IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich

vom 01. Januar 2025

Der Vizepräsident für Infrastruktur und Nachhaltigkeit der ETH Zürich und der Chief Information Security Officer der ETH Zürich

gestützt auf Art. 13, Abs. 3 Bst. g der «Organisationsverordnung ETH Zürich»[1] sowie auf Art. 6 Abs. 4 Bst. d und f der Weisung «Informationssicherheit an der ETH Zürich»[2]

v e r o r d n e n:

Abschnitt 1: Allgemeine Bestimmungen

Artikel 1 Gegenstand

[1] Diese Weisung regelt:

- Aufgaben, Kompetenzen und Verantwortlichkeiten zentraler Rollen im IT-Betrieb
- den Grundschutz für und den Umgang mit IT-Mitteln

[2] Diese Weisung bezweckt, dass für alle IT-Mittel eine verantwortliche Person identifiziert ist und erreicht werden kann und dass bekannte Schwachstellen zeitgerecht beseitigt werden. Zudem regelt sie den Umgang mit externen IT-Diensten. Unter externen IT-Diensten wird eine von der ETH Zürich bezogene IT-Dienstleistung, die ausserhalb des Netzwerks der ETH Zürich von einer Fremdfirma erbracht wird verstanden (z.B. Outsourcing, externer Cloud-Dienst).

[3] IT-Mittel 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 richtet sich an System- und Netzwerkzonenverantwortliche sowie an Service-Vermittelnde der ETH Zürich gemäss Abschnitt 2 dieser Weisung.

Abschnitt 2: Rollen

Artikel 3 Netzwerkzonenverantwortliche

[1] Netzwerkzonenverantwortliche sind verantwortlich für die Sicherheit ihrer Zonen und die dazugehörigen Prozesse.

[2] Die Aufgaben sind:

a. Teilnahme an der von den Informatikdiensten angebotenen Ausbildung für Netzwerkzonenverantwortliche;

[1] RSETHZ 201.021
[2] RSETHZ 203.25

b. Dokumentation der Einsatzzwecke der ihnen zugeteilten Netzwerkzonen;

c. Erstbeurteilung von Ausnahmeanträgen zu IT-Mitteln in ihrer Netzwerkzone, sowie die Weiterleitung der von ihm/ihr unterstützten Anträge an die/den Chief Information Security Officer (CISO) und

d. Kenntnis der Systemverantwortlichen für alle IT-Mittel in ihren Zonen.

[3] Die Kompetenzen sind:

a. Festlegen der Einsatzzwecke der ihnen zugeteilten Netzwerkzonen. Der Einsatzzweck einer Netzwerkzone muss mit dem Typ der bei den Informatikdiensten beantragten Netzwerkzone korrespondieren (z.B. DMZ, IoT, BYOD);

b. Entscheidung, welche IT-Mittel sich in ihre Zonen verbinden dürfen, wobei als Rahmenbedingung dem Typ der Netzwerkzone entsprochen werden soll;

c. Entscheidung über Änderungsanträge bezüglich der Konfigurationen ihrer Zonenfirewalls gemäss Art. 7, Abs. 5 dieser Weisung;

d. Ablehnung von Ausnahmeanträgen, die sich auf IT-Mittel in Netzwerkzonen ihrer Zuständigkeit beziehen gemäss Art. 11 dieser Weisung und

e. Beantragen von Ausnahmen bezüglich der Einhaltung der IT-Richtlinien und IT-Grundschutzvorgaben.

[4] Die Organisationseinheiten dürfen ihre Aufgaben bezüglich Netzwerkzonen (inkl. allfällige Zonenfirewalls) an ETH Zürich-interne Dienstleister delegieren. Voraussetzung dafür ist der Abschluss eines schriftlichen Service Level Agreements (SLA) unter Berücksichtigung der anwendbaren Vorgaben dieser Weisung. Im Falle einer Delegation bleiben die Organisationseinheiten für die Auftragserteilung und die Kontrolle der SLA-Einhaltung verantwortlich.

[5] Die Organisationseinheiten melden die Netzwerkzonenverantwortlichen an die Informatikdienste. Wird eine Zone durch eine Firewall geschützt, muss zusätzlich zur/zum Netzwerkzonenverantwortlichen mindestens eine, maximal drei Stellvertretungen gemeldet werden.

