Protokollierung, Auswertung und Monitoring von Log-Daten an der ETH Zürich

Stand 01. Januar 2025

Der/die Chief Information Security Officer der ETH Zürich

gestützt auf Art. 6 Abs. 4 Bst. d und f der Weisung «Informationssicherheit an der ETH Zürich»[1]

v e r o r d n e t:

1. Abschnitt: Allgemeine Bestimmungen

Artikel 1 Gegenstand

[1] Diese Weisung regelt die Protokollierung, die Auswertung und das Monitoring der Systemaktivitäten von IT-Mitteln sowie von System- sowie Benutzeraktivitäten im Rahmen der Nutzung von IT-Mitteln an der ETH Zürich.

[2] Mit Protokollierung (Logging) ist die Aufzeichnung von Inhalten sowie von System- und Benutzeraktivitäten gemeint.

Auswertung bezeichnet die zielgerichtete Untersuchung aufgezeichneter Daten.

Monitoring ist die systematische Beobachtung, Erfassung oder Messung eines Vorgangs oder Prozesses mittels technischer Hilfsmittel, z.B. die Überwachung von Schwellenwerten, um bei Bedarf in einen Prozess einzugreifen.

IT-Mittel[2] sind alle IT-Geräte und IT-Dienste, welche im Eigentum oder im Auftrag der ETH Zürich eingesetzt werden. Dies beinhaltet auch Drucker, Scanner, Software, Telefonie sowie Haustechniksysteme, Gebäudeautomation und ausgelagerte Dienstleistungen wie externe Cloud-Dienste. Ausgenommen ist die Videoüberwachung gemäss Art. 36i ETH-Gesetz.

Artikel 2 Geltungsbereich

[1] Diese Weisung gilt für alle von der ETH Zürich verwalteten oder im Auftrag der ETH Zürich verwalteten IT-Mittel und betrifft jede Person, die solche IT-Mittel verwaltet oder auswertet bzw. deren Verwaltung oder Auswertung in Auftrag gibt oder genehmigt.

[2] Die Protokollierung, die Auswertung und das Monitoring von IT-Mitteln im Outsourcing wie z.B. die Anbindung externer Cloud-Dienste sind im Sinne dieser Weisung vertraglich separat mit dem Outsourcing-Anbieter bzw. mit dem Anbieter externer Cloud-Dienste zu regeln.

[1] RSETHZ 203.25

[2] Bundes-Terminologie: «elektronische Infrastruktur»

Artikel 3 Ziel und Zweck

[1] Diese Weisung regelt die Erkennung, die Verhinderung und den Nachvollzug sicherheitsrelevanter und betrieblicher Ereignisse durch Protokollierung und Auswertung von Daten sowie das Monitoring von IT-Mitteln.

[2] Diese Weisung bezweckt die Vermeidung und die Bewältigung sicherheitsrelevanter Ereignisse, welche die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen der ETH Zürich verletzen und in der Folge ein Schadenspotential für die Hochschule begründen können.

[3] Betriebliche Ereignisse beeinträchtigen den stabilen, unterbruchfreien Betrieb.

2. Abschnitt: Protokollierung

Artikel 4 Bestimmungsgemässe Protokollierung

[1] Bei der Nutzung von IT-Mitteln dürfen Daten zu folgenden Zwecken protokolliert werden[3]:

a. zur Aufrechterhaltung der Informations- und Dienstleistungssicherheit,
b. zur technischen Wartung der elektronischen Infrastruktur[4],
c. zur Kontrolle der Einhaltung von Nutzungsreglementen, namentlich der Benutzungsordnung für IT-Mittel an der ETH Zürich,
d. zum Nachvollzug des Zugriffs auf die elektronische Infrastruktur,
e. zur Erfassung der Kosten, die durch die Benutzung der elektronischen Infrastruktur entstehen,
f. zur Bewirtschaftung der Arbeitszeit: die Daten über die Arbeitszeiten des Personals,
g. zur Gewährleistung der Sicherheit: die Daten über das Betreten oder Verlassen von Gebäuden und Räumen der Bundesorgane und über den Aufenthalt darin.

Artikel 5 Zu protokollierende Inhalte

[1] System- und Benutzeraktivitäten sowie technische Sicherheitszustände der IT-Systeme (inklusive Konfiguration) dürfen protokolliert werden.

