7	REGELUNGSSTRUKTUR	4

Abbildungsverzeichnis

Abbildung 1: Regelungsstruktur	5
--------------------------------	---

1 Verpflichtung und Verantwortung

Die Erhaltung der Informationssicherheit ist ein wichtiges Ziel für das DIBt und Teil unserer Verpflichtung durch den Gesetzgeber und gegenüber unseren Kunden. Mit der hier vorgelegten Leitlinie zur Informationssicherheit beschreibt das DIBt die Bedeutung der Informationssicherheit für unsere hoheitlichen Aufgaben und verdeutlicht die besondere Wichtigkeit, jedem Mitarbeiter das notwendige Sicherheitsbewusstsein zu vermitteln.

Das DIBt als gemeinsame Einrichtung des Bundes und der Länder erfüllt bautechnische Aufgaben auf dem Gebiet des öffentlichen Rechts und ist dabei von Informationen abhängig. Die Informationssicherheit ist somit ein zentraler Punkt bei der Erteilung von Zulassungen, bei der Anerkennung von Prüf-, Überwachungs- und Zertifizierungsstellen (PÜZ-Stellen), bei der Bekanntmachung der Bauregellisten sowie bei der Marktüberwachung.

Von größter Wichtigkeit ist neben der Genauigkeit und Verfügbarkeit auch die Vertraulichkeit von Informationen. Jeder Mitarbeiter, unabhängig von Position und Aufgabenbereich, muss sich daher der Notwendigkeit der Informationssicherheit bewusst sein und entsprechend handeln. Sicherheitsmaßnahmen sind für uns, unsere Kunden und Auftraggeber sowie beteiligte Behörden unerlässlich.

Jeder Mitarbeiter muss erkennen, dass Informationssicherheit ein wesentliches und durchaus kritisches Element der Institutsphilosophie und unseres Arbeitserfolges ist. Jeder DIBt-Mitarbeiter wird verpflichtet, sicherheitsbewusst in der täglichen Arbeit zu handeln und persönliche Verantwortung für den Schutz der ihm anvertrauten Daten zu übernehmen.

Wir werden angemessene Maßnahmen zum Schutz der DIBt-Informationen (auf Papier oder in elektronischer Form) entsprechend ihres Wertes und des ermittelten Risikos im jeweiligen Aufgabenumfeld und unter den entsprechenden technischen Bedingungen ergreifen.

2 Geltungsbereich

Diese Leitlinie zur Informationssicherheit sowie alle ihr untergeordneten Richtlinien, Handbücher und Arbeitsanweisungen gelten am Standort des DIBt (Kolonnenstr. 30 B in 10829 Berlin) und unabhängig vom Arbeitsort für:

- den Verwaltungsrat
- die Ausschüsse für Grundsatzfragen
- die Sachverständigenausschüsse
- alle internen und freien Mitarbeiter des DIBt
- alle externen Firmen, die für das DIBt Leistungen in diesem Bereich erbringen

Jeder Mitarbeiter des DIBt soll diese Leitlinie zur Informationssicherheit und die daraus abgeleiteten Standards und Handlungsanweisungen beachten. Das DIBt ist verpflichtet, die Einhaltung der konkreten Handlungsanweisungen zu überprüfen und bei Verletzungen entsprechende Maßnahmen zu ergreifen.

Externe Firmen und Mitarbeiter sind vertraglich auf die Einhaltung der Leitlinie zur Informationssicherheit und der sie betreffenden konkreten Sicherheitsbestimmungen zu verpflichten.

3 Gesetzliche Grundlagen

Die gesetzlichen Grundlagen für das Handeln des DIBt und seiner Mitarbeiter bilden in besonderem Maße:

- das Gesetz über das Deutsche Institut für Bautechnik
- das Abkommen über das Deutsche Institut für Bautechnik
- die Satzung des Deutschen Instituts für Bautechnik
- die Bauproduktenrichtlinie und das Bauproduktengesetz
- die Musterbauordnung sowie die Musterverordnungen der Bauministerkonferenz
- die Bauordnungen und die aufgrund der Bauordnungen erlassenen Rechtsverordnungen der Länder
- das Verwaltungsverfahrensgesetz
- das Berliner Datenschutzgesetz
- das Berliner Beamtenrecht und Tarifrecht (TV-L)

Eine detaillierte Darstellung der Rechtsgrundlagen des DIBt wird im "Roten Handbuch"¹ in der jeweils aktuell gültigen Fassung gepflegt und veröffentlicht.