Artikel 4 Systemverantwortliche

[1] Systemverantwortliche sind verantwortlich für die System- sowie Systemsicherheitspflege und der dazugehörigen Prozesse im Rahmen der anwendbaren Vorgaben dieser Weisung.

[2] Die Kompetenzen sind das Beantragen von Ausnahmen gemäss Art. 11 dieser Weisung.

[3] Für IT-Mittel im Eigentum der ETH Zürich dürfen die Organisationseinheiten ihre Aufgaben bezüglich Systeme an ETH Zürich-interne Dienstleister delegieren. Im Falle einer Delegation bleiben die Organisationseinheiten für die Auftragserteilung und die Kontrolle der Auftragserfüllung verantwortlich.

[4] Für nicht ETH Zürich-eigene IT-Mittel im Netzwerk der ETH Zürich, wie beispielsweise private IT-Systeme von Studierenden (BYOD) oder IT-Systeme Dritter wie die auftragsbezogene Verwen-

dung von Laptops oder Smartphones externer Dienstleistenden, gilt der/die angemeldete Benutzer/in als Systemverantwortliche/r, sofern keine Systemverantwortliche oder kein Systemverantwortlicher gemeldet ist.

[5] Die Organisationseinheiten melden die von ihnen ernannten Systemverantwortlichen und deren Stellvertretungen an die Informatikdienste (Ausnahme: BYOD).

Artikel 5 Service-Vermittelnde

[1] Service-Vermittelnde können IT-Betreibende sowie technisch-administrative Mitarbeitende der Departemente und der zentralen Organe oder aber auch wissenschaftliche Mitarbeitende in Forschung und Lehre einschliesslich Professorinnen und Professoren, Dozierende und externe Lehrbeauftragte der ETH Zürich sein[3].

[2] IT-Betreibende für die ETH Zürich sind namentlich die Informatikdienste, die IT Services Groups (ISG) der Departemente und der zentralen Organe sowie Professuren mit eigener IT und das CSCS.

[3] Service-Vermittelnde beziehen externe IT-Dienstleistungen (z.B. Cloud-Dienste, Outsourcing) und stellen diese ETH-Angehörigen zur Verfügung. In diesem Rahmen verantworten sie das Vertragsmanagement mit dem externen Anbieter, insbesondere einhergehend mit der Ver-antwortung für die technische Anbindung des Dienstes und das User-Life-Cycle Management. Dies beinhaltet:

a. Vereinbarung der anwendbaren Vorgaben dieser Weisung und Kontrolle von deren Einhaltung und

b. Freigabe des externen Dienstes zur Nutzung innerhalb der ETH entsprechend dem vorgesehenen Einsatzzweck (Verfassen der Nutzungsbedingungen).

[4] Die Aufgaben sind:

a. Kontrolle der Einhaltung der Vertragsbestandteile und bei Bedarf einfordern notwendiger Verbesserungen bei Service-Anbietern;
b. Bei Bedarf Festlegen und Umsetzung ergänzender technischer oder organisatorischer Massnahmen zur Absicherung des externen IT-Dienstes wie z.B. Backup, Logging, Reporting;
c. Bereitstellen der Dokumentation für Benutzende. Diese erläutert Einsatzzweck und die geltenden Nutzungsbedingungen, wie beispielsweise die Freigabe oder das Verbot der Bearbeitung von vertraulichen Informationen mit dem externen IT-Dienst;
d. Periodisch prüfen, ob und wie die Daten der ETH Zürich bei einem möglichen Nutzungsende des externen IT-Services in IT-Dienste der ETH Zürich migriert werden können und
e. Sicherstellen, bei Nutzungsende des externen IT-Dienste die Daten der ETH Zürich in IT-Dienste der ETH Zürich migriert werden können.

[3] z.B. Professor/innen, Departementskoordinator/innen, Abteilungsleiter/innen

[5] Die Kompetenzen sind:

a. Entscheid über Einsatzzweck des externen IT-Dienstes und der für die Angehörigen der ETH Zürich geltenden Nutzungsbedingungen.

b. Beantragen von Ausnahmen bei Nicht-Einhaltung der Vorgaben dieser Weisung gemäss Art. 11.

[6] Die Service-Vermittelnden melden den externen IT-Dienst, dessen Einsatzzweck und Nutzungsbedingungen dem/der Chief Information Security Officer (CISO). Der/Die CISO ist zuständig für die Informationssicherheit.