[2] Bei der Bearbeitung von Personendaten mit IT-Mitteln sind, wann immer technisch möglich, das Erstellen, Bearbeiten, Speichern, Ändern und Löschen zu protokollieren. Bei der automatisierten Bearbeitung von Personendaten (i.d.R. ohne menschliches Zutun) sind, wann immer technisch möglich, mindestens das Speichern, Ändern, Lesen, Bekanntgeben, Löschen und Vernichten zu protokollieren[5].

[3] Die Protokollierung gibt Aufschluss über die Art, das Datum und die Uhrzeit der Bearbeitung, die Identität der Person (bzw. die technische Identität), die die Bearbeitung vorgenommen hat, sowie gegebenenfalls die Identität der Empfängerin oder des Empfängers der Daten.

[4] Für sicherheitsrelevante Zwecke wird wie folgt protokolliert:

---

[3] BOT Art. 14 und Art. 57l Bst. b, c, d Regierungs- und Verwaltungsorganisationgesetz (RVOG, SR **172.010**)

[4] ETH-Terminologie: «IT-Mittel»

[5] Art. 4 Datenschutzverordnung vom 31. August 2022 (DSV; SR **235.11**)

a. synchronisierter Datum- und Zeitstempel (inkl. anwendbare Zeitzone)
b. Ursprung der Log-Daten (Applikations- / Servicename)
c. Aktivitäts- / Ereignis- / Fehler-Typ
d. Benutzer- oder Objekt-ID / Quellenadresse (IP-Adressen, MAC-Adresse, Hostname)
e. Zielsystem der Aktion (Daten, System, Ressource)
f. Hinweis, ob die Aktion erfolgreich war oder nicht

[5] Eine bestehende Protokollierung für sicherheitsrelevante Zwecke darf im Umfang nur ausnahmsweise und mit schriftlicher Bestätigung durch den/die CISO abgeändert werden.

[6] Für betrieblichen Zwecke können unter Einhaltung der Vorgaben dieser Weisung die aufzuzeichnenden Inhalte durch den Service Owner eines Systems ergänzt werden. Service Owner erbringen eine IT-Dienstleistung gegenüber dem Kunden und sind für besagte Dienstleistung über deren gesamten Lebenszyklus sowie Leistungsumfang verantwortlich.

3. Abschnitt: Auswertung[6]

Artikel 6 Bestimmungsgemässe Auswertung

[1] Log-Daten dürfen gemäss Art. 57m, 57n und 57o RVOG[7] wie folgt ausgewertet werden:

a. nicht personenbezogen;
b. stichprobenweise nicht namentlich personenbezogen (pseudonymisiert) oder
c. namentlich personenbezogen.

[2] Andere Erkenntnisse über die Tätigkeiten von Personen sind zu vermeiden. Falls solche Auswertungen entstehen, ist die/der CISO zu informieren und diese/dieser entscheidet über das weitere Vorgehen. Diese Art von Auswertungen gilt als streng vertraulich[8].

[3] Benutzerinnen und Benutzer haben kein Recht auf Auswertung ihrer Log-Daten.

Artikel 7 Nicht personenbezogene Auswertung

[1] Die nicht personenbezogene Auswertung aufgezeichneter Daten ist zulässig[9]:

a. zur Aufrechterhaltung der Informations- und Dienstleistungssicherheit;
b. zur technischen Wartung der elektronischen Infrastruktur;
c. zur Kontrolle der Einhaltung von Nutzungsreglementen, namentlich der Benutzungsordnung für IT-Mittel an der ETH Zürich[10];

---

[6] Vgl. Abschnitt 3. ff Verordnung über die Bearbeitung von Personendaten und Daten juristischer Personen bei der Nutzung der elektronischen Infrastruktur des Bundes (VBNIB; SR **172.010.442**)

[7] Regierungs- und Verwaltungsorganisationgesetz (RVOG, SR **172.010**)

[8] Art. 57m RVOG; beachte bei Datenauswertung das Berufs-, Geschäfts- und Amtsgeheimnis gem. Art. 57 Personalverordnung ETH-Bereich (PVO-ETH; SR **172.220.113**)

[9] Art. 57m Regierungs- und Verwaltungsorganisationsgesetz (RVOG; SR **172.010**)

[10] RSETHZ 203.21

d. zum Nachvollzug des Zugriffs auf die elektronische Infrastruktur[11] oder

e. zur Erfassung der Kosten, die durch die Benutzung der elektronischen Infrastruktur entstehen.

