Reglement zur Nutzung der ZHAW IT-Infrastruktur

Die Hochschulleitung beschliesst, gestützt auf:

- Fachhochschulgesetz des Kantons Zürich
- Policy Informatiksicherheit ZHAW

Sämtliche Gesetze, Verordnungen und Reglemente beziehen sich auf die jeweils gültige Fassung.

1 Allgemeines

1.1 Präambel

Die ZHAW stellt mit ihren Informatikmitteln eine moderne und funktionierende Infrastruktur zur Verfügung. Den BenutzerInnen soll dadurch unter Beachtung aktueller Sicherheitsstandards sowie der gesetzlichen Bestimmungen ermöglicht werden, ihre Aufgaben effizient zu erfüllen. Im Rahmen ihres Leistungsauftrags unterstützt die ZHAW die BenutzerInnen bei ihrem verantwortungsbewussten Umgang mit den Informatikmitteln.

1.2 Zweck

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

1.3 Geltungsbereich

Diesem Reglement sind als BenutzerInnen unterstellt: Personal, Studierende, KursteilnehmerInnen, Dozierende und alle weiteren Personen, die Zugang zu den Informatikmitteln der ZHAW haben. Das Reglement betrifft alle Informatikmittel, die von der ZHAW zur Verfügung gestellt werden.

Die IT-Sicherheitskommission bzw. der IT-Sicherheitsbeauftragte können im Auftrag der Hochschulleitung für die Benutzung von Informatikmitteln fachtechnische Richtlinien zur Durchführung und Konkretisierung dieses Reglements erlassen und verändern.

2 Inhalt

2.1 Zulässige Nutzung

Die Nutzung der Informatikmittel 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 nicht übermässig ist und die Erfüllung der Arbeits- oder Studienpflichten nicht beeinträchtigt.

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

2.2 Sicherheitsvorschriften

Es ist ausschliesslich mit den Benutzerkennungen zu arbeiten, deren Nutzung gestattet wurde. Die Weitergabe von Benutzernamen und Passwörtern ist untersagt. Unsichere Passwörter sind zu vermeiden, jede Sitzung muss ordnungsgemäss mit dem Logout beendet werden.
Die BenutzerInnen tragen die Verantwortung für alle Aktionen, die sie mit ihrer Benutzerkennung vornehmen oder die durch Dritte vorgenommen werden, wenn sie diesen den Zugang zumindest fahrlässig ermöglicht haben.

2.3 Missbräuchliche Nutzung

Das Herunterladen, die Verwahrung und die Verbreitung oder Verwertung von rechtswidrigen oder rechtswidrig erlangten Daten, Programmen oder Anleitungen sind untersagt.

Die Informatikmittel der ZHAW dürfen nicht verwendet werden für Angriffe auf andere Systeme, zur Verteilung von unerwünschten Massenmails (Spam) sowie für jede weitere nicht zweckgemässe Tätigkeit wie z.B. Missbrauch der Mailverteiler-Listen.

Untersagt sind insbesondere:

- Ausspionieren fremder Passwörter und Daten;
- unbefugtes Verändern, Löschen, Unbrauchbarmachen oder Unterdrücken von Daten;
- unbefugtes Verändern von System- und Netzwerkkonfiguration;
- bereitstellen von Netzwerkzugängen für Dritte (z.B. Access Points).

2.4 Ausserordentliche Nutzung

Werden Einsätze von Informatikmitteln geplant, die den allgemein üblichen Umfang übersteigen oder den Betrieb gefährden könnten (z.B. Netzwerkbelastung, Sicherheit), so ist dafür die Zustimmung des IT-Sicherheitsbeauftragten einzuholen.

BenutzerInnen, die durch ihre ordnungsgemässe Tätigkeit die Möglichkeit zur Einsicht in personelle und andere vertrauliche Geschäftsdaten haben, unterstehen besonderen Verpflichtungen wie den allgemeinen Datenschutzbestimmungen sowie den personalrechtlichen Erlassen. Sie haben zum Schutz dieser Daten die nötigen Vorkehrungen zu treffen.

2.5 Datenschutz

Jeglicher Einsatz von Informatikmitteln, der die Privatsphäre oder die Persönlichkeit von Personen verletzen könnte, ist untersagt.
Personendaten dürfen nur soweit erfasst, verarbeitet und weitergegeben werden, als dies zur Ausführung der anvertrauten Aufgabe innerhalb der ZHAW notwendig ist. Die einschlägigen Gesetze und Verordnungen zum Datenschutz und zur Archivierung sind einzuhalten. Die BenutzerInnen von Informatikmitteln sind dafür verantwortlich, dass Daten nicht durch unbefugte Dritte missbräuchlich verwendet werden können.

3 Verpflichtungen der BenutzerInnen

Informatikmittel müssen sorgfältig, verantwortungsvoll, sicher und ökonomisch eingesetzt werden.

BenutzerInnen sind für den fachlich und rechtlich korrekten Einsatz und Umgang mit den ihnen zur Verfügung stehenden Informatikmittel verantwortlich. Sie haben alles zu vermeiden, was den Betrieb beeinträchtigen, Schäden am System oder bei anderen BenutzerInnen verursachen könnte.

Die BenutzerInnen sind verpflichtet, das ihnen Zumutbare zu unternehmen, um zu verhindern, dass Malware (Viren etc.) auf die Informatikmittel der ZHAW übertragen wird. Sie haben dazu den Empfehlungen der IT-Sicherheitskommission und des IT-Sicherheitsbeauftragten zu folgen.

