cyber-incident

General

- All cyber incidents has to be reported to UZH IT Security.
- UZH IT Security Office coordinates reports to Bundesamt für Cybersicherheit (BACS). Please no direct reports to BACS.
- UZH reporting to BACS must take place within 24 hours of internal discovery. Therefore, the internal report to the IT Security Office must be made within this timeframe.

What needs to be reported?

Incidents that

- Jeopardize the functionality of the affected critical infrastructure,
- result in manipulation or data leakage, or
- involve extortion, threats, or coercion.
- Examples of other types of attacks:
  - Malware successfully installed in the system
  - Ransomware
  - Attacks on availability (e.g., DDoS)
  - Unauthorized access to IT resources through exploitation of vulnerabilities

Who is responsible for reporting?

- **Every member of UZH** is responsible for complying with the internal reporting obligation for cyberattacks.
- Neither the Central IT Services (ZI) nor the CISO are liable for unreported cases from other organizational units.
- If the reporting obligation is repeatedly neglected, BACS can impose fines of up to CHF 100,000 on the responsible individual.

Report

Please report to support@math.uzh.ch (IT Coordinator). Please mention:

- What has been encountered?

- Which systems are affected?
- Is the system still operable? yes/no
  - If yes: remove network connection, remain on power (do not switch off).
- What type of information is affected (confidential / internal / public / personal data / business information)?
- Where is the device located?

If you are not contacted by us within one hour, please report to UZH IT Security:

https://sdesk.uzh.ch/tas/public/ssp/

Again: If we (=IT Support) do not respond within one hour, you have to report by yourself.

Original Request

```
Ab 1. April 2025 tritt die Meldepflicht für Cybervorfälle gegenüber dem
Bundesamt für Cybersicherheit (BACS) in Kraft. *Das bedeutet, dass die
Universität Zürich als Organisation – und somit wir alle – gesetzlich
verpflichtet sind, Cyberattacken unverzüglich zu melden.*

*Wichtig: Meldungen ans BACS werden zentral in Absprache mit dem CISO
der UZH und zusammen mit der IT-Sicherheitsstelle gemacht, nicht durch
die Einheiten selbst.*

*Was muss gemeldet werden?*

Eine Cyberattacke muss gemeldet werden, wenn diese die
Funktionsfähigkeit der betroffenen kritischen Infrastruktur gefährdet,
zu einer Manipulation oder zu einem Abfluss von Informationen geführt
hat oder mit Erpressung, Drohung oder Nötigung verbunden ist.

Beispiele für weitere Angriffsarten:

      * Erfolgreich im System installierte Schadsoftware
      * Verschlüsselungstrojaner
      * Angriffe auf die Verfügbarkeit
      * Unerlaubtes Eindringen in Informatikmittel durch das Ausnutzen von
        Schwachstellen.

*Wer muss melden?*

Die Verantwortung für die Einhaltung der internen Meldepflicht über
```

Cyberattacken liegt bei jedem/ jeder Angehörigen der UZH. Weder die Zentrale Informatik (ZI) der UZH noch der CISO haften bei ungemeldeten Fällen anderer Organisationseinheiten.

Wichtig zu wissen:

* UZH-intern besteht bereits eine Meldepflicht; sie ist im REIM verankert. (Siehe beispielhaft: §8 Abs 1, §12 Abs 4, §14 Abs 2, §19 Abs 3)
https://www.rud.uzh.ch/dam/jcr:3a57415b-727e-4799-8699-d4f1e199fa31/ REIM_2022-11-29_Stand-2024-11-05.pdf
<https://www.rud.uzh.ch/dam/jcr:3a57415b-727e-4799-8699-d4f1e199fa31/ REIM_2022-11-29_Stand-2024-11-05.pdf>

* Die externe Meldung muss *innerhalb von 24 h* nach der internen Entdeckung beim BACS erfolgen. Die interne Meldung an die IT Sicherheitsstelle muss also vor Ablauf der 24h erfolgen.
* ACHTUNG! Bei wiederholter Unterlassung der Meldepflicht kann das BACS Bussen bis zu CHF 100'000.- gegenüber einer säumigen Person aussprechen.

Wo muss gemeldet werden? – Umsetzung der Meldepflicht UZH-intern

Für die UZH-interne Meldung von Cybervorfällen ändert sich nichts. Bitte haltet euch an die bereits etablierten Prozesse und informiert eure Organisation entsprechend.

* Die IT-Sicherheitsstelle gibt als zentrale Ansprechstelle alle Meldungen über Cyberangriffe an das BACS weiter.
* Alle UZH-internen Meldungen erfolgen mit dem ‘*/Meldeformular für Cybervorfälle’/* > Startseite - Self Service Portal <https://sdesk.uzh.ch/tas/public/ssp/> oder direkt über den IT Service Desk.

Weiterführende Informationen

* Zu den internen Verantwortlichkeiten siehe beigelegte Präsentation vom 10. März 2025.
* Link zu den gesetzlichen Grundlagen: > Informationen zur Meldepflicht
<https://www.ncsc.admin.ch/ncsc/de/home/meldepflicht/meldepflicht- info.html>

```
Bei Fragen stehen wir euch gerne zur Verfügung: CISO@uzh.ch
<mailto:CISO@uzh.ch>
```

Revision #3
Created 2026-06-30 10:53:47 CEST by admino
Updated 2026-07-03 14:40:53 CEST by Jonas Valentin Rose