Fachhochschule Nordwestschweiz

Reglement betreffend Nutzung der FHNW IT-Infrastruktur (IT-Reglement)

Vom Leiter Services FHNW erlassen am 12. Mai 2017

Vom Direktionspräsident FHNW genehmigt am 1. Juni 2017

I. Allgemeiner Teil

1. Zweck und Geltungsbereich

1 Dieses Reglement dient der Informatiksicherheit der FHNW und der rechtlich zulässigen Nutzung der IT-Infrastruktur der FHNW.

2 Dieses Reglement gilt für alle Angehörigen der FHNW (Mitarbeitende und Studierende), die über ein persönliches FHNW-Konto verfügen.

3 Dieses Reglement ist ein mitgeltendes Reglement des GAV FHNW gemäss Ziff. 15.1 GAV.

2. Begriffe

1 *FHNW IT-Infrastruktur:* Die IT-Infrastruktur der FHNW umfasst alle Informatikmittel mit denen Daten erstellt, bearbeitet, gespeichert oder präsentiert werden können sowie alle IT- Komponenten, die für den Datentransport eingesetzt werden. Weiter gehören zur FHNW IT-Infrastruktur auch Räume, Systeme und Installationen die zum Betrieb der oben genannten Informatikmitteln und IT-Komponenten gehören.

2 *Identifikationsmethoden:* Verfahren zur eindeutigen Identifizierung einer Person, wie beispielsweise das Abfragen von Passwörtern oder PIN-Codes sowie die Identifizierung über kontaktlose Lesegeräte mit der FH-Card.

3 *SPAM*: Als Spam werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden und mit häufig werbendem Inhalt.

4 *Randdaten*: Sind Aufzeichnungen über die Nutzung der elektronischen Infrastruktur. Darunter fallen Informationen über Absender und Empfänger, Zeitpunkt, Dauer und Weg der Kommunikation.

5 *Sicherheitsmassnahmen:* Durch verschiedene Sicherheitsfunktionen und Sicherheits-anwendungen werden die FHNW IT-Infrastruktur und die Daten der Angehörigen der FHNW insbesondere vor Missbrauch, Diebstahl oder Beschädigung geschützt. Dies erfolgt insbesondere mittels Virenschutz, Ad-Blocker, Firewall, Verschlüsselungs-techniken, passwortgeschütztem Zugang, dem Protokollieren der Nutzung der FHNW IT-Infrastruktur (Aufzeichnen von Randdaten) für Auswertungen und der Möglichkeit der Reaktion per Fernzugriff.

6 *Missbrauch:* Missbräuchlich ist jede Nutzung der FHNW IT-Infrastruktur, welche die Vorschriften dieses Reglements missachtet, gegen übergeordnetes Recht verstösst oder Rechte Dritter verletzt (wie zum Beispiel die Verarbeitung, Speicherung oder Über-mittlung von Material mit widerrechtlichem oder unsittlichem Inhalt, insbesondere Gewaltdarstellungen und Pornografie; die Aufforderung zu Verbrechen oder zur Gewalttätigkeit; Störung der Glaubens- und Kultusfreiheit oder Rassendiskriminierungen).

II. Rechte und Pflichten der Angehörigen der FHNW sowie Haftung

3. Recht der Mitarbeitenden FHNW

1 Die FHNW stellt den Mitarbeitenden gemäss Ziffer 11.7 GAV die für die interne und externe Kommunikation notwendigen Hilfsmittel zur Verfügung. Weiter haben sie das Recht die FHNW IT-Infrastruktur zur Aufgabenerfüllung zu nutzen.

2 Die Nutzung von Informatikmitteln der FHNW ist für private Zwecke erlaubt, soweit die berufliche Leistungsfähigkeit nicht beeinträchtigt ist und sie nicht gegen die legitimen Interessen der FHNW verstösst.

