Nutzungsbedingungen
IT-Ressourcen ZHdK

Die ZHdK stellt ihren Angehörigen eine aktuelle Informatik Infrastruktur zur Verfügung. Diese soll unter Beachtung der Sicherheitsstandards sowie der gesetzlichen Bestimmungen effizient genutzt werden können.

1. Allgemeine Bestimmungen

1.1 Zweck

Dieses Reglement beschreibt die Nutzung der Informations- und Kommunikationstechnologie (IT Ressourcen), im Speziellen die Verwendung von E-Mail und Internet sowie mobile Geräte. Es legt den verantwortungsvollen Umgang mit Informationen (insbesondere Personendaten) fest. Es stellt die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen sicher.

1.2 Geltungsbereich

Das Reglement gilt für alle Angehörigen der ZHdK sowie für Externe, soweit diese auf IT Ressourcen der ZHdK zugreifen. Das Reglement betrifft die gesamten IT Ressourcen der ZHdK.

1.3 Grundlagen

Dieses Reglement stützt sich auf die kantonalen und schweizerischen Rechtsgrundlagen sowie die Nutzungsbedingungen der SWITCH und das Sicherheitskonzept der ZHdK.

1.4 Begriffe

In diesem Reglement gelten die nachfolgenden Definitionen:
- **IT-Ressourcen** beinhalten IT-Mittel, Informationen und IT-Dienste.
- **IT-Mittel** definiert als Geräte, Einrichtungen und Programme materieller und immaterieller Art, die der elektronischen Verarbeitung, Speicherung, Übermittlung oder Vernichtung von Informationen dienen, namentlich:
    - Computersysteme und Smart Devices,
    - Peripherie-Geräte (wie Speichermedien, Eingabegeräte usw.), Netzwerke (wired und wireless) und Netzwerk-Geräte (wie Router, Repeater, Security-Devices, Wireless Access Points),
    - Software inkl. Zugriffsdaten,
    - Telefon-Infrastruktur
- Als **Informationen** gelten Personen- und Sachdaten.
- **IT-Dienste** beinhalten zentrale Dienste wie E-Mail, DNS, Web-Services, Netzwerkzugang (auch Fernzugriff), Digital Libraries usw., welche den berechtigten Benutzern zur Verfügung gestellt werden.
- Als **digitaler Inhalt** gelten Daten und Informationen, welche auf digitalen Medien gespeichert sind (auch als digital gespeicherte Daten bezeichnet).
- Als **Arbeitsplätze** gelten auch Studien- und Ateliersplätze.
- **Externe Dienste**: Die Verwendung digitalen Inhalten auf von externen digitalen Diensten (wie Cloud-Dienste, Soziale Netze [«Social Medias»]).

2. Aufgaben, Pflichten und Zuständigkeiten

2.1 IT Sicherheitsbeauftragter (IT-SiBe)

Der IT Sicherheitsbeauftrage der ZHdK (nachfolgend IT-SiBe) ist für die Umsetzung dieses Reglements verantwortlich und ist Ansprechstelle für Fragen und für sicherheitsrelevante IT-

Vorkommnisse. Er ist befugt, den Angehörigen der ZHdK Weisungen bezüglich IT-Informationssicherheit zu erteilen.

2.2 Informationstechnologie Zentrum (ITZ)

Das Informationstechnologie-Zentrum (ITZ) ist ein zentraler Serviceanbieter der ZHdK und als solcher zuständig für die gesamte IT-Infrastruktur. Angehörige der ZHdK werden bei der Verwendung von IT-Ressourcen unterstützt und entsprechend geschult.