4 Grundsätze der Informationssicherheit

Zur Wahrung der Informationssicherheit verfolgt das DIBt den Schutz folgender Eigenschaften von Informationen:

- **Vertraulichkeit**, d. h. Schutz vor unbefugter Preisgabe von Informationen:
Es ist sicherzustellen, dass zur Bewahrung der Geschäftsbetriebsgeheimnisse Informationen nur für berechnigte Personen zugänglich sind. Jeder Mitarbeiter hat die dementsprechende Dienstanweisung des "Roten Handbuches"² exakt einzuhalten.
- **Integrität**, d. h. Schutz vor unbefugter Veränderung von Informationen:
Es ist sicherzustellen, dass Informationen korrekt und vollständig vorliegen. Im gesamten Schriftverkehr des DIBt sind die im Roten Handbuch³ festgelegten Abzeichnungs-, Mitzeichnungs- und Schlusszeichnungsregelungen konsequent einzuhalten.
Dabei sind auch die Unterkategorien zur Integrität (Authentizität, Revisionsfähigkeit und Transparenz) von Informationen zu schützen, die in der Definition des Berliner Datenschutzgesetzes anzuwenden sind.
- **Verfügbarkeit**, d. h. Schutz vor unbefugter oder ungewollter Vorenthaltung von Informationen oder Betriebsmitteln:
Es ist sicherzustellen, dass berechnigte Personen zeitnah Zugang zu aktuellen Informationen und Diensten erhalten. Außerdem ist durch Archivierung eine langfristige Informationsbewahrung zu gewährleisten. Die konkret zu beachtenden Vorschriften der Kennzeichnung und Aufbewahrung von Akten sind im "Roten Handbuch"⁴ geregelt.

Diese Eigenschaften der Informationen stellen gleichzeitig die zu schützenden Grundwerte der Informationen dar. In Abhängigkeit vom möglichen Schadenpotential bei Verlust des jeweiligen Grundwertes sind alle Informationen des DIBt in drei Schutzstufen zu klassifizieren. Die Details sind zu regeln.

Zur Gewährleistung der Informationssicherheit sind technologische Maßnahmen mit organisatorischen Rahmenbedingungen zu verbinden. Das DIBt sorgt dafür, dass:

- für Informationen (Daten, unterstützende Systeme und Verfahren) Informationseigentümer ernannt werden und dass diese für die Festlegung des erforderlichen Kontrollumfangs mitverantwortlich sind.
- der jeweils für die Informationen geltende Sicherheits- und Kontrollumfang am jeweiligen Aufgabenrisiko ausgerichtet ist.
- die einzelnen Nutzer für die zweckgebundene und sicherheitsbewusste Verwendung von Informationen verantwortlich sind.

1 Dokument G 1.01

2 Allgemeine Dienstanweisung 1.04 - b Dienstverschwiegenheit, Geheimhaltung, Datenschutz

3 Geschäftsgang 1.05 - c Schriftverkehr

4 Geschäftsgang G 1.05 - e Aktenverwaltung/Aktenplan/Aufbewahrung

- es eine unabhängige Überprüfung der Verwaltung und Nutzung von Informationen gibt.
- Zugriffsrechte auf Daten, Zugangsrechte zu Systemen und Zutrittsrechte zu sensiblen Räumen nach dem Minimalprinzip ("so wenig wie möglich, so viel wie nötig") vergeben werden.

Das DIBt stellt durch bewusstseinsbildende Maßnahmen (Schulungen, E-Learning, Intranetinformationen usw.) sicher, dass jeder Mitarbeiter:

- genaue Kenntnisse über die Erfordernisse der Informationssicherheit innerhalb des eigenen Verantwortungsbereiches hat.
- ausreichende Kenntnisse über Gefährdungen und Risiken erlangt, die beim Umgang mit Informationen in seinem Arbeitsgebiet bestehen.
- die Fähigkeit besitzt, die ihm anvertrauten Informationen sicher zu verarbeiten.

