Reglement zur Nutzung der ZHAW IT-Infrastruktur

Der Verwaltungsdirektor beschliesst, gestützt auf:

- Fachhochschulgesetz des Kantons Zürich
- Gesetz über die Information und den Datenschutz des Kantons Zürich
- Policy Informationssicherheit

1. Allgemeines

1.1 Gegenstand

Dieses Reglement hat das Ziel, die ordnungsgemässe Nutzung der Informatikmittel an der ZHAW sicherzustellen und einen sicheren sowie störungsfreien Betrieb zu gewährleisten.

1.2 Geltungsbereich

Diesem Reglement sind als Benutzende unterstellt: Hochschulangehörige der ZHAW und alle weiteren Personen, die Zugang zu den Informatikmitteln der ZHAW haben.

Das Reglement betrifft

a. alle Informatikmittel, die von der ZHAW zur Verfügung gestellt werden und
b. alle Informatikmittel, welche an das Datennetz der ZHAW angeschlossen werden.

1.3 Begriffe

Authentisierungsmittel

Authentisierungsmittel sind eine grundlegende Komponente der Sicherheitsinfrastruktur und dienen dazu, die Identität von Benutzenden und Entitäten (z.B. Computersystemen) zu überprüfen. Typische Authentisierungsmittel umfassen Passwörter, Zertifikate und Tokens.

Cloud-Dienste

Cloud-Dienste sind Dienstleistungen, die über das Internet bereitgestellt werden. Diese Dienste ermöglichen es Benutzenden, geschäftliche Daten online zu speichern und zu bearbeiten.

Informatikmittel

Informatikmittel umfassen datenverarbeitende Systeme (u.a. Computer, Tablets, Server, Drucker, Kameras, Sensoren), Netzwerkkomponenten, Applikationen und Cloud-Dienste, die zur Bearbeitung, Speicherung und Übertragung von Daten sowie zur Ausführung von Applikationen verwendet werden.

Protokolldaten

Protokolldaten enthalten Informationen über die Nutzung und den Betrieb von Informatikmitteln. Sie werden generiert, um Fehler in Informatikmitteln zu diagnostizieren und Vorgänge rekonstruieren zu können. Zudem dienen sie dazu, sicherheitsrelevante Anomalien zu erkennen und regulatorische Anforderungen zu erfüllen.

Schadsoftware

Schadsoftware ist eine Software, die entwickelt wurde, um unerwünschte oder schädliche Aktivitäten auf Informatikmitteln auszuführen.

Software Agents

Software Agents ist Software, die autonom oder halbautonom handelt und spezifische Aufgaben auf Informatikmitteln ausführen kann.

Spam

Spam bezeichnet unerwünschte E-Mails, die in grossen Mengen verteilt werden und oft Werbung, betrügerische Angebote, unerwünschte Inhalte oder Links zu schädlichen Websites enthalten.

2. Inhalt

2.1 Zulässige Nutzung

Die Nutzung der Informatikmittel der ZHAW ist für diejenigen Zwecke erlaubt, für welche die Informatikmittel zur Verfügung gestellt werden (bestimmungsgemässe Nutzung).

Eine Nutzung für private nichtkommerzielle Zwecke ist erlaubt, soweit sie zurückhaltend stattfindet, auf ein Minimum beschränkt wird und

a. weder gegen dieses Reglement verstösst noch in anderer Weise rechtswidrig ist;
b. für die ZHAW nicht rufschädigend ist;
c. die Erfüllung der Arbeits- oder Studienpflichten nicht beeinträchtigt;
d. keine technischen Störungen verursacht;
e. ausschliesslich durch ZHAW geprüfte und freigegebene Software nutzt;
f. private Daten klar von geschäftlichen Daten getrennt sind;
g. die Nutzungs- und Lizenzbedingungen der genutzten Dienste und Applikationen nicht verletzt und
h. allgemein benutzte Informatikmittel der ZHAW nicht unverhältnismässig bzw. übermässig beansprucht (Netzwerk, Bandbreite, Internet-Zugang, Speicher etc.).

Eine kommerzielle Nutzung der Informatikmittel der ZHAW ist nur mit schriftlicher Einwilligung des Verwaltungsdirektors bzw. der Verwaltungsdirektorin zulässig.

