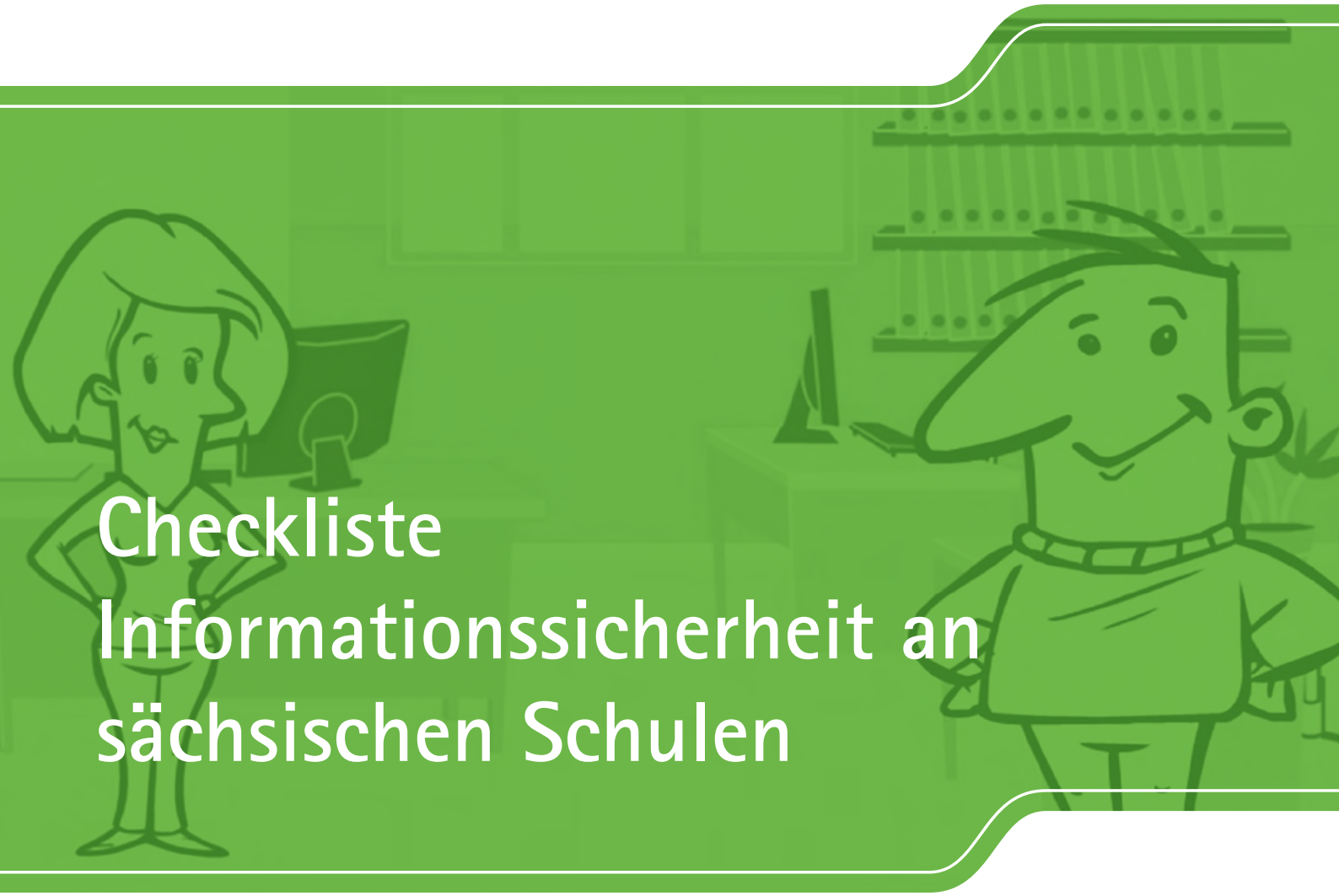
LANDESAMT FÜR
SCHULE UND BILDUNG

Freistaat
SACHSEN



Checkliste Informationssicherheit an sächsischen Schulen

Inhaltsverzeichnis

1. Passwortsicherheit

- [ ] **Passwort sicher?**
- [ ] Langes Passwort (mindestens 8+ Zeichen)
- [ ] Keine Wörter verwendet
- [ ] Passwort nicht auf Papier hinterlegt
- [ ] **Verschiedene Zeichengruppen verwendet (z.B. Buchstaben, Ziffern, Sonderzeichen)?**
- [ ] **2-Faktorauthentifizierung aktiviert?**
- [ ] Wenn möglich bei Sozialen Netzwerken etc. 2FA nutzen
- [ ] **Jede Anwendung mit einem eigenen Passwort?**
- [ ] **Verschiedene Passwörter für »normale Nutzer« und »Administratoren«?**
- [ ] **Passwörter in einer verschlüsselten Datei oder in einem Passwortmanager abgelegt?**
- [ ] **Langes WLAN-Passwort?**
- [ ] WPA2 oder besser nur WPA 3 aktiviert
- [ ] WPS und UPnP deaktiviert

2. Datenträger/Daten verschlüsseln

- [ ] **Datenträger mit Hardwareverschlüsselung verwendet?**
- [ ] **Dateien in verschlüsseltem (Dateisystem-) Container (z.B. mit VeraCrypt) abgelegt?**
- [ ] **Digitaler Schlüssel an anderer Stelle abgelegt, als den Datenträger?**
- [ ] **Daten an einer anderen Stelle sicher als Backup abgelegt?**
- [ ] **Aktuelle (Office-) Dokumentenformate genutzt, die sichere Verschlüsselung erlauben (XLSX, DOCX, ...)?**
- [ ] **Smartphone mit PIN/biometrischen Daten gesichert?**

3. Daten regelmäßig sichern

