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

28. März 2025

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 Servicenow oder OTRS (Incident)
Service Desk DSC Sek II	• 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, Regierung, AFI-intern
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 Support und Operation DSC, ISID BI, Kommunikation MBA, ggf. weitere

Leitung DSC Sek II	• Je nach Vorfall: Einberufung TaskForce zusammen mit Schule, SOC, Verantwortliche ISID Sek II, Behörden / Polizei, Lieferanten, 2nd-/ 3rd-Level Spezialisten
Rektor/in	• Meldung des Vorfalls an das Bundesamt für Cybersicherheit (BACS) BACS Report • Meldung an die Datenschutzbeauftragte des Kantons Zürich https://datenschutz.ch/datenschutz-in-oeffentlichen-organen/datenschutzvorfall-melden

Wichtige Adressen / Tel-Nr.

Service Desk DSC Sek II	**servicedesk.dsc@edu.zh.ch** **oder Telefon 043 259 77 27** Montag - Freitag 07:30 - 12:00 / 13:00 - 17:30 Uhr
Security Operation Center AFI	https://serviceportal.zh.ch / +41 43 259 19 91
Verantwortliche für Informationssicherheit und Datenschutz Sek II	bettina.irnhauser@mba.zh.ch +41 43 259 83 06
Leitung DSC Sek II	daniel.stoeri@mba.zh.ch
Leitung Support und Operation DSC Sek II	ferhat.sutter@mba.zh.ch
Bundesamt für Cybersicherheit (BACS)	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.