

## Inhaltsverzeichnis

<b>1. Einleitung.....</b>	<b>23</b>
1.1. Daten – Informationen – Informationssicherheit.....	23
1.2. Wegweiser durch das Handbuch.....	26
1.3. Vorgehen bei der Umsetzung der Informationssicherheit .....	29
<b>2. Informationssicherheits-Managementsystem (ISMS) .....</b>	<b>39</b>
2.1. Informationssicherheit in KMU und in Verwaltungen.....	39
2.2. Oft verwendete Standards.....	42
2.3. Komponenten eines ISMS gemäss ISO 27001 .....	43
2.4. Der Prozess der Informationssicherheit .....	45
2.5. Management-Prinzipien.....	47
2.6. Umsetzung des ISMS in einem KMU .....	52
2.7. IT-Risiko-Analyse .....	56
2.8. IT-Grundschutz.....	61
2.9. Umgang mit Risiken .....	66
<b>3. Rechtliche Aspekte.....</b>	<b>69</b>
3.1. Datenschutz.....	69
3.2. Vertragliche Grundlagen / Allgemeine Geschäftsbedingungen (AGB).....	78
3.3. E-Commerce .....	83
3.4. Verträge mit Outsourcing- resp. Cloud-Anbietern .....	86
3.5. Lizenzen .....	93
3.6. Urheberrecht.....	96
3.7. Vertraulichkeitsvereinbarung mit externen Partnern .....	100
3.8. Aufzeichnungs- und Archivierungspflichten.....	103
3.9. Schutz vor Missbrauch im Cyberspace .....	108
3.10. Überwachung am Arbeitsplatz.....	110
3.11. Haftung .....	114
3.12. Versicherungen .....	119
3.13. Strafrecht und Computer Forensics.....	121
<b>4. Organisatorische Aspekte .....</b>	<b>125</b>
4.1. Benutzerrichtlinien.....	125
4.2. Passwörter.....	129
4.3. BYOD (Bring Your Own Device).....	132
4.4. Zielpublikumsorientierte Awareness.....	135
4.5. Sicherer Zahlungsverkehr (Online-Banking) .....	145
4.6. Handhabung von Datenträgern und Dokumenten.....	149
4.7. Umgang mit Geschäftsunterlagen .....	153
4.8. Verhalten im Notfall – Krisenmanagement .....	158
4.9. Cloud-Nutzung.....	167
4.10. Berechtigungsvergabe.....	173
4.11. Umgang mit Schwachstellen und Sicherheitsvorfällen.....	179

4.12. Unterhalt, Wartung und Reparatur .....	185
4.13. Sicherheit im Projektmanagement .....	190
4.14. Change Management.....	193
4.15. Physische Sicherheit.....	197
4.16. Homeoffice.....	207
<b>5. Technische Aspekte.....</b>	<b>211</b>
5.1. Verschlüsselung, digitale Signatur und PKI .....	211
5.2. Back-up.....	215
5.3. Schutz vor Malware / Cyber Defence.....	220
5.4. Microsoft Windows Server-Sicherheit .....	223
5.5. Einsatz von Arbeitsplatz-Clients.....	235
5.6. Collaboration-Tools (SaaS).....	238
5.7. Sichere E-Mails .....	242
5.8. Netzwerksicherheit.....	246
5.9. Sicherheit in drahtlosen Netzwerken (WLAN).....	250
5.10. VPN.....	254
5.11. Internet-Anbindung.....	257
5.12. Fernwartung .....	261
5.13. Telekommunikationsgeräte und VOIP .....	264
5.14. Einsatz mobiler Geräte (Notebooks, Smartphones, Tablets usw.) .....	268
5.15. Serverraum-Sicherheit .....	272
5.16. Sicherheit von Webanwendungen .....	277
5.17. Datenbank-Sicherheit.....	283
5.18. Sicherheit in der Applikationsentwicklung und Einführung.....	288
5.19. Internet der Dinge (IoT).....	293
<b>6. Abkürzungsverzeichnis und Glossar .....</b>	<b>296</b>
<b>7. Index .....</b>	<b>317</b>
<b>8. Lizenzbedingungen und Beilagen .....</b>	<b>323</b>