- [ ] **Kurzzeit-Datensicherung ggf. auf gleichem Datenträger angelegt (evtl. via Nextcloud oder Schattendateisystem)?**
- [ ] **Verschlüsseltes Backup auf anderem Datenträger (Festplatte/Stick) angelegt?**
- [ ] Backup-Datenträger verschlüsselt
- [ ] Backup-Datenträger sicher verwahrt (im Safe?) und vom PC getrennt
- [ ] Wiederherstellung getestet

☐	**Daten online gesichert?**	
☐	Daten verschlüsselt	
☐	Passwort und/oder Schlüsseldatei sicher verwahrt (z.B. in einem Safe)	
☐	**Backup automatisiert, oder in die Abläufe integriert?**	

4. Sichere E-Mail-Kommunikation

	Allgemein	
☐	Vertrauenswürdigkeit des Absenders geprüft (z.B. bekannte Telefonnummer)	
☐	Anhänge auf Viren geprüft	
☐	Verschlüsselung möglich/nötig	
☐	S/Mime	*https://volksverschluesselung.de/index.php*
☐	GPG oder PGP	*https://www.mailvelope.com/de/help* *https://www.gpg4win.de*
☐	SecureMail	
☐	E-Mail-Anwendung nur im Text-Modus	
☐	Zugriff auf E-Mail-Anwendung via	
☐	*TLS / SSL*	
☐	*VPN*	
☐	Empfänger ausgedünnt	
☐	*Empfänger geprüft*	
☐	*Nur berechtigte Empfänger*	
☐	**Schulinterne Kommunikation**	
☐	Schulportal verwendet	
☐	Vom Träger bereitgestelltes E-Mail-Konto verwendet	
☐	**Kommunikation mit Institutionsexternen oder Schulexternen**	
☐	Virenscanner genutzt	
☐	Wenn möglich nur Text-E-Mails genutzt	
☐	Links nur anklicken, wenn der Absender vertrauenswürdig ist	
☐	**Zugriff auf E-Mails und interne Dateien nur via VPN**	
☐	**Messenger mit Verschlüsselung**	
☐	Desktopintegration regelmäßig prüfen, damit keiner unbemerkt mitlesen kann	