2.3 Angehörige der ZHdK

- Die Angehörigen der ZHdK sind verpflichtet, die gesetzlichen Vorgaben, dieses Reglement und andere interne Regelungen zu beachten.
- Die Angehörigen der ZHdK sind verpflichtet, die ihnen zur Verfügung gestellten IT-Ressourcen recht- und zweckmässig einzusetzen und mit den Informationen, insbesondere mit Personendaten und besonderen personenbezogen Daten, sorgfältig umzugehen.
- Die Angehörigen der ZHdK melden alle sicherheitsrelevanten Ereignisse (Probleme, Vorfälle, Mängel usw.) sowie Schäden und/ oder den Verlust von IT-Ressourcen dem IT-SiBe oder dem ITZ.
- Die Angehörigen der ZHdK informieren sich auf der Webseite des ITZ über die empfohlenen Arbeitsweisen und die zur Verfügung gestellten IT-Ressourcen und halten sich an die entsprechenden Anleitungen.

3. Datenschutz und Informationssicherheit

3.1 Zugangs- und Zugriffsschutz

- Die Angehörigen der ZHdK haben dafür zu sorgen, dass Unbefugte keinen Zutritt zu den Arbeitsräumlichkeiten haben. Halten sich externe Personen (z.B. Servicetechniker usw.) in den Büroräumlichkeiten auf, ist dafür zu sorgen, dass diese keinen unbefugten Zugriff auf Informationen erhalten.
- Der Arbeitsplatz ist bei Abwesenheiten so zu hinterlassen, dass keine vertraulichen oder schutzbedürftigen Informationen und IT-Ressourcen zugänglich sind (Abschliessen der Büros, Sperren oder Herunterfahren des Computers, Wegschliessen von mobilen Geräten).
- Arbeiten die Angehörigen der ZHdK ausserhalb der üblichen Arbeitsräumlichkeiten, zum Beispiel in Heim-Arbeit, auf Reisen etc., so sorgen sie dafür, dass Dritte keinen Zugriff auf Informationen der ZHdK erhalten und der Verkehr ausschliesslich über anerkannte gesicherte Verschlüsselungen erfolgt.
- Das ITZ stellt nur für die Daten, welche auf der zentralen Datenablage gespeichert sind ein sicheres Backupsystem zur Verfügung.
- Ausdrucke mit vertraulichen Informationen jeder Art sind umgehend aus dem Drucker zu entfernen.
- Die Angehörigen der ZHdK dürfen nur ihre persönlichen Benutzerkonten oder die ihnen zugeteilten funktionellen Konten verwenden und diese nicht an andere Personen weitergeben. Für die erfolgten Zugriffe sind die jeweiligen Benutzerkonten-Inhaber verantwortlich.
- Der Zugriff auf Personendaten ist nur berechtigten Benutzerkonten gestattet.
- Der Verlust von IT-Mitteln und Informationen ist umgehend dem IT-SiBe oder dem ITZ zu melden. Besteht der Verdacht, dass Zugangs- oder Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden, ist das ITZ umgehend zu informieren.
- Austretende Angehörige der ZHdK haben unterschriftlich zu bestätigen, dass alle schützenswerten Informationen (insbesondere besondere Personendaten), die ihnen zugänglich waren und die ausserhalb der ZHdK bearbeitet oder gespeichert wurden, unwiderruflich gelöscht oder zurückgegeben wurden. Ein einfaches Löschen und Papierkorb entleeren, ist nicht ausreichend. Das ITZ ist befugt Stichproben durchzuführen.

3.2 Passwörter

- Alle Passwörter sind vertraulich zu behandeln. Sie dürfen nicht unverschlüsselt auf Systemen gespeichert oder anderen Personen (z. B. Vorgesetzten, Informatikverantwortlichen, IT-SiBe usw.) bekannt gegeben werden. Falls Passwörter aufgeschrieben werden, ist dieses Passwort-Dokument geschützt vor unbefugtem Zugriff aufzubewahren (z.B. abschliessbaren Schrank, Schublade usw.).
- Es müssen sichere Passwörter gewählt werden, das ITZ stellt Anleitungen zur Verfügung und hilft bei der Wahl von sicheren Passwörtern.
- Gruppenpasswörter werden nur vergeben, wenn dies zwingend erforderlich ist. Sie sind umgehend zu ändern, wenn sich die Zusammensetzung der Gruppe verändert. Gleiches gilt, wenn sie unautorisierten Personen bekannt geworden sind.
- Initialpasswörter müssen unverzüglich (d. h. nach dem ersten Einloggen) geändert werden.