2.2 Zugriffsberechtigungen

Es sind nur Zugriffe auf Informatikmittel der ZHAW im Rahmen der erhaltenen Zugriffsberechtigungen mit den vorgesehenen Authentisierungsmitteln erlaubt. Zugangsdaten sind stets persönlich und realen Personen zugeordnet. Die Benutzenden sind für ihre Zugriffe auf Informatikmittel der ZHAW verantwortlich. Ermöglichen die Benutzenden durch Verletzung ihrer Pflichten gemäss diesem Reglement unberechtigten Dritten Zugriffe auf Informatikmittel der ZHAW, so sind die Benutzenden hierfür ebenfalls verantwortlich.

Authentisierungsmittel dürfen grundsätzlich nicht weitergegeben werden, ausser es dient der Initialisierung oder technischen Verwaltung der Authentisierungsmittel.

2.3 Missbräuchliche Nutzung

Missbräuchlich ist jede Nutzung der Informatikmittel der ZHAW, die gegen dieses Reglement verstösst oder in anderer Weise rechtswidrig ist. Untersagt ist insbesondere:

a. das Verletzen strafrechtlicher Bestimmungen;
b. das aktive Abrufen, Speichern und/oder Versenden von rechtswidrigen Applikationen, Inhalten, Pornografie, gewaltverherrlichenden Darstellungen, rassistischen Inhalten;
c. das Verbreiten von beleidigenden, herabwürdigenden, diskriminierenden oder sexistischen Inhalten und das Verletzen von Persönlichkeitsrechten Dritter;
d. das Verletzen von Urheberrechten, wie das rechtswidrige Abrufen und die rechtswidrige Verteilung von urheberrechtlich geschützten Daten (z.B. mittels Peer-to-Peer);
e. die Verletzung von Lizenzbestimmungen;
f. die Verteilung von unerwünschten Massenmails (Spam) sowie der Missbrauch der E-Mail-verteiler-Listen;
g. die nicht bewilligte Durchführung von Hacking-Aktivitäten (z.B. Port- und Schwachstellenscans, Ausspionieren von Authentisierungsmitteln und Daten, Denial of Service Angriffe, Verbreitung von Schadsoftware);
h. die Belästigung Dritter durch Nutzung von Informatikmitteln;
i. der Zugriff auf Informatikmittel von Drittpersonen ohne deren Zustimmung;
j. das unbefugte Zugreifen, Lesen, Verändern, Löschen, Unbrauchbarmachen oder Unterdrücken von Daten;
k. das unbefugte Verändern von System- und Netzwerkkonfiguration und
l. das unautorisierte Bereitstellen von Netzwerkzugängen für Dritte (z.B. Access Points).

In Zweifelsfällen entscheiden der Leiter bzw. die Leiterin ICT oder der bzw. die Chief Information Security Officer, ob eine missbräuchliche Nutzung vorliegt.

Keine missbräuchliche Nutzung liegt vor, wenn die Handlungen im Rahmen vom Leistungsauftrag der ZHAW erfolgen und zuvor durch den Leiter bzw. die Leiterin ICT oder den bzw. die Chief Information Security Officer bewilligt wurden.

2.4 Ausserordentliche Nutzung

Für die Nutzung von Informatikmitteln, die den allgemein üblichen Umfang übersteigen oder den Betrieb gefährden könnten (z.B. Netzwerkbelastung, Sicherheit), ist die Zustimmung des Leiters bzw. der Leiterin ICT oder des bzw. der Chief Information Security Officer einzuholen.

2.5 Datenschutz

Die datenschutzrechtlichen Vorgaben sind bei der Nutzung der Informatikmittel und beim Einsatz von Kontroll- und Überwachungsmassnahmen stets einzuhalten. Insbesondere dürfen Personendaten nur bearbeitet werden, soweit dies zur Erfüllung des gesetzlichen Leistungsauftrags der ZHAW geeignet und erforderlich ist.

Die Benutzenden sind für die datenschutzkonforme Nutzung der Informatikmittel verantwortlich.

Bei Angelegenheiten sowie Fragestellungen zum Datenschutz im Geltungsbereich dieses Reglements ist der oder die Datenschutzbeauftragte der ZHAW einzubeziehen.

