Informationssicherheitsbeauftragter der kantonalen Verwaltung Basel-Stadt

CYBERSECURITY POCKETBOOK

GERÄTESICHERHEIT

WLAN, Bluetooth und NFC
Deaktivierung von WLAN, Bluetooth und NFC, wenn nicht in Gebrauch, um unerwünschte Verbindungen zu vermeiden

Betriebssystem
Das Betriebssystem regelmässig aktualisieren und auf dem neuesten Stand halten

Regelmässiger Neustart
Das mobile Gerät regelmässig (mindestens alle 24 Stunden) neu starten, um potenziell im Hintergrund laufende schädliche Anwendungen zu beenden.

Mobile Hotspot
Verwendung eines eigenen mobilen WLAN-Hotspots anstelle öffentlicher WLANs zur Erhöhung der Sicherheit.

Öffentliches WLAN
Vermeidung der Nutzung öffentlicher WLAN-Netze

Applikationen
Die Applikation regelmässig aktualisieren und auf dem neuesten Stand halten.

Peripherie
Vermeide die Verwendung fremder Peripherie und Datenspeichergeräte (USB-Sticks, externe Festplatten).

Passwort
Verwende immer ein sicheres Passwort (mindestens 12 Zeichen, wenn möglich alphanumerisch – sowie Sonderzeichen).

Standort
Deaktivierung von Standortdiensten, wenn nicht notwendig, und Kontrolle über die Standortfreigabe in Apps.

Privacy Screen
Verwende einen Blickschutzfilter.

INFORMATIONSSICHERHEIT

Gespräche in der Öffentlichkeit
Vermeidung von vertraulichen Gesprächen in öffentlichen Bereichen, um das Risiko des Mithörens zu minimieren

Identität
Überprüfung der Identität von Kommunikationspartnern und immer misstrauisch sein, insbesondere bei unerwarteten oder unklaren Anfragen.

Verlust
Melde den Verlust von digitalen Einsatzmitteln umgehend der Hotline.

Clean Desk
Halte Dich an die Clean Desk Policy (beim Verlassen des Raumes ist kein sensibles und schützenswertes Dokument für Dritte zugänglich, z. B. Kontaktlisten). In allen Situationen den Sichtschutz beachten.

SOZIALE MEDIEN & KOMMUNIKATION

Kommunikation
Verweise an die Kommunikationsverantwortlichen für sämtliche öffentliche Anfragen.

Posts auf sozialen Medien
Teile operative Inhalte nicht auf sozialen Medien oder mit unbeteiligten Personen.

Keine Standortfreigabe
Vermeidung der Freigabe des Standorts in privaten Apps; Standortdienste deaktivieren, wenn nicht benötigt, um Missbrauch von Standortdaten zu vermeiden.

Link-Vorschau
Deaktivierung von automatischen Medien- und Linkvorschauen, um potenzielle Schwachstellen zu vermeiden und vor schädlichen Inhalten zu schützen.

CYBER-VORFALL: RICHTIG HANDELN

1. Reagiere sofort – handle mit Bedacht!

- Nutze das Gerät nicht weiter: Öffne keine Programme oder Dateien, gebe keine Passwörter ein.
- Trenne das Gerät vom Netzwerk: Deaktiviere WLAN/LAN.
- Melde den Vorfall sofort an die Meldestelle.

2. Was kannst Du tun bei verdächtigen Inhalten?

- Lösche keine E-Mails und Nachrichten: Melde verdächtige Mails an die Meldestelle und dokumentiere Auffälligkeiten.
- Leite keine verdächtigen Links / Anhänge an andere weiter.

MELDESTELLE

Bitte wenden Sie sich an Ihren Service Desk oder ISBD des jeweiligen Departementes.

Eine Übersicht der ISBDs steht Ihnen im Intranet zur Verfügung.
Ansprechpartner Informationssicherheit