3.3 Datensicherung, Datenlöschung und die Entsorgung von Informationsträgern

- Personendaten und vertrauliche Daten dürfen nur auf den vom ITZ zur Verfügung gestellten zentralen Datenablagen gespeichert werden und müssen jederzeit gegen unberechtigten Zugriff geschützt sein.
- Nicht mehr benötigte Daten müssen von Datenträgern (z.B. USB-Datenträger, Speicherkarten, interne und externe Festplatten etc.) unwiederbringlich gelöscht werden (einfaches Löschen genügt nicht).
- Nicht mehr benötigte Informationsträger (z.B. CD-ROM, USB-Datenträger usw.), die vertrauliche Informationen enthalten oder einmal enthielten, müssen physisch vernichtet oder für die Vernichtung dem ITZ übergeben werden.

3.4 Virenschutz

- Die Angehörigen der ZHdK dürfen die Sicherheitssoftware (Virenschutz, Firewall usw.) nicht ausschalten, blockieren oder umkonfigurieren.
- Im E-Mail-und Internet-Verkehr ist stets Vorsicht geboten: E-Mails mit verdächtigem Absender, Inhalt oder Anhang sollten nicht geöffnet und im Zweifelsfall gelöscht oder dem ITZ weitergeleitet werden. Es darf nicht auf verdächtige Plattformen zugegriffen werden;
- Jeder Verdacht auf Virenbefall muss sofort dem ITZ gemeldet werden.

3.5 Unerlaubte Nutzungen

In Ergänzung zu den bestehenden Regelungen, soll insbesondere auf folgende Verbote hingewiesen werden:

- Externe Internet-Dienste (wie z.B. Online-Dateiablagen, Online-Kollaborationsmittel usw.) oder E-Mail-Systeme dürfen nicht zur Verarbeitung und Speicherung von vertraulichen oder personenbezogenen Daten verwendet werden.
- Die Nutzung von rechtswidrigen oder rechtswidrig erlangten Inhalten oder Software ist untersagt, insbesondere das Herunterladen, die Aufbewahrung, die Verbreitung oder Verwertung solcher Daten. Ausgenommen davon sind entsprechende Nutzungen im Zusammenhang mit einem expliziten Auftrag der ZHdK.
- Die IT-Ressourcen der ZHdK dürfen nicht verwendet werden in Bezug auf fremde Systeme. Untersagt sind insbesondere:
    - Angriffe auf andere Systeme,
    - Ausspionieren fremder Passwörter und Daten,
    - Unbefugtes Verändern, Löschen, Unbrauchbarmachen oder Unterdrücken von Daten,
    - Unbefugtes Verändern von System- und Netzwerkkonfigurationen,
    - Bereitstellen von Netzwerkzugängen für Dritte (z.B. Access Points)

- Hochschulkritische- und Personendaten dürfen weder privat genutzt noch in privaten Datenablagen gespeichert werden.

- Das Versenden von Inhalten mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt, mit unnötig grossem Verteiler oder mit der Aufforderung zum Weiterversand im Schneeballsystem sind verboten.

4. Nutzung von E-Mail, Internet und Internet-Diensten (insbesondere Cloud-Dienste)

4.1 Allgemeine Bestimmungen

E-Mail, Internet und Internet-Dienste können für die Erfüllung geschäftlicher Aufgaben nach den Grundsätzen der Wirtschaftlichkeit, der Datensicherheit eingesetzt werden. Dabei sind die rechtlichen Anforderungen zwingend zu beachten.

Die Verwendung von externen digitalen Diensten (wie Cloud-Dienste, Soziale Netze [«Social Medias»]) bedingt eine vertragliche Basis zwischen den Anbieter und dem Nutzer (meist mittels AGB und Zustimmung). Es liegt dabei in der persönlichen Verantwortung des jeweiligen Benutzers, zu prüfen, ob überhaupt auf das Vertragsverhältnis (gemäss den vorgelegten AGB) eingegangen werden kann.

