Mindestsicherheitsstandards des StMUK
für die Nutzung privater digitaler Endgeräte im Schuldienst

1. Konfiguration des Endgeräts

1.1 Sicherheitstechnische Einstellungen eines sicheren Endgeräts und eines sicheren Betriebssystems

Aktuelle Betriebssysteme, die vom jeweiligen Anbieter gepflegt werden, können als sicher betrachtet werden, solange die Sicherheitsfunktionen beachtet bzw. nicht bewusst deaktiviert werden.

Sicherheitsfunktionen sind heute üblicherweise im Betriebssystem integriert. Als Mindestsicherheitsfunktionen muss

- die Festplatte des Geräts sicher verschlüsselt sein (z. B. mit Bitlocker),
- eine geschützte Anmeldung (z.B. Passwort, Bildschirmcode) eingerichtet sein,
- nur Software aus sicheren Quellen (App-Stores/direkt von Hersteller bezogen) installiert werden,
- das Betriebssystem und die Software (durch regelmäßige, im besten Fall automatisierte Updates) auf dem neuesten Stand gehalten werden.

Zudem müssen die betriebssystemeigenen Schutzprogramme (z.B. der Windows-Defender) aktiviert sein.

1.2 Datenschutztechnische Einstellungen

Bei der Nutzung des Betriebssystems und der installierten Software muss auf eine datensparsame Einstellung geachtet werden. Darunter sind vor allem die Einschränkung der Übermittlung der Diagnosedaten, die Überprüfung der Trackingfunktion sowie auch die Anpassung der Anwendungsberechtigungen zu verstehen.

2. Sichere Softwareauswahl/-einsatz

2.1 Software aus anerkannt sicheren Quellen

Beim Download und bei der Installation von Software ist generell Vorsicht geboten, da dieser Weg die einfachste Methode darstellt, um Schadsoftware oder unerwünschte Software (z.B. Adware) auf ein Endgerät zu bringen.

Sichere Anbieter von Software sind insbesondere

- Softwareportale der Betriebssysteme (Apple Appstore, Google Playstore, Microsoft Store)
- Webseiten des Herstellers der Hard- oder Software
- vertrauenswürdige Softwareportale, z. B. Heise oder Snapfiles.

Bei vielen Softwareportalen wird allerdings oft zusätzliche Adware mitinstalliert.

2.2 Installation der Software

Die durch die Schule zur dienstlichen Nutzung freigegebene Software darf nur mit dem geringsten notwendigen Funktionsumfang installiert und ausgeführt werden.

3. Betrieb des Endgeräts in verschiedenen Netzwerkumgebungen

Bei der Verwendung des schulischen und häuslichen WLANs sind keine weiteren Netzwerk-Sicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten notwendig.

Bei der Verwendung von öffentlichen Hotspots sollte auf die Verarbeitung von personenbezogenen Daten aus Sicherheitsaspekten verzichtet werden.

Bei der Verwendung von öffentlichen Hotspots müssen folgende Punkte beachten werden:

- Verwendung einer VPN-Verbindung bei einem notwendigen Zugriff auf das schulische Netzwerk von außen
- Verschlüsselte Übertragung (z. B. per https)
- Ggfs. aktivierte Firewall bei MacOS, Windows Betriebssystem

4. Zugriff auf das Endgerät nur durch die jeweilige Lehrkraft

Der Zugriff auf das Endgerät muss durch einen Zugriffsschutz gesichert werden (z. B. mit Benutzernamen und starkem Passwort, biometrische Anmeldeverfahren).

Link zum Bundesamt für Sicherheit in der Informationstechnik bzgl. sicheres Passwort:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Umgang-mit-Passwoertern/umgang-mit-passwoertern_node.html

Beim Verlassen des Arbeitsplatzes muss sich

- die Lehrkraft abmelden oder
- das Endgerät sperren.

Bei zu langer Inaktivität muss eine automatische Sperrung des Endgeräts (spätestens nach 15 Minuten) erfolgen.

5. Nutzerkonten

Bei Verwendung eines Gerätes mit Windows oder MacOs, sollte neben dem administrativen Zugang ein lokales Nutzerkonto ohne administrative Rechte eingerichtet und grundsätzlich genutzt werden, um die Sicherheit zu erhöhen.

6. Umgang mit Zugangsdaten und Passwörtern

Werden Zugangsdaten bzw. Passwörter auf dem privaten Endgerät gespeichert, ist sicherzustellen, dass diese vor fremden Zugriff gesichert sind. Dies kann durch einen lokalen Passwortmanager erfolgen.

7. Ablage von dienstlichen Daten

Die Ablage von dienstlichen Daten muss getrennt von privaten Daten erfolgen. Dies kann erreicht werden, indem verschiedene Verzeichnisse für dienstliche bzw. private Daten angelegt werden. Das Verzeichnis für dienstliche Daten muss vor Fremdzugriff mit Hilfe von geeigneten Lösungen verschlüsselt gesichert werden.

8. Aufbewahrungs- und Löschfristen

Die jeweils geltenden Aufbewahrungs- und Löschfristen sind einzuhalten.

9. Backup der dienstlichen Daten

Die dienstlichen Daten sollten in regelmäßigen Abständen gesichert werden. Eine Vermischung des Backups von dienstlichen und privaten Daten ist nicht gestattet. Wird ein Backup erstellt, muss auf den Zugriffsschutz und eine Verschlüsselung geachtet werden. Bei Backups sind ebenfalls die unter Ziffer 8 genannten Aufbewahrungs- und Löschfristen einzuhalten.

10. Sicheres Löschen von Datenträgern

Werden Datenträger gewechselt oder entsorgt, müssen diese vor der Entsorgung oder Weitergabe an Dritte sicher gelöscht oder vernichtet werden.

Link zum Bundesamt für Sicherheit in der Informationstechnik bzgl. Löschen:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html