Inhaltsübersicht

	Seite
Teil I: Rechtliche Aspekte der IT-Sicherheit	35
1. Kapitel: Grundlagen	37
§ 1 Legaldefinition IT-Sicherheit	37
§ 2 Technische Regelwerke zur IT-Sicherheit und deren Bedeutung.	37
§ 3 Signaturrecht	47
2. Kapitel: Datenschutzrecht	55
§ 1 Grundsätze des Datenschutzrechts	55
§ 2 Acht goldene Regeln zur Sicherheit personenbezogener Daten	59
§ 3 Auftragsdatenverarbeitung	81
§ 4 Der Datenschutzbeauftragte	86
§ 5 Sanktionen bei Verstoß gegen Datenschutzrecht	89
§ 6 Datenschutzaudit	91
3. Kapitel: Gesellschaftsrecht	94
§ 1 Einführung	94
§ 2 Organisation der IT Sicherheit im Unternehmen	94
§ 3 IT-Sicherheit im Konzern	130
4. Kapitel: Strafrecht	136
§ 1 Straftaten von Mitarbeitern im Zusammenhang mit der Unternehmens-IT	136
§ 2 Straftaten der Unternehmensleitung	155
5. Kapitel: Vertragliche und deliktische Haftung	159
§ 1 Einleitung	159
§ 2 Haftung für Herstellung, Planung und Vertrieb von Soft- bzw. Hardware	165
§ 3 Haftung von IT-Verwendern	175
§ 4 Zusammenfassung	193
6. Kapitel: Handels- und Steuerrecht	198
§ 1 Handels- und steuerrechtliche Vorgaben an das IT-System	198
§ 2 Digitaler Datenzugriff und Prüfbarkeit digitaler Unterlagen durch die Finanzverwaltung	219
7. Kapitel: Urheberrecht – DRM	226
§ 1 Einführung	226
§ 2 Rechtliche Gesichtspunkte	231
8. Kapitel: Wettbewerbsrecht	249
§ 1 Unzumutbare Belästigungen § 7 UWG	249
§ 2 Betriebsspionage § 17 Abs. 2 UWG	250

§ 3 Verwertung von Vorlagen § 18 UWG.	250
§ 4 „Vorteil durch Rechtsbruch“ § 4 Nr. 11 UWG.	251
9. Kapitel: Gewerberecht	253
§ 1 Sinn und Zweck der Gewerbeuntersagung nach § 35 Gewerbeordnung (GewO).	253
§ 2 Voraussetzungen der Gewerbeuntersagung	255
§ 3 Adressat der Untersagungsverfügung	259
§ 4 Zuständige Behörde	259
§ 5 Bindung an strafrechtliche Entscheidungen	260
§ 6 Folgen der Untersagungsverfügung	260
10. Kapitel: Vergaberecht	262
§ 1 Einführung in das Vergaberecht	262
§ 2 IT-Sicherheit in der Leistungsbeschreibung öffentlicher Auftraggeber	266
§ 3 IT-Sicherheit bei Wertung der Angebote durch öffentliche Auftraggeber	268
11. Kapitel: Arbeitsrecht	272
§ 1 Überblick	272
§ 2 Pflichten des Arbeitnehmers	273
§ 3 Sanktionierung von Pflichtverletzungen	296
§ 4 Haftung des Arbeitnehmers	301
§ 5 Elektronische Personalakte	308
12. Kapitel: IT-Sicherheit und Basel II	318
§ 1 Basel II und Eigenkapitalvorschriften für Kreditinstitute	318
§ 2 Rating-Systeme und ihre Auswirkungen auf die Unternehmens-IT ..	319
§ 3 Basel II und IT-Anforderungen bei Banken	322
13. Kapitel: Branchenspezifische Aspekte	323
§ 1 Banken	323
§ 2 Krankenhäuser	338
14. Kapitel: Fazit	348
Teil II: Technische und organisatorische Aspekte der IT-Sicherheit	349
1. Kapitel: Die Berücksichtigung der Informationssicherheit im Unternehmen	351
§ 1 Grundbegriffe	351
§ 2 Schaffung der organisatorischen Voraussetzungen	354
§ 3 Das Informationssicherheits-Managementsystem	358
§ 4 Die Bedeutung der Zertifizierung	359
2. Kapitel: Erstellung, Implementierung und Anpassung eines IT-Sicherheitskonzepts im Unternehmen	361
§ 1 Identifikation der Sicherheitsanforderungen	361

	Seite
§ 2 Definition der IT-Sicherheitsleitlinie	363
§ 3 Risikoanalyse	365
§ 4 Maßnahmenplanung	365
§ 5 Definition von Maßnahmen	391
§ 6 Implementierung von Maßnahmen	396
§ 7 Überwachung von IT-Sicherheitsmaßnahmen	401
§ 8 Kontinuierliche Verbesserung der IT-Sicherheitsmaßnahmen	402