[2] Sie ist ferner zulässig:

a. bei allen Daten, einschliesslich des Inhalts elektronischer Post: zu deren Sicherung (Backups);

b. bei Daten über die Arbeitszeiten des Personals: zur Bewirtschaftung der Arbeitszeit;

c. bei Daten über das Betreten oder Verlassen von Gebäuden und Räumen der Bundesorgane und über den Aufenthalt darin: zur Gewährleistung der Sicherheit.

[3] Für die nicht personenbezogene Auswertung von Daten ist keine Anordnung des/der CISO notwendig.

Artikel 8 Nicht namentliche personenbezogene Auswertung

[1] Die nicht namentliche personenbezogene (pseudonymisierte) Auswertung aufgezeichneter Daten ist stichprobenartig zulässig[12]:

a. zur Kontrolle der Nutzung der elektronischen Infrastruktur oder

b. zur Kontrolle der Arbeitszeiten des Personals.

[2] Die Extraktion (Sicherstellung von Daten) oder Auswertung von nicht namentlichen personenbezogenen Aufzeichnungen erfolgt ausschliesslich auf Anordnung der/des CISO. Die nicht namentliche personenbezogene Auswertung von Daten erfolgt auf Anordnung des/der CISO[13].

Artikel 9 Namentliche personenbezogene Auswertung

[1] Die namentliche personenbezogene Auswertung aufgezeichneter Daten ist zulässig[14]:

a. zur Abklärung eines konkreten Verdachts auf Missbrauch der elektronischen Infrastruktur und Ahndung eines erwiesenen Missbrauchs;

b. zur Analyse und Behebung von Störungen der elektronischen Infrastruktur und Abwehr konkreter Bedrohungen dieser Infrastruktur;

c. zur Bereitstellung benötigter Dienstleistungen;

d. zur Erfassung und Fakturierung erbrachter Leistungen oder

e. zur Kontrolle der individuellen Arbeitszeiten.

[2] Auswertungen nach Abs. 1 Bst. a sind nur zulässig:

a. ausschliesslich im Auftrag der/des CISO;

b. wobei je nach der Schwere des Missbrauchs in der Regel zusammen mit dem/der direkten Vorgesetzten sowie weiteren für die betroffene Person zuständigen Personen (z.B. HR-Beratende, Studiendelegierte) entschieden wird, ob die Auswertung zur Identifikation der be-

[11] Diese Auswertung beinhaltet namentlich auch die Überprüfung der vertragsgemässen Nutzung von Software oder Software-Services (Software Asset Management).

[12] Art. 57n RVOG

[13] Ausgenommen sind übliche personenbezogene Auswertungen, wie z.B. bei ETHIS oder SAP.

[14] Art. 57o RVOG

troffenen Person sofort oder erst nach wiederholter Feststellung eines Missbrauchs erfolgt; oder

c. auf Antrag einer Strafbehörde, z.B. einer Staatsanwaltschaft und

d. erfolgen in jedem Fall nur, nachdem die betroffene Person schriftlich über den Missbrauchsverdacht informiert worden ist[15].

[3] Die Extraktion (Sicherstellung) von Daten zu Beweiszwecken nach Abs. 1 Bst. a ist nur zulässig:

a. ausschliesslich im Auftrag der/des CISO;

b. bei Bestehen eines konkreten Verdachts strafbarer Handlungen. Der Entscheid, ob Anzeige gegen fehlbare Mitglieder des Lehrkörpers oder Mitarbeitende der ETH Zürich erstattet wird, liegt beim Präsidenten der ETH Zürich.[16] Weitere personenbezogene Auswertungen obliegen allein der zuständigen Strafbehörde oder

c. auf Antrag einer Strafbehörde, z.B. einer Staatsanwaltschaft, wobei die Herausgabe der Daten nach Prüfung auf Verhältnismässigkeit durch den/die CISO erfolgt.