[7] Benutzende, die eine externe IT-Dienstleistung ausschliesslich für sich selbst beziehen, gelten nicht als Service-Vermittelnde. Als Benutzerinnen oder Benutzer gelten die Angehörigen der ETH Zürich gemäss Art. 13 ETH-Gesetz (namentlich Mitarbeitende und Studierende) sowie Gäste gemäss Gästereglement.

Artikel 6 Erreichbarkeit

Systemverantwortliche, Netzwerkzonenverantwortliche, Service-Vermittelnde und deren Stellvertretungen müssen innerhalb eines Arbeitstages auf Meldungen und Anfragen bezüglich möglicher IT-Sicherheitsvorfälle reagieren.

Abschnitt 3: IT-Grundschutzvorgaben

Artikel 7 Vorgaben für Netzwerkzonenverantwortliche

[1] Nach Möglichkeit sollen IT-Mittel nur in jener Zone des Netzwerkes der ETH Zürich platziert oder verbunden werden, die einen ähnlichen Schutzbedarf und Einsatzzweck haben.

[2] Enthält eine Zone IT-Mittel, bei denen die Vorgaben dieser Weisung länger als 20 Tage nicht eingehalten werden, ist die Zone so zu isolieren, dass allfällige Schwachstellen von ausserhalb der Zone nicht ausnutzbar sind. Alternativ können die betroffenen Systeme in eine bereits isolierte Zone verschoben werden.

[3] Die Netzwerkzonenverantwortlichen kennen für alle IP-Adressen/IT-Mittel die zuständigen Systemverantwortlichen in ihrer Netzwerkzone oder können diese zeitnah eruieren.

[4] Die Verwendung von IP-Adressen muss regelmässig überprüft werden (DHCP-Fixierungen). Ungenutzte IP-Adressen müssen den Informatikdiensten zurückgegeben werden.

[5] Firewalls sind so zu konfigurieren, dass sämtliche Dienste standardmässig geschlossen und nur wirklich benötigte Dienste geöffnet sind («white-list»). Ports und/oder Protokolle werden durch die Informatikdienste nur mit Bewilligung der/des Netzwerkzonenverantwortlichen geöffnet. Die/Der Netzwerkzonenverantwortliche beurteilt Firewall-Regeln auch vor dem Hintergrund der Stabilität und Verwundbarkeit des Netzwerks sowie des Schutzbedarfs der Datenbestände.

[6] Aktivierungen, Änderungen und Deaktivierungen von Firewall-Regeln müssen nachvollziehbar sein. Für jede Firewall-Regel ist der/die Antragsteller/in, der/die Ausführende, der Zweck/die Funktionalität sowie der Zeitpunkt zu dokumentieren.

[7] Firewall-Regeln müssen mindestens jährlich überprüft und aktualisiert werden. Nicht mehr benötigte Regeln sind zu entfernen.

[8] Firewall-Logs müssen durch die Netzwerkzonenverantwortlichen periodisch auf Unregelmässigkeiten überprüft werden.

[9] Benutzende und IT-Systeme müssen sich über Network Access Control-Technologien (NAC) authentisieren resp. autorisieren, um in eine Zone verbunden zu werden. Die Liste an zugelassenen Benutzenden und IT-Systemen (Zertifikate, MAC-Adressen) wird regelmässig überprüft. Authentisierungs- und Autorisierungs-Logs werden periodisch durch die Netzwerkzonenverantwortlichen auf Unregelmässigkeiten überprüft (RADIUS).

[10] Jedes IT-System muss einen Eintrag im Domain Name System (DNS) der Informatikdienste haben. Die DNS-Konfigurationen einer Zone müssen regelmässig überprüft und aktualisiert werden.

[11] Netzwerkanschlüsse müssen mit NAC-Technologien vor Fremdzugriffen geschützt werden. Netzwerkanschlüsse, die nicht mit NAC geschützt sind, dürfen sich ausschliesslich in geschlossenen Räumen befinden, in die nur berechtige Personen Zutritt haben (Ausnahme z.B. Hörsäle oder analog dazu).

