Kanton Zürich
Bildungsdirektion
Mittelschul- und Berufsbildungsamt
Digital Service Center Sek II

Kontakt: Mittelschul- und Berufsbildungsamt, Digital Service Center Sek II, Ausstellungsstrasse 80, 8090 Zürich
Telefon 043 259 77 27

Meldung Informationssicherheits-vorfall und Datenschutzverletzung

Prozess / Zuständigkeiten

Mitarbeitende / Lehrpersonen / SuS / Lernende	• Durchführen von potenziellen Erst-Massnahmen (Details am Ende des Dokumentes) • Meldung an vor Ort Support / IT
Schule / Vor Ort Support Schule	• Einleiten von Sofortmassnahmen • Meldung des Vorfalls über ITSM-Ticket SNOW (Incident)
Service Desk DSC	• Einleiten von Sofortmassnahmen • Rasche Triage des Tickets nach Vorfall / Schwere / Dringlichkeit / potenzielle Auswirkungen • Weiterleitung des Tickets an AFI SOC (Security Operation Center) • Information an die Verantwortlichen für Informationssicherheit und Datenschutz Sek II • Regelmässig Statusmeldungen an Meldende
Service Desk AFI	• Rasche Triage des Tickets nach Vorfall / Schwere / Dringlichkeit / potenzielle Auswirkungen • Weiterleitung des Tickets AFI SOC (Security Operation Center)
SOC AFI	• Massnahmen, analog 2nd Level • Einberufung CSIRT (Computer Security Incident Response Team) bei «grossen» Vorfällen • Information FAGIS, Datenschützerin des Kt. ZH, Regierung, NCSC
2nd / 3rd Level Verantwortliche DSC / AFI / Lieferanten	• Analyse des Vorfalls • Definition und Umsetzung von Massnahmen
Verantwortliche für Informationssicherheit und Datenschutz Sek II (ISID Sek II)	• Bestimmen von weiteren Massnahmen in Zusammenarbeit mit den technischen Verantwortlichen und SOC • Je nach Vorfall Information des Leiters DSC, Leiter Operation DSC, ISID BI, ggf. weitere

Leitung DSC	• Je nach Vorfall: Einberufung TaskForce zusammen mit Schule, SOC, Verantwortliche ISID Sek II, Behörden / Polizei, Lieferanten, 2nd-/ 3rd-Level Spezialisten

Wichtige Adressen / Tel-Nr.

Service Desk DSC	servicedesk.dsc@edu.zh.ch oder Telefon 043 259 77 27 Montag - Freitag 07:30 - 12:00 / 13:00 - 17:30 Uhr
Meldung potenziell „verseuchte“ Mail	check.opsec@abxsec.com
Security Operation Center AFI	servicedesk@bi.zh.ch / +41 43 259 23 00
Verantwortliche für Informationssicherheit und Datenschutz Sek II	Bettina.irnhauser@mba.zh.ch +41 43 259 83 06
Leitung DSC	Daniel.stoeri@mba.zh.ch +41 79 548 99 42
Leitung Operation DSC	kaan.oezsoy@mba.zh.ch
NCSC	https://www.ncsc.admin.ch/
Datenschützerin des Kt. ZH	https://datenschutz.ch/

Potenzielle Erst-Massnahmen

- Foto vom Bildschirm machen (ggf. mit Smartphone)
- PC / Laptop vom Netz trennen
- Ablauf notieren. Was ist genau passiert, möglichst jedes Detail
- Auswirkungen notieren: Was funktioniert nicht mehr? Was ist „komisch“ (langsam, unzuverlässig, bricht ab, etc.)
- PC / Laptop untersuchen mit spezialisiertem Malware-Scanner, z.B. Hitman Pro (https://www.ibarry.ch/de/sicherheits-checks/)

AFI SOC unterhält detaillierte Playbooks (Abläufe, Checklisten), um verschiedene Securityvorfälle abzuhandeln.