[4] Dringend erforderliche Sofortmassnahmen nach Abs. 1 Bst. a und b können auch von den IT-Betreibenden veranlasst werden, insbesondere vom Direktor bzw. der Direktorin der Informatikdienste oder dem IT-Services Leiter bzw. der Leiterin der jeweiligen organisatorischen Einheit. Solche Massnahmen sind unverzüglich dem/der CISO zur Genehmigung vorzulegen.

4. Abschnitt: Technisches Monitoring

Artikel 10 Überwachung und Scanning von Schwachstellen

[1] Werden IT-Mittel der ETH Zürich genutzt oder in deren Auftrag betrieben, so dürfen für die in Art. 4, Art. 7, Art. 8 und Art. 9 beschriebenen Zwecke folgende Daten zur Feststellung von Schwachstellen erhoben (gescannt) und ausgewertet werden:

a. Daten über den technischen Stand jener IT-Mittel, z.B. Patch-Stände, offene Ports, verwendete Protokolle, Betriebssystem-Version etc. und/oder

b. die Randdaten über die Nutzung jener IT-Mittel, z.B. welcher Telefonanschluss, E-Mail- oder IP-Adresse etc. hat wann, wie lange und mit wem kommuniziert.

[2] Scanning für betriebliche, wie für sicherheitsrelevante Zwecke ist den zuständigen Stellen innerhalb ihres Verantwortungsbereichs erlaubt (insb. zuständige Systemverantwortliche, Cyber and Information Security Center - CISEC).

[15] Art. 57o Abs. 2 RVOG.

[16] Art. 14 Abs. 2 Geschäftsordnung der Schulleitung vom 10. August 2004 (RSETHZ 202.3).

5. Abschnitt: Aufbewahrung und Löschung

Artikel 11 Löschfristen

[1] Daten gemäss dieser Weisung sind, soweit der Auswertungszweck dies erfordert, spätestens nach der unten aufgeführten Aufbewahrungszeit durch die zuständige Stelle zu löschen[17] (Ausnahme: bring your own device, BYOD):

a. für Backups aller Daten, einschliesslich des Inhalts elektronischer Post, sofern diese vom Hochschularchiv nicht übernommen werden: höchstens **2 Jahre**;

b. für Daten über die Nutzung der elektronischen Infrastruktur gemäss Art. 4, insbesondere auch Daten über den technischen Zustand der IT-Mittel sowie Randdaten (sicherheitsrelevante Ereignisse gemäss Art. 3): höchstens **2 Jahre**;

c. für Daten über die Arbeitszeiten des Personals zur Bewirtschaftung der Arbeitszeit**:** höchstens **5 Jahre** und

d. für Daten über das Betreten oder das Verlassen von Gebäuden und Räumen der ETH Zürich und über den Aufenthalt darin zur Gewährleistung der Sicherheit: höchstens **3 Jahre**.

[2] Protokolldaten zu Personendaten sind mindestens **1 Jahr**[18] aufzubewahren. Für Personaldossiers und medizinische Personaldaten gilt Art. 10 Personendatenschutzverordnung ETH-Bereich[19] (Personaldossier: Aufbewahrungsdauer 10 Jahre).

[3] Log-Daten zu betrieblichen Ereignissen gemäss Art. 3 und Art. 10 dürfen maximal **180 Tage** lang aufbewahrt werden.

Artikel 12 Auswertungen

[1] Für sichergestellte Daten und Auswertungsergebnisse gelten die Löschfristen gemäss Art. 11 nicht.

[2] Daten, die ausgewertet werden, dürfen nur so lange aufbewahrt werden, wie sie erforderlich sind. Sie sind spätestens drei Monate nach Abschluss der Auswertung oder nach Ablauf der Aufbewahrungsfristen nach Abs. 1 durch die zuständigen Stellen zu vernichten.

6. Abschnitt: Zentralisierte Speicherung im CISEC Log-Container

Artikel 13 Weiterleitung von Log-Daten

[1] Sicherheitsrelevante Log-Daten sind nach Anforderung des CISEC an dieses zu übermitteln. Der/die Service Owner/in überträgt seine/ihre Log-Daten mittels geeigneter Schnittstelle unverändert und verschlüsselt als Realtime-Information in den dafür vom CISEC designierten Log-Container. Die Weiterleitung erfolgt nach Rücksprache. Die Speicherung der Log-Daten beim CISEC dient der Identifikation potenzieller Sicherheitsrisiken.