ZHdK Angehörige dürfen keine Personendaten oder sonstige vertrauliche Daten in Cloud-Diensten speichern. Bei der Verwendung von Cloud-Diensten ist grösste Vorsicht geboten, da das ITZ keine Sicherheit (vor allem Vertraulichkeit und Verfügbarkeit) für die dort gespeicherten Daten gewähren kann.

Generell unzulässig ist die Verwendung von Diensten, welche auf der «schwarzen Liste» des ITZ stehen.

Die Verantwortung insbesondere für Inhalt und Rechtsfolgen liegt aber in jedem Falle beim jeweiligen Benutzer.

4.2 E-Mail

Das automatische Weiterleiten von E-Mails und das Freigeben der persönlichen Mailbox an eine Drittperson, die nicht ZHdK Angehöriger ist, sind nicht erlaubt.

4.3 Internet / Internet-Dienste

- Hochschulrelevante Daten dürfen nur mit dem formellen Einverständnis der Hochschulkommunikation der ZHdK im Internet publiziert oder z.B. in Formularen bekannt gegeben werden.

- Schützenswerte Informationen (besonders schützenwerte Personendaten sowie vertrauliche Daten) und nicht anonymisierte Personendaten dürfen nur hinreichend verschlüsselt über das Internet übermittelt werden.

- Auf der Webseite des ITZ ist eine Liste mit Internet-Diensten zu finden, die nicht verwendet werden dürfen (Black List). Diese Liste ist wird laufend aktualisiert.

5. Private Nutzung von IT-Ressourcen

- Die zurückhaltende Benutzung von IT-Ressourcen für private Zwecke ist grundsätzlich gestattet, soweit dadurch die geschäftsrelevanten Systemressourcen wie Speicher und Übertragungskapazität sowie die Arbeitszeit nicht beeinträchtigt werden. Private E-Mails im ZHdK-E-Mail-Konto müssen entweder umgehend gelöscht oder in einem persönlichen Ordner mit entsprechender Bezeichnung abgelegt werden.

- Der Zugriff auf Internet-Seiten zu privaten Zwecken ist auf ein absolutes Minimum zu beschränken.

- Das Laptop darf für private Zwecke genutzt werden. Das ITZ bietet aber nur Hilfe bei Problemen mit Geschäftsapplikationen und -daten.

- Daten wie Text-, Bild- und Tondokumente, die nicht im Interesse der ZHdK verwendet werden, dürfen nicht auf den zentralen Datenablagesystemen der ZHdK gespeichert werden. Dazu zählen auch private Daten auf dem persönlichen Verzeichnis (Userhome bzw. Laufwerk H:).

- Die Benutzung der IT-Ressourcen zur Erbringung des Leistungsauftrages der Hochschule hat gegenüber anderen Nutzungszwecken stets Vorrang.

- Die Nutzung der IT-Ressourcen zu kommerziellen Zwecken oder zu privaten Werbezwecken bedarf einer Bewilligung der IT-Leitung.

6. Einsatz mobiler Geräte (inkl. BYOD[1])

- Auf mobilen Geräten und Datenträgern (z.B. Notebooks, USB-Sticks, Smartphones usw.) müssen Dokumente mit vertraulichem bzw. schützenswertem Inhalt verschlüsselt gespeichert werden. Bei häufigem Umgang mit schützenswerten Daten muss auf den mobilen Geräten die umfassende Verschlüsselung der Daten aktiviert werden.

- Mobile Geräte welche von der ZHdK zur Verfügung gestellt werden, dürfen in öffentlich zugänglichen Räumen nicht unbeaufsichtigt gelassen werden.

- Persönliche Geräte mit ZHdK-Inhalten dürfen Dritten nicht zur Nutzung überlassen werden.