5. Verwendung aktueller Virenscanner/ Firewalls

- [ ] **Betriebssystem Updates installiert?**
- [ ] Browser Updates installiert
- [ ] *Addons regelmäßig ausgedünnt*
- [ ] *Tracker blockiert (uBlock origin)*
- [ ] *Berechtigungen der Webseiten geprüft*
- [ ] *Links von z.B. Banken nicht aus E-Mails geöffnet, sondern immer aus der Lesenzeichenverwaltung*
- [ ] Windows Updates installiert
- [ ] Office Updates installiert
- [ ] *Office Makros deaktiviert*
- [ ] Vorschau von Dateien im Dateimanager deaktiviert
- [ ] Smartphone Updates installiert
- [ ] *Nur Hersteller App Stores für die App-Installation genutzt*
- [ ] *Apps auf ihre Rechte geprüft*
- [ ] *Smartphone nicht gerootet (keine erweiterten Rechte eingestellt)*
- [ ] Router Updates installiert
- [ ] **Antivirenprogramm (vom Betriebssystem) installiert, aktiviert und konfiguriert?**
- [ ] **Firewall (vom Betriebssystem) installiert, aktiviert und konfiguriert?**
- [ ] **Dateien nur aus vertrauenswürdigen Quellen geöffnet und bezogen?**

6. Social Engineering

- [ ] **Soziale Netzwerke**
- [ ] Nur wenige persönliche Informationen in Sozialen Netzwerken gepostet
- [ ] Pseudonyme genutzt
- [ ] 2FA aktiviert
- [ ] Anfragen genau geprüft und ggf. auf anderen Wegen nachgefragt
- [ ] Private Nachrichten ggf. über anderen Kanal verifiziert
- [ ] **Regeln für Videokonferenzen mit Kolleginnen und Schülerinnen festgelegt?**

Seien Sie skeptisch und vorsichtig bei Geschenken oder Zufallsfunden!
Wenn etwas kostenlos ist, dann sind Sie oder Ihre Daten die Ware.

- [ ] Keine Aufnahmen ohne Zustimmung etc.
- [ ] Kameraberechtigungen von Apps geprüft und nur Ausgewählten den Zugriff gestattet
- [ ] **Wichtige Kontakte im Adressbuch gespeichert?**
- [ ] **Verschlüsselung und Signaturen für E-Mails verwendet?**
- [ ] **Informationen ggf. über andere Quellen verifiziert?**
- [ ] **Achten Sie auf Änderungen der Hardware?**
- [ ] Neue Geräte
- [ ] Neue Kabel
- [ ] **Handy nur an vertrauenswürdigen Netzteilen und mit ebensolchen Kabeln geladen?**
- [ ] **Nach Möglichkeit PIN oder biometrische Authentifizierungsmethoden genutzt?**
- [ ] Besondere Daten mit Kombinationen aus PIN und biometrischen Methoden geschützt
- [ ] **Alle Geräte, wenn Sie diese aus den Augen lassen, gesperrt?**
- [ ] Kritische Geräte vor dem Verlassen heruntergefahren
- [ ] Hardwareverschlüsselung beim Handy/Notebook aktiviert
- [ ] **Bei Unsicherheit – Hilfe geholt oder Experten in der Schule gefragt?**

7. Sonstiges

- [ ] **Private und berufliche Daten getrennt?**

Herausgeber und Redaktion: Landesamt für Schule und Bildung • Referat 33 | Medienbildung und Digitalisierung
Annaberger Straße 119 • 09120 Chemnitz • Telefon: +49 371 5366-0 • E-Mail: poststelle@lasub.smk.sachsen.de
www.lasub.smk.sachsen.de • **Beratung:** 4viewture GmbH, Kesselsdorf • **Gestaltung und Satz:** Hi Agentur e.K., Dresden
Redaktionsschluss: Oktober 2021 • **Bezug:** Dieser Artikel ist elektronisch als PDF verfügbar