---

[17] Art. 4 Verordnung über die Bearbeitung von Personendaten und Daten juristischer Personen bei der Nutzung der elektronischen Infrastruktur des Bundes (VBNIB; SR **172.010.442**)

[18] Art. 4 Datenschutzverordnung (DSV; SR **235.11**); Art. 9 Personendatenschutzverordnung ETH-Bereich (PDV-ETH; SR **172.220.113.14**)

[19] Art. 10 Personendatenschutzverordnung ETH-Bereich (PDV-ETH; SR **172.220.113.14**)

Der/Die Service-Owner/in darf Log-Daten im Sinne dieser Weisung lokal speichern. Geliefert werden müssen grundsätzlich Log-Daten:

a. wichtiger Applikationen oder Datenbanken aktiv bewirtschafteter Personendaten;
b. zu IT-Mittel, die kritische Prozesse gemäss Risikomanagement der ETH Zürich unterstützt;
c. von IT-Mittel mit hohem oder sehr hohem Schutzbedarf[20]

[2] Das CISEC benachrichtigt im Falle einer Unterbrechung der Übertragung den/die Service Owner/in.

[3] Das CISEC leitet Informationen zu identifizierten Sicherheitsrisiken sowie zu konkreten sicherheitsrelevanten Vorfällen, an die zuständigen Stellen weiter (z.B. Systemverantwortliche, Service-Vermittelnde).

7. Abschnitt: Sicherheitsanforderungen

Artikel 14 Vertraulichkeit

[1] Log-Daten sind mindestens als vertraulich klassifiziert.

[2] Sicherheitsrelevante, personenbezogene Auswertungen gelten als vertraulich, sofern diese von der/dem CISO nicht als streng vertraulich klassifiziert werden.

[3] Jeder Zugriff auf Log-Daten und Auswertungen ist stark eingeschränkt:

a. Beigezogene Dritte werden sorgfältig ausgewählt, nach Bedarf einer Personensicherheitsüberprüfung (PSP) unterzogen und zur Wahrung der Vertraulichkeit verpflichtet (Geheimhaltungsvereinbarung).
b. Der Zugriff auf Log-Daten ist für Personen soweit möglich mittels aktuell geltenden Zugriffsschutz-Mechanismen wie Multifaktor- (MFA) oder zertifikatsbasierte Authentisierung (SSH) abzusichern.

[4] Der Zugriff auf Log-Daten für betriebliche Auswertungen wird auf ETH-Mitarbeitende mit Administrationsrollen beschränkt.

[5] Der Zugriff auf den CISEC Log-Container wird auf Mitarbeitende des CISEC eingeschränkt und muss nachvollziehbar sein. Mitarbeitende im CISEC und berechtigte Personen müssen zwingend einer erweiterten Personensicherheitsüberprüfung (PSP) unterzogen werden.

[6] Der/die ISO entscheidet über die Vergabe zusätzlicher Berechtigungen im eigenen Verantwortungsbereich. Diese sind periodisch zu überprüfen (jährlich oder bei Bedarf). Die Entscheide sind in nachvollziehbarer Weise revisionssicher zu dokumentieren und können von der/die CISO geprüft werden.

Artikel 15 Integrität

[1] Log-Daten müssen nachvollziehbar, vollständig und inhaltlich unverändert sein:

a. sie dürfen nicht gelöscht oder geändert werden.
b. Die Protokollierung darf nicht abgeschaltet werden.

[20] Weisung Inventarisierung und Klassifizierung RSTEHZ 203.28

c. Es muss genügend Speicherkapazität zur Verfügung gestellt werden, so dass keine Einträge verloren gehen bzw. überschrieben werden. Eine vordefinierte Reduktion der Log-Daten ist nach Rücksprache mit dem CISEC möglich.

d. Die zeitliche Reihenfolge der Log-Einträge ist korrekt: alle Systeme setzen auf eine Network Time Protocol (NTP) basierte Zeitsynchronisation.

[2] Änderungen an der Protokollierung sind zu dokumentieren.