- Der Verlust eines mobilen Gerätes ist unverzüglich dem ITZ zu melden; bei Geräten im persönlichen Eigentum nur dann, wenn das Gerät einen Zugriff auf ZHdK Informationen ermöglicht.

- Komponenten für die drahtlose Kommunikation (z.B. Bluetooth, WLAN, Infrarot etc.) und Ortungsdienste sind bei Nichtgebrauch zu deaktivieren.

Arbeiten Angehörige der ZHdK mit Geräten des persönlichen Eigentums und nutzen sie damit das ZHdK Netzwerk, verpflichten sie sich folgende Sicherheitsmassnahmen einzuhalten:

- Sämtliche dem heutigen Stand der Technik angemessenen Sicherheitsmassnahmen sind auf dem Gerät zu ergreifen. Darunter fallen zwingend folgende Installationen:
    - Aktuelle Betriebssystem Patches
    - Aktuelle Security-Patches für Adobe und Java
    - Einen aktuellen Virenscanner mit den neuesten Updates der Software und der Antivirus Definitions-Dateien
    - Eine Personal Firewall

Diese Schutzmassnahmen sind

- auf dem Gerät regelmässig zu aktualisieren bzw. auf Updates zu überprüfen,

- vor dem ersten Zugriff auf das Netzwerk der ZHdK zu installieren und solange aufrecht zu erhalten, wie die Zugriffsberechtigung auf das Netzwerk der ZHdK gültig ist.

7. Ausserordentliche Nutzungen und Ausnahmen

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

- Die IT-Leitung entscheidet über Ausnahmen von der vorliegenden Regelung. Entsprechende Gesuche sind ihr mit Begründung per E-Mail einzureichen.

8. Protokollierung und Kontrolle

- Zur Überwachung der Funktionalität, der Sicherheit, der Integrität und der Verfügbarkeit der Informatik werden Systeme eingesetzt, die Nutzungsdaten erheben.
- Internetzugriffe werden aufgezeichnet und ein halbes Jahr lang gespeichert. Eine personenbezogene Auswertung ist nur nach vorgängiger Information des Benutzenden und in Absprache mit dem Sicherheitsverantwortlichen der ZHdK möglich.

---

[1] Bring your onw device: Privates Gerät eines ZHdK Angehörigen, welches an der ZHdK eingesetzt wird.

9. Massnahmen bei Verstössen

Bei Zuwiderhandlungen egal ob aus Unwissen oder Fahrlässigkeit, gegen diese Regelung oder gegen die einschlägigen Gesetzesbestimmungen kann die Hochschulleitung von sich aus oder auf Antrag der IT-Leitung ungeachtet einer allfälligen strafrechtlichen Ahndung oder Schadenersatzforderungen einer fehlbaren Person

- den Zugang zu den IT-Ressourcen einschränken oder ihr den Zugang vollständig untersagen,
- gegenüber Angestellten eine personalrechtliche Sanktion aussprechen,
- gegenüber Studierenden disziplinarische Massnahmen anordnen.

Die entsprechenden Massnahmen werden innerhalb der vorgesehenen Verfahren durchgeführt. Vorbehalten bleiben weitere arbeitsrechtliche, disziplinarische und strafrechtliche Massnahmen durch entsprechende Stellen.

9.1 Massnahmen durch die ITZ-Leitung

Die ITZ-Leitung kann die folgenden Massnahmen anordnen:

- Blockierung missbräuchlicher oder rechtswidriger Daten sowie deren Sicherung und Aufbewahrung zu Beweiszwecken.
- Löschung missbräuchlicher oder rechtswidriger Daten, soweit dies aus Sicherheitsgründen erforderlich ist.
- Antragstellung von weiteren Massnahmen gegenüber den zuständigen internen Instanzen.
- Blockierung, Deaktivierung und vorübergehende Ausschaltung von IT-Systemen.

10. Schlussbestimmungen

Dieses Reglement wurde von der Hochschulleitung am 4. Juni 2014 erlassen und ist ab 4. Juni 2014 gültig.