Artikel 8 Vorgaben für Systemverantwortliche

[1] Aktualität der Software

a. Firmware, Betriebssysteme, Applikationen, Apps, etc. muss in aktuellen, vom Hersteller unterstützten Versionen eingesetzt und bezüglich Sicherheitsaktualisierungen auf neuestem Stand sein.

b. Sicherheitsaktualisierungen müssen unmittelbar nach dem Erscheinen getestet und schnellstmöglich verteilt werden. Spätestens nach zehn Kalendertagen ab ihrem Erscheinungsdatum müssen Aktualisierungen auf die Zielsysteme verteilt werden ausser es überwiegen betriebliche Probleme und Risiken.

c. Aktualisierungen und ein allfälliger Neustart der Zielsysteme müssen spätestens zwei Arbeitstage nach der Verteilung erfolgen ausser es überwiegen betriebliche Probleme und Risiken.

d. Bei Notfällen können die/der CISO oder die zuständigen IT-Betreibenden eine unmittelbare Verteilung und Installation von Sicherheits-aktualisierungen anordnen.

[2] Schutz vor Schadprogrammen

a. Sofern verfügbar und nutzbringend, müssen IT-Mittel mit Malware-Scannern betrieben werden.

b. Die Schutzprogramme müssen aktuell sein bzgl. Software-Version, Updates und Schutzsignaturen und sind so zu konfigurieren, dass Dateien automatisch bei Zugriff geprüft werden.

c. Zur Laufzeit eines IT-Systems muss automatisch - nach Möglichkeit mindestens stündlich - nach Aktualisierungen gesucht und diese eingespielt werden.

[3] Speichermedien von Desktops und mobilen Geräten wie Laptops, Tablets und Smartphones sind, sofern möglich, vollständig zu verschlüsseln.

[4] Spätestens nach 10 Minuten Inaktivität muss auf den IT-Mitteln eine Bildschirmsperre aktiviert werden (Ausnahmen z.B. durch einen adäquaten Zutrittsschutz). Diese lässt sich nur durch Eingabe eines Passwords, PINs, Fingerabdrucks oder mittels ähnlichen Authentisierungsmethoden freischalten.

[5] Zugriffskontrolle

a. Der Zugriff auf priviligierte Konten, wie beispielsweise «admin» oder «root», oder zu Gruppen mit Administrationsprivilegien, wie z.B. «Administratoren» oder «sudoers», muss auf möglichst wenige, für die jeweilige Rolle autorisierte Personen beschränkt werden (need-to-know Prinzip).

b. Konten für die Systemadministration müssen auf das notwendige Minimum (Least Privilege) eingeschränkt und regelmässig überprüft werden.

c. Zugriffe auf vertrauliche oder streng vertrauliche Datenbestände oder auf IT-Mittel mit hohem oder sehr hohem Schutzbedarf bzgl. Integrität oder Verfügbarkeit darf nur den verifizierbar bzw. individuell berechtigten Personen zur Verfügung gestellt werden. Die Zugriffsrechte werden zudem regelmässig überprüft.

d. Geteilte Benutzungskonten (shared accounts) sind nur gestattet, sofern diese zwingend erforderlich sind. Zugriffe dürfen nur den berechtigten Personen zur Verfügung gestellt werden. Die Zugriffberechtigungen müssen regelmässig überprüft werden.

e. Nicht verwendete, vorkonfigurierte Benutzungskonten (z.B. «guest») müssen gelöscht werden. Falls das nicht möglich ist, müssen sie deaktiviert bzw. für eine Anmeldung gesperrt werden. Das voreingestellte Passwort muss gewechselt werden.

[6] Die Passwort- und PIN-Regeln der ETH Zürich müssen, sofern technisch möglich, z.B. im IAM, Active Directory oder auf den lokalen Medien konfiguriert werden.

[7] Datensicherung

a. Die Datensicherung muss als Vertragsbestandteil geregelt oder anderweitig dokumentiert sein.

b. Die Wiederherstellbarkeit von Backups muss periodisch stichprobenartig geprüft werden.

[8] Fernzugriff bedeutet der Zugang zu IT-Mitteln von ausserhalb des Datennetzes der ETH Zürich (remote access). Es gilt:

a. Fernzugriffe dürfen nur mit aktuell als sicher geltenden Verschlüsselungsprotokollen erfolgen.

b. Bei Verwendung von Virtual Private Network (VPN) als Zugangstechnologie muss der Zugriff auf dem VPN-Endpunkt der Informatikdienste terminieren.

c. Alternative Fernzugriffsmethoden zum VPN (wie «Jump Hosts», SCION, Protokoll-Tunneling, Proxy-Technologien) müssen geschützt und überwacht werden.

d. Systeme welche via Fernzugriff auf IT-Mittel der ETH Zürich zugreifen, halten die Vorgaben dieser Weisung ein.