2.6 Pflichten der Benutzenden

Die Benutzenden sind dafür verantwortlich, dass die Nutzung der Informatikmittel nicht gegen dieses Reglement verstösst oder in anderer Weise rechtswidrig ist. Die Pflichten der Benutzenden beinhalten zudem folgende Punkte:

a. Informatikmittel müssen sorgfältig, verantwortungsvoll, sicher und ökonomisch eingesetzt werden.
b. Zur Bearbeitung und Speicherung geschäftlicher Daten und zur geschäftlichen Kommunikation sind ausschliesslich durch die ZHAW bereitgestellte oder ausdrücklich genehmigte Informatikmittel erlaubt.
c. Informatikmittel der ZHAW sind stets vor Diebstahl, Verlust und Manipulation zu schützen. Sie müssen sicher aufbewahrt und transportiert werden.
d. Die Benutzenden sind für den fachlich und rechtlich korrekten Einsatz und Umgang mit den ihnen zur Verfügung stehenden Informatikmitteln und den von ihnen geschäftlich oder im Rahmen des Studiums eingesetzten privaten Informatikmitteln verantwortlich. Sie haben alles zu vermeiden, was den Geschäftsbetrieb der ZHAW beeinträchtigen, Schäden an Informatikmitteln der ZHAW oder bei anderen Benutzenden verursachen könnte.
e. Die Benutzenden sind verpflichtet, das ihnen Zumutbare zu unternehmen, um zu verhindern, dass Schadsoftware Informatikmittel und Informationen der ZHAW kompromittiert.
f. Benutzende sind verpflichtet, zur Verfügung gestellte Anleitungen und Handlungsempfehlungen zu beachten und an obligatorischen Schulungen zur sicheren und ordnungsgemässen Nutzung der Informatikmittel teilzunehmen.
g. Bei Beendigung des Arbeitsverhältnisses verbleiben die ZHAW-eigenen Informatikmittel bei der ZHAW. Alle nicht-geschäftlichen Daten auf den Informatikmitteln der ZHAW sind zum Austritt aus der ZHAW durch die Benutzenden zu löschen.
h. Die Kenntnis schwerer oder wiederholter missbräuchlicher Nutzung, die Kenntnis von schwerwiegenden Sicherheitslücken, die Kenntnis von Verlust oder Diebstahl von Informatikmitteln der ZHAW und die Kenntnis von Verlust oder Diebstahl von privaten Informatikmitteln mit betrieblichen Daten verpflichtet die Benutzenden zur unverzüglichen Meldung an den Leiter bzw. die Leiterin ICT oder den bzw. die Chief Information Security Officer.
i. Anordnungen des Leiters bzw. der Leiterin ICT und des bzw. der Chief Information Security Officer sind für alle Benutzenden verbindlich.
j. Für vorsätzlich oder grobfährlässig verschuldete Schäden an Informatikmitteln der ZHAW haftet der Verursacher bzw. die Verursacherin.

2.7 Kontroll- und Überwachungsmassnahmen

Kontroll- und Überwachungsmassnahmen sind Verfahren und Technologien zur Diagnose und Rekonstruktion von Fehlern sowie betrieblichen und sicherheitsrelevanten Vorgängen in Informatikmitteln. Diese Massnahmen werden kontinuierlich durchgeführt und ermöglichen durch eine weitestgehend automatisierte Erkennung die schnelle automatisierte und auch manuelle Reaktion.

Für Kontroll- und Überwachungsmassnahmen durch die ZHAW gelten die folgenden Grundsätze:

a. Kontroll- und Überwachungsmassnahmen dienen ausschliesslich der Einhaltung geltenden Rechts, der Sicherstellung des Geschäftsbetriebs der ZHAW, der Optimierung und der Gewährleistung der Sicherheit der Informatikmittel. Sie erfolgen im Rahmen der rechtlichen Vorgaben.

