## Merkblatt Informationssicherheitsvorfall (Incident)

### Einleitung

Informationssicherheitsvorfälle (Security Incidents) sind Ereignisse, welche die Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit von Informationen beeinträchtigen können. Der folgende Prozess definiert, wie solche Vorfälle innerhalb der Organisation erkannt, dokumentiert, klassifiziert, gemeldet und bearbeitet werden.

Das Merkblatt richtet sich in erster Linie an Schulen, die

### Definition des Sicherheitsvorfalls

Ein Sicherheitsvorfall ist jedes Ereignis, das die Informationssicherheit gefährdet, z.B.:

* unbefugter Zugriff auf Systeme oder Daten,
* Verlust oder Diebstahl von Geräten, die sensible Daten enthalten,
* Malware- oder Ransomware-Angriffe,
* Phishing-Versuche,
* Datenmanipulation oder -zerstörung.

### Erkennung von Incidents

Alle Lehrpersonen und Mitarbeitenden werden periodisch geschult, um Anzeichen von Sicherheitsvorfällen zu erkennen und zu melden.

### Dokumentation von Incidents

#### Meldeformular

Ein standardisiertes Formular (siehe Vorlage Meldung Informationssicherheitsvorfall) wird verwendet, um alle relevanten Details des Vorfalls zu erfassen.

#### Incident-Register

Alle Incidents werden intern durch die IT dokumentiert.

### Klassifizierung von Incidents

Vorfälle werden durch die IT nach ihrem Schweregrad klassifiziert:

* gering: Keine oder minimale Auswirkungen
* mittel: Mässige Auswirkungen, aber keine langfristigen Schäden
* hoch: Erhebliche Auswirkungen, möglicherweise langfristige Schäden

Die Klassifikation umfasst auch den betroffenen Bereich:

* Intern: Betrifft nur interne Systeme und Daten
* Extern: Betrifft auch externe Partner oder Kunden

### Meldung von Incidents

#### Interne Meldung

Alle Benutzer/innen der SCHULE-Infrastruktur sind verpflichtet, Vorfälle mittels Formular unverzüglich an das IT-Supportteam zu melden (E\_MAIL\_ADRESS\_SCHULE@edu.zh.ch). Das IT-Supportteam informiert die Schulleitung.

#### Meldung an DSC/MBA Service Desk

Alle Vorfälle (Klassifizierung mittel oder hoch) werden via IT-Supportteam dem DSC Sek II Service Desk gemeldet.

#### Meldung an die Datenschutzbeauftragte des Kantons (DSB)

Die Meldung an die DSB erfolgt durch die Schule. Informationen sind auf folgender Webseite einsehbar:

<https://datenschutz.ch/datenschutz-in-oeffentlichen-organen/datenschutzvorfall-melden>

### Bearbeitung von Incidents

#### Erstmassnahmen

Sofortige Massnahmen zur Eindämmung und Minderung der Auswirkungen durch den IT-Support:

* Passwortänderungen
* Isolierung betroffener Geräte
* Trennung vom Netzwerk
* Ausschalten WLAN

Allfällig weitere erforderliche Massnahmen (z.B. Abschaltung gesamtes System) erfolgen in Zusammenarbeit mit dem DSC Sek II und dem AFI.

#### Untersuchung und Analyse

Das IT-Sicherheitsteam führt eine gründliche Untersuchung durch, um die Ursache und den Umfang des Vorfalls zu ermitteln.

Genehmigung: Schulleitung