Zum rechtlich korrekten Einsatz gehören insbesondere die Beachtung von Urheber- und Lizenzrechten, Bestimmungen zum Schutz der Persönlichkeit sowie der strafrechtlichen Bestimmungen über Pornographie und Rassendiskriminierung.

BenutzerInnen sind ausserdem verpflichtet, die zur Verfügung gestellten Anleitungen und Leitfäden zur Benutzung zu beachten.

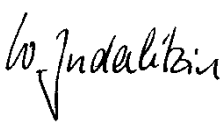
4 Sanktionen bei Missbrauch

Die Sanktionen bei Missbrauch sind im Anhang geregelt.

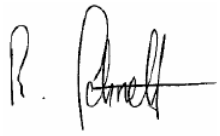
5 Schlussbestimmungen

Dieses Reglement tritt per 1.9.2009 in Kraft und gilt bis zum Widerruf durch die herausgebende oder deren vorgesetzte Stelle.

Zürcher Hochschule für Angewandte Wissenschaften



Prof. Dr. Werner Inderbitzin
Gründungsrektor



Reto Schnellmann
Verwaltungsdirektor

Erlassverantwortliche/-r	LeiterIn ICT	Ablageort	1.04.01 Führungsgrundlagen
Beschlussinstanz	HSL	Publikationsort	Public
Genehmigungsinstanz			

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

Anhang 1 zum Reglement zur Nutzung der ZHAW IT-Infrastruktur
Kategorien und Sanktionen in Bezug auf Missbrauch der IT Mittel der ZHAW

Die aufgeführten Sanktionen betreffen alle Angehörigen der ZHAW gemäss 1.3 des Reglements.

Kategorie	Sanktion	Bemerkungen
Unwissentlicher Missbrauch ohne Kostenfolgen für die ZHAW	Hinweis eines Mitglieds der IT SiKo	Der Missbrauch wird nicht bewusst durchgeführt, z.B. erstmaliges Versenden von Spam im Sinne von Wohnungsvermietung oder Autoverkauf
Unwissentlicher Missbrauch mit Kostenfolgen für die ZHAW	Hinweis eines Mitglieds der IT SiKo	
Bewusster Missbrauch ohne Kostenfolgen für die ZHAW	1. Sperrung des ZHAW Accounts mindestens bis zum 2. Gespräch mit dem/der jeweiligen DirektorIn oder dem/der Vorgesetzten (Angestellte) oder dem/der StudiengangleiterIn (Studierende) und 3. Erteilen einer schriftlichen Ermahnung.	Gilt z.B., wenn der Missbrauch als Scherz gemeint war oder bei wiederholter Versendung von Spam-Mails.
Bewusster Missbrauch mit Kostenfolgen für die ZHAW	1. Sperrung des ZHAW Accounts mindestens bis zum 2. Gespräch mit dem/der jeweiligen DirektorIn oder dem/der Vorgesetzten (Angestellte) oder dem/der StudiengangleiterIn (Studierende) und 3. Erteilen einer schriftlichen Ermahnung. 4. Evtl. Übernahme der nachweisbaren Kosten	Gilt z.B., wenn der Missbrauch als Scherz gemeint war oder bei wiederholter Versendung von Spam-Mails. Es wird angestrebt, dass der/die verursachende Mitarbeitende/Studierende die nachweisbaren Kosten für den Missbrauch übernimmt. Dies wird im Einzelfall geprüft.
Bewusster Missbrauch mit Verschleierung ohne Kostenfolgen für die ZHAW	1. Sperrung des ZHAW Accounts mindestens bis zum 2. Gespräch mit dem/der jeweiligen DirektorIn oder dem/der Vorgesetzten (Angestellte) oder dem/der StudiengangleiterIn (Studierende) und 3. Erteilen einer schriftlichen Ermahnung. 4. Evtl. Einleitung eines Disziplinarverfahrens (gemäss FHV oder PG). Bei Personal: Prüfung weiterer personalrechtlicher Sanktionen (bis hin zur Kündigung)	Gilt, wenn der Missbrauch bewusst verschleiert wurde, z.B. durch Missbrauch fremder ZHAW-Accounts oder durch Fälschen der E-Mail Absender Adresse.
Bewusster Missbrauch mit Verschleierung und mit Kostenfolgen für die ZHAW	1. Sperrung des ZHAW Accounts mindestens bis zum 2. Gespräch mit dem/der jeweiligen DirektorIn oder dem/der Vorgesetzten (Angestellte) oder dem/der StudiengangleiterIn (Studierende) und 3. Erteilen einer schriftlichen Ermahnung. 4. Evtl. Übernahme der nachweisbaren Kosten 5. Evtl. Einleitung eines Disziplinarverfahrens (gemäss FHV oder PG). Bei Personal: Prüfung weiterer personalrechtlicher Sanktionen (bis hin zur Kündigung) 6. Je nach Schweregrad des Missbrauchs wird der/die fehlbare Mitarbeitende/Studierende verzeigt. Der Entscheid liegt beim Rektor.	Gilt, wenn der Missbrauch bewusst verschleiert wurde, z.B. durch Missbrauch fremder ZHAW-Accounts oder durch fälschen der E-Mail Absender Adresse. Es wird angestrebt, dass der/ die verursachende Mitarbeitende/Studierende die nachweisbaren Kosten für den Missbrauch übernimmt. Dies wird im Einzelfall geprüft.

Anhang 2 zum Reglement zur Nutzung der ZHAW IT-Infrastruktur
Nutzung Cloud-Dienste an der ZHAW

Link