[9] Unbefugte dürfen keinen Zutritt zu IT-Mitteln erhalten. Unbefugte sind Personen, welche zur Erfüllung ihrer Aufgabe an der ETH Zürich keine Notwendigkeit zum Betreten der entsprechenden Räumlichkeiten benötigen. Die notwendigen Sicherheitsmassnahmen sind an die räumlichen Gegebenheiten anzupassen. Es gelten die für die jeweilige Organisationseinheit anwendbaren Vorgaben zur physischen Sicherheit.

Artikel 9 Vorgaben für Service-Vermittelnde

Für externe IT-Dienste gelten die folgenden Vorgaben sofern sie im jeweiligen Kontext relevant sind.

[1] Verträge mit solchen Service-Anbietern respektive die AGB der ETH Zürich regeln insbesondere:

a. Aus Gründen der Rechtsdurchsetzbarkeit gilt folgende Präferenz bezüglich Gerichtsstand und anwendbarem Recht: 1. Schweiz, 2. EU, 3. Andere.

b. Personendaten werden in der Schweiz oder der EU bearbeitet verarbeitet und gespeichert). Bei ungenügendem Datenschutzniveau im Speicher-/Verarbeitungsland (siehe Staatenliste des Eidg. Datenschutzbeauftragten) sind Personendaten durch die Vereinbarung von Standard Contractual Clauses (SCC) oder vergleichbare vertragliche Massnahmen zu schützen.

c. Service-Anbieter bestätigen, dass sie die für die ETH Zürich im Kontext der Anwendung relevanten Gesetze und Verordnungen einhalten z.B. die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union[4].

d. Alle Zuständigkeiten sind eindeutig einer Partei zugeordnet.

e. Externe Service-Anbieter verpflichten sich zu regelmässigen unabhängigen Prüfungen der IT-Sicherheit und stellen Audit-Berichte bzw. Zertifizierungsdokumente zur Verfügung oder gewähren der ETH Zürich ein Prüfrecht.

f. Gegenseitige Ansprechpersonen, garantierte Reaktionszeiten sowie die Kommunikationskanäle sind definiert.

g. Die Daten der ETH Zürich müssen von den Daten anderer Kundinnen sowie dem administrativen Bereich der Service-Anbieter (logisch) getrennt sein.

[4] Datenschutz-Grundverordnung (DSGVO) der Europäischen Union: EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu) (abgerufen am 1.7.2022)

h. Im Vertrag muss für den Fall der Kündigung des externen Dienstes die Übernahme der Daten und der Nutzungsprotokolle (Log-Daten) durch die ETH geregelt sein. Zudem wird das unwiederbringliche Löschen dieser Daten auf Seiten der Service-Anbieter vereinbart.

[2] Eine Freigabe zur Bearbeitung von *internen* Daten darf erfolgen, wenn die folgenden Bedingungen erfüllt sind:

a. Benutzende und Administratoren der ETH Zürich und der externen Service-Anbieter arbeiten mit persönlichen Benutzungskonten und authentisieren sich mit mindestens einem Faktor (z.B. Passwort).

b. Daten sind im Transport und in der Ablage verschlüsselt, jeweils mit nach aktuellem Stand der Technik als sicher geltenden Methoden.

c. Aktivitäten von Benutzenden und von Administratoren der ETH Zürich sind nachvollziehbar. Die Log-Daten müssen mindestens ein Jahr verfügbar sein und werden spätestens nach zwei Jahren unwiederbringlich gelöscht.

d. Eine Schnittstelle zur zeitnahen Übernahme von Log-Daten («near realtime») über die Aktivitäten von Benutzenden und Administratoren der ETH Zürich durch die ETH Zürich steht zur Verfügung. Ist dies nicht möglich oder im jeweiligen Kontext nicht sinnvoll, sollen verantwortliche Stellen der ETH Zürich anderweitig auf diese Informationen zugreifen können, z.B. über entsprechende Programmschnittstellen (APIs) oder online-Verwaltungsfunktionen (Dashboards) des Services.

e. Aktivitäten der Service-Anbieter, bei denen auf Daten der ETH Zürich zugegriffen wird, müssen durch die Service-Anbieter aufgezeichnet und für mindestens zwei Jahre aufbewahrt werden.