5 Sicherheitsziele

Die Informationsverarbeitung spielt eine Schlüsselrolle für unsere Aufgabenerfüllung. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik unterstützt. Erklärtes Ziel ist die Gewährleistung der Informationssicherheit im DIBt.

5.1 Institutsweite Schwerpunkte

Durch den sicheren Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen sorgt unser Institut für die:

- Verlässlichkeit der Arbeitsprozesse und Arbeitsergebnisse
- Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Organisation
- Sicherung der Qualität der Informationen
- langfristige Sicherung der Werte der verarbeiteten Informationen
- Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen
- Wahrung der Reputation und der Werte des DIBt
- Reduzierung der im Schadensfall entstehenden Kosten und Wiederherstellungszeiträume

5.2 Schwerpunkte in Teilbereichen

Diese Angaben sind nur im Intranet zu finden.

6 Verantwortlichkeiten

Diese Angaben sind nur im Intranet zu finden.

7 Regelungsstruktur

Alle Dokumente zur Informationssicherheit bilden gemeinsam das **Informationssicherheitshandbuch**. Dabei ist die Regelungsstruktur der Informationssicherheitsorganisation hierarchisch aufgebaut. Auf erster Ebene ist die hier formulierte **Leitlinie zur Informationssicherheit** das führende Dokument und beschreibt den Handlungsrahmen.

In der zweiten Ebene wird eine analytische Grundlage fixiert, die die notwendigen Dimensionen für den Schutz der Daten beleuchtet und damit objektiviert. Es werden folgende Aspekte definiert:

- die Schutz- und Daten-Klassifizierung
- die Schutzbedarfsfeststellung
- das Sicherheitsmanagement verbunden mit der Verpflichtung zur kontinuierlichen Verbesserung

In dieser Ebene werden die Vorgehensweisen und Standards zur Erfüllung der Sicherheitsanforderungen ohne technische Einzelheiten und konkrete Umsetzungsanweisungen beschrieben. Zusammen bilden diese Unterlagen das **Informationssicherheitskonzept**.

Auf dieser Grundlage werden in der dritten Ebene sehr konkret technische und organisatorische Handlungsanweisungen formuliert. Hier sind detaillierte technische Beschreibungen für einzelne Systeme und Plattformen sowie die **Arbeitsanweisungen** (gleichzeitig Bestandteil des "Roten Handbuchs") zu finden.

Die Arbeitsanweisungen zur Informationssicherheit bilden innerhalb des Informationssicherheitshandbuchs die verpflichtende Basis für alle Mitarbeiter. Darin befinden sich u. a. folgende Regelungen:

- Personalregelungen mit Bezug zur Informationssicherheit
- technische Sicherheitskonzepte
- Regelungen zur Absicherung des Netzwerkes
- Regelungen zum Einsatz von Hardware
- Regelungen zur Absicherung von Software

Mit dieser dreistufigen Dokumentenhierarchie wird eine steigende Konkretisierung erreicht, die die folgende Grafik darstellt:

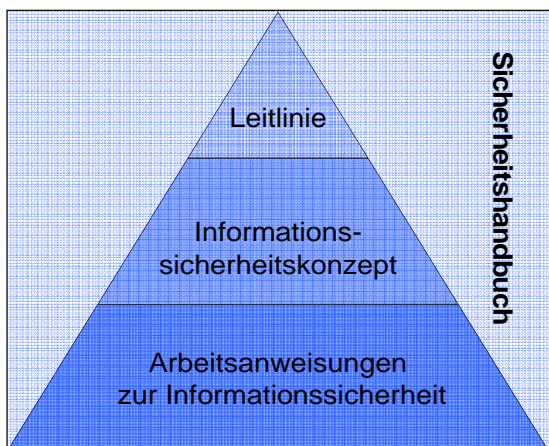


Abbildung 1: Regulationsstruktur