[3] Als Service Owner des Log-Containers stellt das CISEC sicher,

a. dass die Daten im Log-Container sicher aufbewahrt, regelkonform ausgewertet und fristgerecht gelöscht werden und

b. die Log-Quellen, Aufbewahrungsfristen, Auswertungen und Löschungen dokumentiert sind.

Artikel 16 Verfügbarkeit

[1] Der/die Service Owner/in überwacht fortlaufend die Protokollierung und stellt Log-Daten seiner/ihrer IT-Mittel bereit. Er/sie stellt sicher, dass

a. die Protokollierung gemäss den Anforderungen des CISEC konfiguriert und verfügbar ist;

b. Verzögerungen von Log-Lieferungen in den CISEC Log-Container eliminiert werden und

c. die Einhaltung dieser Vorschriften nicht umgangen wird.

[2] Es ist nach Rücksprache mit dem CISEC die maximal tolerierbare Zeitspanne einzuhalten, während welcher eine Protokollierung maximal aussetzen darf.

8. Abschnitt: Pflichten

Artikel 17 Service-Vermittelnde

[1] Service-Vermittelnde beziehen externe IT-Dienstleistungen (z.B. Cloud-Dienstleistungen) und stellen diese Dienste Angehörigen sowie Gästen der ETH Zürich zur Verfügung.

[2] Service-Vermittelnde vereinbaren mit einem externen Cloud-Anbieter die Protokollierung, die Auswertung und das Monitoring im Sinne dieser Weisung.

Artikel 18 Systemverantwortliche

[1] Systemverantwortliche tragen die Verantwortung für ein zugeordnetes IT-Mittel bzw. eine Netzwerkzone.

[2] Mit Bezug zur Protokollierung, Auswertung und Monitoring: Systemverantwortliche

a. protokollieren die Ereignisse auf ihren IT-Mitteln;

b. stellen diese Log-Daten auf Aufforderungen hin dem Service Owner bzw. dem CISEC zur Verfügung und

c. löschen unwiederbringlich ihre Log-Daten nach Ablauf der maximalen Aufbewahrungszeit gemäss Abschnitt 5.

d. melden einen allfällig festgestellten Missbrauch oder einen konkreten Verdacht auf Missbrauch umgehend and den/die CISO.

[3] Systemverantwortliche sind Informationseignerinnen bzw. -eigner ihrer Log-Daten.

Artikel 19 Service Owner

[1] Service Owner erbringen eine IT-Dienstleistung gegenüber den Kunden und sind für besagte Dienstleistung über deren gesamten Lebenszyklus sowie Leistungsumfang verantwortlich.

[2] Mit Bezug zur Protokollierung, Auswertung und Monitoring: Service Owner

a. richten für ihre Umgebung eine geeignete Logging-Infrastruktur ein.
b. protokollieren und «monitoren» gemäss den Vorgaben dieser Weisung
c. löschen unwiederbringlich ihre Log-Daten nach Ablauf der maximalen Aufbewahrungszeit gemäss Abschnitt 5.
d. überwachen die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Log-Daten bzw. stellen diese sicher.
e. legen die aufzuzeichnenden Log-Daten gemäss den Anforderungen des CISEC fest.
f. bieten ihre Log-Daten in geeigneter Form dem CISEC an bzw. stellen dies als dienstleistungserbringende Instanzen zusammen mit den Systemverantwortlichen sicher.
g. stellen ihre Log-Daten nur autorisierten Personen zu.
h. führen betrieblich relevante nicht personenbezogene Auswertungen in Eigenverantwortung durch.
i. holen bei nicht namentlichen bzw. bei namentlichen personenbezogenen Auswertungen gemäss Abschnitt 3 die dafür benötigte Autorisierung der/des CISO ein.
j. melden einen allfällig festgestellten Missbrauch oder einen konkreten Verdacht auf Missbrauch umgehend and den/die CISO.

[3] Service Owner sind die Informationseignerinnen bzw. -eigner der Log-Daten.

Artikel 20 Information Security Officer

[1] Die Information Security Officer (ISO) sind in ihrem Verantwortungsbereich erste Anlauf- und Beratungsstelle für alle Belange der Informationssicherheit.

