Kurzübersicht aller Hinweise und Empfehlungen zur Schwerpunktprüfung 2021 IT-Sicherheit

Bereich	Detail	Hinweis & Empfehlung
5.1 Organisation	5.1.1 IT-Struktur	Definition eines IT-Verantwortlichen
		Beschränkung des Zugriffs für Anwender auf für sie relevante Daten und Programme
		Administratoren sollen zusätzlich eigenen Account haben und nicht als Administrator arbeiten
		Erstellung eine Berechtigungskonzepts für Programme sowie Berechtigungserteilung im Vieraugenprinzip
		Erstellung eines Notfallkonzepts
	5.1.2 Datensicherungen	konsequente und regelmässige Datensicherung. Kopie auf Offline-Datenträger ist empfehlenswert
		bei Auswahl des Cloud-Dienstes darauf achten, eine mit zusätzlichen Sicherheitsvorkehrungen wählen
		Merkblatt mit Empfehlungen zur Datensicherung auf autonomen Einzelgeräten
	5.1.3 Beschaffung und Entsorgung von Hard- und Software	Beschaffung im Rat behandeln und entsprechend budgetieren
		fachgerechte Entsorgung von Hardware nicht unterschätzen und vernachlässigen. Festplatten und Datenträger am besten physisch zerstören
	5.1.4 Sensibilisierung der Anwender	Benutzerrichtlinien schriftlich festhalten
		regelmässige Sensibilisierung der Anwender auf aktuelle Risiken
		Websites zur Informationsbeschaffung betreffend IT-Sicherheit: - swisscom.ch/de/magazin/datensicherheit-infrastruktur/phishing-entlarven-melden-loeschen/ - ncsc.admin.ch/ncsc/de/home.html - cybercrimepolice.ch
5.2 Technik	5.2.1 Netzwerk	periodische Überprüfung zur Reduktion oder Ausweitung der bestehenden Infrastruktur
		bei Auswahl des Cloud-Dienstes auf die lokale Datenschutzgesetzgebung (Serverstandort) achten
5.3 Sicherheit	5.3.1 Sicherheitsprogramme	Virenschutzprogramm und weitere Präventivmassnahmen durch Vorgaben (insbesondere bei autonome Einzelgeräten)
	5.3.2 Updates	zeitnahe Updates aller im Einsatz befindliche Programme
		laufende Aktualisierung der Virenschutzprogramme und der Firewall
		Sensibilisierung der Anwender auf veraltete Betriebssoftware sowie laufende Aktualisierung
	5.3.3 Zugriffschutz, Passwörter	zwingend für den Zugriff auf das Gerät verwenden
		keine Passwörter beim Gerät deponieren
		Passwortmanager verwenden
		Vorgabe zur periodischen Anpassung von Passwörtern und Hinweis auf Erhöhung der Sicherheit durch Komplexität
5.4 Kontrolle	5.4.1 IKS	Aufnahme der IT-Risiken im IKS
	5.4.2 Kontrolltätigkeiten	GPK: Thema IT im Rahmen der Prüfung der Amtsführung aufgreifen
		externes Sicherheitsaudit in Betracht ziehen
		Branchenstandards des Bundes anschauen www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards.html