b. Die Benutzung der Informatikmittel kann personenbezogen protokolliert werden. ZHAW ICT trifft angemessene Massnahmen, um den Schutz personenbezogener Protokolldaten zu gewährleisten. Dies betrifft insbesondere den Schutz vor unberechtigten Zugriffen und vor unberechtigten Manipulationen und die Einhaltung von Löschfristen und anderen rechtlichen Vorgaben.
c. Die systematische Auswertung von personenbezogenen Protokolldaten zur Verhaltenskontrolle oder zur Profilerstellung ist untersagt.
d. Personenbezogene Protokolldaten dürfen höchstens 6 Monate, bei laufenden Verfahren bis zum Abschluss des Verfahrens, aufbewahrt werden.
e. Personenbezogene Auswertungen von Protokolldaten sind unter Beachtung des Datenschutzrechts, insbesondere der Verhältnismässigkeit, zulässig, wenn ein konkreter Verdacht auf einen Verstoss gegen dieses Reglement vorliegt, die Sicherheit oder der Geschäftsbetrieb der ZHAW konkret gefährdet sind.
f. Personenbezogene Auswertungen können ausschliesslich durch den bzw. die Chief Information Security Officer beantragt und durch den Verwaltungsdirektor bzw. die Verwaltungsdirektorin in Absprache mit dem Rechtsdienst der ZHAW angeordnet werden. ZHAW ICT ist für die Umsetzung dieser Massnahmen verantwortlich.
g. Der bzw. die Chief Information Security Officer informiert den Verwaltungsdirektor über durchgeführte personenbezogene Auswertungen.
h. Technische Massnahmen wie Filtersperren und die Entschlüsselung verschlüsselter Daten sind zulässig, sofern dies für die Einhaltung geltenden Rechts, die Gewährleistung der Sicherheit, zur Gefahrenabwehr oder zur Sicherstellung des Geschäftsbetriebs der ZHAW unumgänglich ist.
i. ZHAW ICT ist jederzeit Zugriff auf die Informatikmittel der ZHAW zu gewähren, z.B. manuell, durch Fernwartung oder mittels vorinstallierter Software Agents. Dem bzw. der Chief Information Security Officer muss zudem ermöglicht werden, die Sicherheit der ZHAW-eigenen Informatikmittel zu überprüfen und zu gewährleisten.
j. ZHAW ICT kann zur Einhaltung geltenden Rechts, zur Gewährleistung der Sicherheit und zur Sicherstellung des Geschäftsbetriebs der ZHAW einzelne oder eine Kombination mehrerer Massnahmen ergreifen. Diese sind insbesondere
    - Sperren von Zugriffen;
    - Isolierung/Quarantäne von Informatikmitteln;
    - Sperren oder Abschaltung von Informatikmitteln und
    - Löschen von Daten.

2.8 Sanktionen

Die Feststellung und allenfalls Sanktionierung von Verstössen gegen dieses Reglement obliegt dem bzw. der Chief Information Security Officer sowie dem Leiter bzw. der Leiterin ICT. Sanktionen können aus einzelnen oder einer Kombination mehrerer Massnahmen bestehen:

a. Schriftliche Ermahnung;
b. Information an die vorgesetzte Person.

Überdies können personalrechtliche Massnahmen ergriffen werden. Die Strafverfolgung und die Geltendmachung von Schadenersatzansprüchen bleiben vorbehalten.

3. Schlussbestimmungen

Der Leiter bzw. die Leiterin ICT oder der bzw. die Chief Information Security Officer können im Auftrag der Hochschulleitung Richtlinien zur Durchführung und Konkretisierung dieses Reglements erlassen und verändern. Die Genehmigung dieser Richtlinien erfolgt durch den Verwaltungsdirektor bzw. die Verwaltungsdirektorin.

Dieses Reglement tritt per 1.9.2024 in Kraft.

4. Erlassinformationen

4.1 Metadaten Erlass

Betreff	**Inhalt**
Erlassverantwortliche/r	Chief Information Security Officer und Leiter/in ICT
Beschlussinstanz	Verwaltungsdirektor/in
Themenzuordnung	6.05.02 ICT Servicebetrieb
Publikationsart	Public

4.2 Erlassverlauf

Version	**Beschluss**	**Beschlussinstanz**	**Inkrafttreten**	**Beschreibung Änderung**
1.0.0	15.08.2009	HSL	01.09.2009	Originalversion ersetzt AUP vom 01.03.2007
1.0.1	-	-	-	formale, redaktionelle Korrekturen, Umstellung auf GPM Ablage 31.08.2013
1.0.2	-	-	-	formale Anpassung des Anhangs, Tabelle auf 1 Seite reduziert. 15.01.2015
1.0.3	-	-	-	Layout überarbeitet für GPM. 26.04.2017
1.0.4	-	-	-	Einfügung des Links zum Anhang 2, 12.09.2017
2.0.0	12.06.2024	Verwaltungsdirektor	01.09.2024	Vollständige Überarbeitung des Reglements