[2] Mit Bezug zum Zugriff auf Log-Daten: Der/die ISO

a. entscheidet über zusätzliche, notwendige Berechtigungen im eigenen Verantwortungsbereich;
b. dokumentiert die Entscheide bezüglich zusätzlicher privilegierter Zugriffsrechte für den eigenen Verantwortungsbereich und
c. überprüft periodisch Entscheide bzgl. der Vergabe zusätzlicher privilegierter Zugriffsrechte.

Artikel 21 Cyber and Information Security Center

[1] Das CISEC ist im Auftrag des/der CISO ETH Zürich-weit für die technisch-operative Behandlung von Informationssicherheitsvorfällen sowie zur Überprüfung von IT-Mitteln auf Sicherheitsmängel zuständig.

[2] Mit Bezug zur Protokollierung, Auswertung und Monitoring: Das CISEC

a. ist ETH-weit zuständig für das zentralisierte Log-Management sicherheitsrelevanter Log-Daten und die Durchführung sicherheitsrelevanter Auswertungen.
b. betreibt den zentralen CISEC Log-Container und überwacht den Empfang der Log-Daten.

c. gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit der von den IT-Mitteln übermittelten Log-Daten während des gesamten Lebenszyklus.

d. meldet dem/der CISO einen aufgrund einer Auswertung festgestellten Missbrauch oder einen konkreten Verdacht auf Missbrauch.

[3] Das CISEC ist Informationseignerin der zentralisierten, sicherheitsrelevanten Log-Daten.

Artikel 22 Chief Information Security Officer

[1] Der/Die Chief Information Security Officer der ETH Zürich (CISO) ist zuständig für die Informationssicherheit an der ETH Zürich.

[2] Mit Bezug zur Protokollierung, Auswertung und Monitoring: Der/die CISO

a. ist ausschliessliche/r Auftraggeber/in nicht namentlich und namentlich personenbezogener Auswertungen;

b. entscheidet über eine Verlängerung der Aufbewahrung nicht namentlich und namentlich personenbezogener Auswertungen und den zugrunde liegenden Log-Daten;

c. kann die Einhaltung der Vorgaben dieser Weisung überprüfen;

d. kann Massnahmen und Sanktionen insbesondere im Falle einer nicht bestimmungsgemässen Auswertung von Log-Daten anordnen.

[3] Der/die CISO ist Informationseignerin bzw. -eigner nicht personenbezogener Auswertungen und der zugrunde liegenden Log-Daten.

9. Abschnitt: Compliance

Artikel 23 Verstösse und Sanktionen

Aufgrund einer Auswertung von Daten darf der/die CISO sichernde und vorsorgliche Massnahmen oder Sanktionen gemäss Abschnitt 4 der Benutzungsordnung IT-Mittel an der ETH Zürich anordnen.

Artikel 24 Missbräuchliche Auswertung protokollierter Daten

[1] Der/die CISO kann die Einhaltung der Vorgaben dieser Weisung prüfen oder prüfen lassen.

[2] Bei nicht bestimmungsgemässer Auswertung von Log-Daten kann die/der CISO folgende Massnahmen und Sanktionen anordnen:

a. Abmahnung sowie im Wiederholungsfall Weiterleitung an die Rechtsabteilung / VPPL / Rektorat oder sonstige zuständige Stelle zur weiteren Behandlung

b. die vorsorgliche Sperrung des Zugangs zu den Log-Servern

c. die Blockierung/Sicherung der Daten zu Beweiszwecken.

[3] Die vorsätzliche oder wiederholte nicht bestimmungsgemässe Auswertung von Log-Daten gilt als schwerer Missbrauch und kann disziplinarische oder personalrechtliche Massnahmen zur Folge haben.

[4] Die Kenntnis schweren Missbrauchs im Sinne von Absatz 3 verpflichtet zur Meldung an den/die CISO.

10. Abschnitt: Schlussbestimmungen

Artikel 25 Inkraftsetzung

Diese Weisung tritt am 01. Januar 2025 in Kraft. Artikel 5 Absatz 2 (Protokollierung von Personendaten) ist prüfbar ab 01. Januar 2027.

Zürich, 01. Januar 2025

Johannes Hadodo
Chief Information Security Officer
ETH Zürich