f. Die Verfügbarkeit der Daten der ETH Zürich muss entsprechend der Anforderungen der ETH Zürich sichergestellt sein. Vorzugsweise wird das durch ein regelmässiges Backup aller Daten gewährleistet, dessen Funktionsweise periodisch überprüft wird.

g. Die Verfügbarkeit der Daten der ETH Zürich muss auch für ausserordentliche Ereignisse (Krankheit, Todesfall etc.) sichergestellt sein. Der/die Service-Vermittelnde oder ein/eine IT-Administrator/in und deren Stellvertretungen sollen im Bedarfsfall auf die Daten zugreifen können.

h. Eine Rückführung der Daten der ETH Zürich auf IT-Services der ETH Zürich muss bei Bedarf möglich sein.

[3] Eine Freigabe zur Bearbeitung v*ertraulicher* Daten darf erfolgen, wenn die Bedingungen zur Bearbeitung interner Daten sowie die folgenden Vorgaben erfüllt sind. Als vertraulich gelten Informationen, deren Kenntnisnahme durch Unberechtigte die Interessen der ETH Zürich erheblich beeinträchtigen kann:

a. Administratoren der externen Service-Anbieter, die auf Daten und Dienste der ETH Zürich zugreifen, setzen sichere Authentisierungsmethoden, wie beispielsweise Multifaktorauthentisierung oder FIDO2 ein.

b. Benutzende und Administratoren der ETH Zürich authentifizieren sich mit Multifaktorauthentisierung.

c. Die Anbieter der Dienstleistung verwenden Schlüssel für die Ablageverschlüsselung exklusiv für die ETH Zürich. Für Daten anderer Kunden werden andere Schlüssel eingesetzt.

d. Die Verwaltung von Benutzungskonten und Zugriffsrechten erfolgt zentral durch die ETH Zürich. Eine Anbindung an die von den Informatikdiensten betriebenen Identitätsverwaltungs- und Föderationsdienste (z.B. ADFS, DirX) muss umgesetzt werden, sofern möglich und sinnvoll.

e. Für Benutzende oder Gruppen von Benutzenden müssen granulare Zugriffsrechte auf einzelne Datenbestände vergeben werden können (z.B. Erzeugen, Lesen, Verändern, Löschen).

[4] Eine Freigabe für die Speicherung oder Bearbeitung *streng vertraulicher* Daten ist nicht gestattet. Als streng vertraulich gelten Informationen, deren Kenntnisnahme durch Unberechtigte die Interessen der ETH Zürich schwerwiegend beeinträchtigen kann.

[5] Aktualität der Software

a. Sofern im jeweiligen Kontext anwendbar, ist punktuell zu kontrollieren, ob der Service-Anbieter Sicherheitsaktualisierungen innerhalb der vereinbarten Fristen einspielt. Verstösse gegen die Vertragsbestandteile sind mit den Service-Anbietern zu thematisieren und im Wiederholungsfall abzumahnen.

b. Liegt die Zuständigkeit für das Einspielen von Sicherheitsaktualisierungen bei der ETH Zürich, ist wie in Art. 8, Abs. 1 und Abs. 2 dieser Weisung zu verfahren.

[6] Ergänzend gilt Art. 10.

Artikel 10 Grundsätze für die Bereitstellung und Nutzung externer Cloud-Dienste

[1] Die Informatikdienste bzw. die IT Services Groups stellen eine Auswahl externer Cloud-Dienste zur Verfügung, die einen Grossteil der Bedürfnisse der ETH-Angehörigen abdeckt. Für die darüber hinausgehende Bereitstellung und Freigabe externer Cloud-Dienste gilt für Service-Vermittelnde:

a. Es ist Service-Vermittelnden nebst den Informatikdiensten (z.B. Professorinnen und Professoren, Departementskoordinierende, Abteilungsleitende sowie weitere IT-Betreibende wie die IT Services Groups in den Departementen) erlaubt, nach Bedarf zusätzliche Cloud-Dienste bereitzustellen und für die ETH-interne Nutzung freizugeben.

b. Für die Freigabe externer Cloud-Dienste ist die vorgängige schriftliche Beurteilung des Erfüllungsgrades der Vorgaben dieser Weisung erforderlich (Self-Assessment).

c. Der/die CISO führt ein zentrales Register externer Cloud-Dienste (Meldepflicht)[5].

d. Für die Bereitstellung und Freigabe externer Cloud-Dienste, die die Vorgaben nicht einhalten können, müssen Service-Vermittelnde befristete Ausnahmebewilligungen bei dem/der CISO einholen.

