Weisung betreffend Nutzung von Informatikmitteln

Nachfolgend werden die wichtigsten Bestimmungen zur Nutzung der Informatikmittel der Fachhochschule Nordwestschweiz (FHNW) zusammengefasst:

- Die Zugangsberechtigung und Identifikationsmethoden wie Passwörter, PINs, Chipkarten, etc. sind persönlich und daher vertraulich; sie dürfen weder weitergegeben noch Dritten zugänglich gemacht werden.
- Die **Nutzung von Informatikmitteln** ist für diejenigen Zwecke erlaubt, für welche die Informatikmittel dem Benutzenden zur Verfügung gestellt werden („bestimmungsgemässe Nutzung"). Die Nutzung von Informatikmitteln **ist für private Zwecke erlaubt**, soweit sie nicht übermässig ist und die Erfüllung der Arbeits- oder Studienpflichten nicht beeinträchtigt. Die Nutzung von Informatikmitteln der FHNW darf nicht zu einer technischen Störung oder Beeinträchtigung des Betriebs der FHNW oder zu einer unverhältnismässigen Beanspruchung oder Belastung von allgemein genutzten Ressourcen (Netzwerke, Internetzugang, etc.) führen.
- Das **vollständige oder teilweise Kopieren von FHNW-lizenzierter Software** (Programme und Dokumentation), gleich welcher Herkunft, ist untersagt, soweit nicht Lizenzbestimmungen oder das Urheberrechtsgesetz dies ausdrücklich erlauben.
- Die **private Nutzung** von **FHNW-lizenzierter Software** ist für an der FHNW immatrikulierte Studierende bzw. Mitarbeitende erlaubt, soweit dies der jeweilige Lizenzvertrag zulässt. Der Basisdienst der Hochschule bzw. des Sitzes gibt über die entsprechenden Nutzungsmöglichkeiten Auskunft.
- Alle Benutzenden sind **persönlich** dafür **verantwortlich,** dass die Benutzung der Informatikmittel nicht gegen Bestimmungen dieser Benutzungsordnung oder gegen die Rechtsordnung (z.B. Strafrecht, Datenschutz) verstösst bzw. die Rechte Dritter (z.B. Urheberrechte, Lizenzbestimmungen, Persönlichkeitsrechte) verletzt.
- Die Benutzenden haben die ihnen von der FHNW zur Verfügung gestellten Informatikmittel mit der **gebotenen Sorgfalt zu nutzen**. Technische und betriebliche Anordnungen der Abteilung Information and Communication Technologies ICT, der bzw. des Systemverantwortlichen der Benutzereinheiten oder der bzw. des ICT-Sicherheitsbeauftragten sind für alle Benutzenden verbindlich.
- Für grobfahrlässig oder absichtlich verursachte Schäden und technische Störungen an Informatikmitteln der FHNW haftet in jedem Fall der bzw. die Verursachende. Bei nicht bestimmungsgemässer Nutzung haften Verursachende auch für leichte Fahrlässigkeit. Bei grobfahrlässiger oder absichtlicher Verletzung von Rechten Dritter (insbesondere Urheberrechten und Lizenzbestimmungen) werden die Benutzenden auch für denjenigen Schaden haftbar, für den die FHNW allenfalls von Dritten belangt wird.
- **Die Verwendung von privaten Geräten im Netzwerk der FHNW ist nur mit Einhaltung von Sicherheitsmassnahmen erlaubt.** Dazu gehören insbesondere: Installation und Aktivierung der neuesten Antivirus-Software; Installation der Sicherheitsupdates der Betriebssysteme; regelmässige Datensicherung; sofortiges Melden von Sicherheitsproblemen an den ICT Basisdienst der Hochschule bzw. des Sitzes. Die Verantwortung für die Erfüllung der Sicherheitsmassnahmen obliegt der Eigentümerin oder dem Eigentümer des privaten Gerätes.

Missbräuchlich ist jede Nutzung von Informatikmitteln der FHNW, die die Vorschriften dieser Benutzungsordnung missachtet, gegen übergeordnetes Recht verstösst oder Rechte Dritter verletzt. Als **missbräuchlich gelten namentlich die folgenden Verhaltensweisen:**

