

## 24 Monate Curriculum zur Umsetzung der IT-Sicherheit und des Datenschutzes in kleinen und mittleren Unternehmen (KMU)

Quartal		Einheit	Themenblöcke	Referenz	Zeit in min.	Status
Q 01	Block 01	Q1	Einführung in die System-Anwendung (die ersten Schritte)			
			Bestandsaufnahme IT-Infrastruktur			
			Analyse aller Lizenz- und Nutzungsverträge HW/SW/Internet			
	Block 02		Mitarbeiter-Orientierung und -Aufklärung			
		Risikoanalysen zu IT-Sicherheit und zum Datenschutz				
		Einsatz von Virenschutzprogrammen				
Q 02	Block 03	Q2	Anwendung von sicheren Passwörtern			
			Aufklärung über Internet-Angriffe, z.B. Phishing			
			Firewalls und deren Aktualisierung			
	Block 04		Konformität der Mitarbeiterverträge mit IT-Sicherheit und Datenschutz			
		Sicherheitsprüfungen Software und Installations-Standards, Back-Ups				
		Regelmäßige Sicherheits-Updates				
Q 03	Block 05	Q3	Begrenzung der Datenzugriffsmöglichkeiten			
			Berechtigungskonzept und Admin-Rechte			
			Zugangs-, Zutritts- und Zugriffsschutz			
	Block 06		Einsatz von Druckern, Kopierern und Multifunktionsgeräten			
		Umgang mit Webbrowsern				
		Umgang mit E-Mail-Programmen				
Q 04	Block 07	Q4	Rekonstruktion von Datensicherungen (Prozess und Test)			
			Internetbasierte Telefonie und Videotelefonie			
			Formate der Prozessbeschreibungen nach ISO 9001			
	Block 08		Notfallmanagement für Informationssicherheit/Datenschutz			
		Entsorgung und Reparatur von IT-Systemen und Datenträgern				
		Schutz der IT-Systeme vor physikalischen Einflüssen				
Q 05	Block 09	Q5	Fernwartung			
			Umgang mit externen Speichermedien			
			Festlegung und Dokumentation von Maßnahmen			
	Block 10		Sicherheitsmanagement Webanwendungen, Fileservern, Datenbanksystemen			
		Sicherheit bei Smartphones und Tablets				
		Sicherheit bei vernetzten Peripherie-Systemen (z.B. branchenspezifisch)				

Q 06	Block 11	Q6	Sicherheit bei Faxgeräten			
			Häusliche und mobile Arbeitsplätze			
			Regelungen für neue und ausscheidende Mitarbeitende			
	Block 12		Einsatz von Fremdpersonal (z.B. IT- und Telekommunikations-Service)			
			Raum oder Schrank für technische Infrastruktur			
			Optimierungs-Management (PDCA)			
Q 07	Block 13	Q7	DSGVO und Datenschutzbeauftragte			
			Prüfung durch den DSB und Jahresbericht			
			Archivierungs-Management und Sicherung (lanfristig)			
	Block 14		Aktualisierung Risikoanalyse mit Jahresbericht			
			Regelung zur Groupware (z.B. Exchange, Outlook)			
			Regelung für einen zentralen Verzeichnisdienst/Administration			
Q 08	Block 15	Q8	Regelungen zu IoT-Geräten			
			Einrichtung eines ISMS			
			Einrichtung eines ISMS/DSMS nach DSGVO			
	Block 16		Variabel für Updates und Ergänzungen			
			Variabel für Updates und Ergänzungen			
			Variabel für Updates und Ergänzungen			