[5] Register externer Cloud-Dienste: https://ethz.ch/staffnet/de/service/informationssicherheit/nutzung-externer-cloud-dienste/freigabeliste-fuer-externe-cloud-dienste.html

[2] Für die Auslagerung (Speicherung und Bearbeitung) von Informationsbeständen in externen Cloud-Diensten gilt für Informationseignerinnen und -eigner:

a. Die Nutzung externer Cloud-Dienste erfolgt in Eigenverantwortung der Informationseignerinnen und -eigner[6] oder durch Benutzende, die im Auftrag der Informationseignenden handeln.

b. Die Auslagerung (Speicherung und Bearbeitung) vertraulicher Informationsbestände mittels externer Cloud-Dienste ist erlaubt, sofern

   - der Cloud-Dienst die Voraussetzungen zur Speicherung und Bearbeitung öffentlicher, interner oder vertraulicher Daten insbesondere Art. 9 sowie Art. 10 Abs. 1 Bst. b erfüllt und
   - der Informationsbestand sich für die Auslagerung in den vorgesehenen Cloud-Dienst eignet. Zur Beurteilung der Eignung des Informationsbestandes steht ein Self-Assessment zur Verfügung. Die Auslagerung streng vertraulicher Informationen bleibt weiterhin untersagt.

c. Die Informationseignerinnen und -eigner können bezüglich dem auszulagernden Informationsbestand die Zweitmeinung der/des CISOs einholen.

Abschnitt 4: Ausnahmen / Compliance

Artikel 11 Ausnahmen zu den vorgenannten Vorgaben

[1] Für externe IT-Dienste, für welche die Vorgaben dieser Weisung nicht eingehalten werden können, muss eine Ausnahmebewilligung bei dem/der CISO eingeholt werden.

[2] Der/die Direktor/in der Informatikdienste und der/die CISO können verfügen, dass ein externer IT-Dienst nicht verwendet werden darf bzw. dessen Verwendung eingestellt werden muss, wenn dieser andauernd rechtliche, vertragliche oder interne Vorgaben der ETH Zürich verletzt.

[6] Informationseigner sind verantwortlich für die Informationsbestände, die durch sie/ihn oder in ihrem/seinem Auftrag erhoben und bearbeitet werden. Quelle: Weisung «Informationssicherheit an der ETH Zürich», RSETHZ 203.25

[3] Für IT-Mittel im Netzwerk der ETH Zürich, für welche die im jeweiligen Kontext anzuwendenden Vorgaben dieser Weisung nicht eingehalten werden können, gilt:

a. Nicht-konforme IT-Mittel sind in abgeschotteten Zonen des Netzwerks der ETH Zürich zu platzieren. Allfällige Schwachstellen dürfen von ausserhalb der isolierten Zonen nicht ausnutzbar sein.

b. Für IT-Mittel, die nicht in einer isolierten Zone betrieben werden müssen, obwohl die Vorgaben länger als 10 Arbeitstage nicht eingehalten werden, muss eine Ausnahmebewilligung eingeholt werden.

[4] Die Informatikdienste führen den Ausnahmeprozess im Auftrag der/des CISO durch.

[5] Ausnahmebewilligungen sind befristet. Bei Ablauf überprüft der/die Antragsteller/in ggf. ein neues Gesuch.

Abschnitt 5: Schlussbestimmungen

Artikel 12 Verantwortung für die Weisung

Diese Weisung wird jährlich überprüft und vom Vizepräsident für Infrastruktur und Nachhaltigkeit der ETH Zürich und vom Chief Information Security Officer der ETH Zürich in Kraft gesetzt.

Artikel 13 Aufhebung bisherigen Rechts

Die folgenden Erlasse werden aufgehoben:

1. Vorherige Versionen der IT-Richtlinien und IT-Grundschutzvorgaben (RSETHZ 203.23)

Artikel 14 Übergangsbestimmung

Keine

Artikel 15 Inkrafttreten

Diese Weisung tritt am 01. Januar 2025 in Kraft.

Zürich, 01. Januar 2025

Prof. Dr. Ulrich A. Weidmann
Vizepräsident für Infrastruktur und Nachhaltigkeit
ETH Zürich

Johannes Hadodo
Chief Information Security Officer
ETH Zürich