- Die Verarbeitung, Speicherung oder Übermittlung von Material mit widerrechtlichem oder unsittlichem Inhalt, wie z.B. Gewaltdarstellungen, Pornographie (Art. 197 des Schweizerischen Strafgesetzbuches StGB), Aufforderung zu Verbrechen oder Gewalttätigkeit (Art. 259 StGB), Störung der Glaubens- und Kultusfreiheit (Art. 261 StGB) oder Rassendiskriminierungen (Art. 261bis StGB);
- Die Herstellung, die Anleitung zur Herstellung oder absichtliche Verbreitung von schädlichen Programmen oder Programmteilen im Sinne von Art. 144bis Ziff. 2 StGB (Viren, Würmer, Trojaner, etc.). Die Anleitung zur Herstellung von solchen Programmen zu Zwecken der Lehre und Forschung kann erlaubt werden, wenn angemessene Vorkehrungen gegen ihre schädigende Verwendung getroffen werden und vorgängig die schriftliche Zustimmung der Schulleitung oder der von dieser als zuständig erklärten Stelle eingeholt worden ist;
- Das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB „Hacking“): Ausspionieren von Passwörtern, unautorisiertes Absuchen von internen und externen Netzwerken auf Schwachstellen (z.B. Port-Scanning), Vorkehrung und Durchführung von Massnahmen zur Störung von Netzwerken und Computern (z.B. Denial of Service Attacks). Im Einzelfall kann das „Hacking“ in einer sicheren Testumgebung zu Zwecken der Lehre und Forschung erlaubt sein, sofern vorgängig die schriftliche Zustimmung der Schulleitung oder der von dieser autorisierten Stelle eingeholt worden ist. Für die Beseitigung von Verwundbarkeiten und Sicherheitslücken dürfen die Netzwerkbereich- und Systemverantwortlichen der ICT die aufgeführten Methoden (z.B. Port-Scanning) anordnen und durchführen.
- Datendiebstahl (Art. 143 StGB) und Datenbeschädigung (Art. 144bis Ziff. 1 StGB);
- Die Nutzung von Informatikmitteln der FHNW in absichtlicher Verletzung von Lizenzbestimmungen oder Urheberrechten;
- Das Versenden von Mitteilungen mittels elektronischer Kommunikationsmittel mit vorgetäuschten oder irreführenden Absenderangaben (inkl. technischer Adresse) oder von unverlangten Werbe-E-Mails (SPAM);
- Die Belästigung oder Irreführung von Angehörigen der FHNW oder Dritter durch Mitteilungen mit elektronischen Kommunikationsmitteln (z.B. mit persönlichkeitsverletzenden, sexistischen, rassistischen, rufschädigenden oder diskriminierenden Inhalten);
- Das Einrichten von Direktanschlüssen an die FHNW-Kommunikationsnetze (z.B. durch Modems, oder WLAN Access Points) ohne vorgängige schriftliche Zustimmung der Abteilung ICT der Services.

Als schwerer Missbrauch gelten:
- Missbräuche welche vorsätzlich bzw. absichtlich erfolgen
- Missbräuche im Wiederholungsfall

Wird ein Missbrauch festgestellt, so kann die bzw. der ICT-Sicherheitsbeauftragte entsprechende Massnahmen und Sanktionen anordnen, wie etwa die Sperrung des Zugangs zu Informatikmitteln. Bei **schwerem Missbrauch** wird **in jedem Fall ein Disziplinarverfahren** und gegebenenfalls auch ein Zivil- und Strafverfahren eingeleitet. Besonders schwere Fälle können zur Entlassung bzw. Exmatrikulation führen. Die bzw. der ICT-Sicherheitsbeauftragte leitet Fälle von schwerem Missbrauch an die Direktion der FHNW zur weiteren Behandlung und Entscheidung weiter.

Alle Benutzenden eines offen zugänglichen Unterrichtscomputers der FHNW haben sich auf Nachfrage gegenüber Dozierenden, Assistentinnen und Assistenten, der Mitarbeitenden der Abteilung Information and Communication Technologies ICT sowie der bzw. dem ICT-Sicherheitsbeautragten durch Immatrikulationsausweis oder Personalausweis auszuweisen.

Kontaktstellen:
1. ICT Basisdienst der Hochschule bzw. des Sitzes
2. Abteilung Information and Communication Technologies ICT der Services
3. ICT-Sicherheitsbeauftragte der FHNW

Anmerkungen:
Bei Lizenzverletzungen durch Anbieten bzw. durch zur Verfügung stellen von Musik-, Film oder anderen Dateien auf Websites oder anderen Datenhaltungssystemen müssen die Mitarbeitenden bzw. Studierenden mit möglichen Schadenersatzforderungen rechnen.

Der bzw. die ICT-Sicherheitsbeauftragte kann gestützt auf die Datenschutzgesetzgebung die Mitarbeitenden der Abteilung Information and Communication Technology ICT beauftragen, Protokollierungen (z.B. Logfiles) summarisch auszuwerten, ohne dabei bestimmte Personen zu identifizieren. Ergibt sich aus dieser nicht personenbezogenen Auswertung ein Verdacht auf Verstoss gegen die Weisung betreffend Nutzung von Informatikmitteln, kann der oder die ICT-Sicherheitsbeauftragte nach Ankündigung die Aufzeichnungen personenbezogen während einer begrenzten Zeitdauer auswerten, um fehlbare Personen zu ermitteln.

Grundsätzlich werden die Mitarbeitenden, die Studierenden im Voraus darüber informiert, wenn eine personenbezogene Prüfung vorgenommen wird. Auf die Vorankündigung kann auf Anordnung der bzw. des ICT-Sicherheitsbeauftragten verzichtet werden, wenn
- die Datensicherheit, insbesondere die Verfügbarkeit der Systeme nicht mehr garantiert werden kann oder
- Anhaltspunkte für ein rechtswidriges, insbesondere strafbares Handeln vorliegen.

Wird aufgrund der personenbezogenen Prüfung ein Missbrauch festgestellt, werden die Direktionspräsidentin, der Direktionspräsident bzw. die Strafverfolgungsbehörde informiert.