4. Recht der Studierenden FHNW

1 Die Studierenden der FHNW haben das Recht, die zur Verfügung gestellte FHNW IT-Infrastruktur zu Zwecken des Studiums zu nutzen.

5. Pflichten der Angehörigen der FHNW

1 Die Angehörigen nutzen die FHNW IT-Infrastruktur sorgfältig, fachlich und rechtlich korrekt.

2 Die Zugangsberechtigung und Identifikationsmethoden sind persönlich und daher vertraulich. Sie dürfen Dritten nicht zugänglich gemacht werden.

3 Passwörter müssen der Richtlinie "Passwörter für Benutzende, Administratoren und Dienste erstellen und anwenden" entsprechen.

4 Die Verwendung von privaten Geräten zur Bearbeitung von Daten der FHNW ist nur unter Einhaltung der Sicherheitsmassnahmen gemäss Ziffer 2 Abs. 5 erlaubt. In begründeten Fällen kann die FHNW spezifische Sicherheitsmassnahmen verlangen. Bei Verwendung privater Geräte liegt die Verantwortung für die Erfüllung der Sicherheitsmassnahmen bei den Angehörigen der FHNW.

5 Das Versenden und Weiterleiten von SPAM ist zu unterlassen.

6 Das Erweitern, Ändern oder Stören der FHNW IT-Infrastruktur ist zu unterlassen. Ausnahmen zum Zwecke der Lehre und Forschung werden vom Direktor, der Direktorin der Hochschule angeordnet und benötigen die vorgängige Genehmigung des Leiters Corporate IT, der Leiterin Corporate IT.

7 Analysen der FHNW IT-Infrastruktur bezüglich IT-Sicherheit und Architektur sind ausschliesslich durch die zuständigen Angehörigen der Corporate IT FHNW durchzuführen.

8 Die Angehörigen der FHNW müssen ihnen bekannt gewordene, sicherheitsrelevante Vorfälle, rechtswidriges Verhalten oder relevante Sicherheitsmängel umgehend an it-security@fhnw.ch oder den IT-Support vor Ort melden.

6. Haftung

1 Die Angehörigen der FHNW haften für Schäden, die durch eine grobfahrlässige oder vorsätzliche Verletzung des vorliegenden Reglements entstehen.

2 Die FHNW lehnt jede Haftung für Schäden ab, die sich aus der privaten Nutzung der FHNW IT-Infrastruktur ergeben.

III. Sicherstellung der IT-Sicherheit und Massnahmen bei Missbrauch

7. Auswertungen der Protokolle

1 Zur Sicherstellung der IT-Sicherheit ordnet der oder die Informatik-Sicherheitsbeauftragte (I-SIBE) regelmässig die Auswertung der anonymisierten Protokolle der Informatikaktivitäten an. Personen sind dabei nicht identifizierbar.

2 Besteht ein begründeter Verdacht auf rechtswidriges Verhalten, insbesondere Missbrauch, werden die massgebenden Informationen gesichert und personenbezogen ausgewertet. Bei personenbezogenen Auswertungen sind die betroffenen Personen identifizierbar. Der Vizepräsident (Leiter Services) ordnet in seiner Funktion als Gesamtverantwortlicher Sicherheit FHNW auf schriftlichen Antrag des, der I-SIBE oder eines Mitglieds der Direktion FHNW die personenbezogenen Auswertungen an. Der Vizepräsident entscheidet über den Beizug der vorgesetzten Stelle.

3 Der I-SIBE informiert die betroffenen Angehörigen der FHNW vor der personenbezogenen Auswertung. Bei Vereitelungsgefahr oder zeitlicher Dringlichkeit kann die Information nach der personenbezogenen Auswertung erfolgen.
Jede personenbezogene Auswertung wird vom I-SIBE dokumentiert.

8. Massnahmen bei Missbrauch

1 Stellt der I-SIBE aufgrund einer personenbezogenen Auswertung einen Missbrauch durch eine Angehörige, einen Angehörigen der FHNW fest, sichert der I-SIBE die entsprechenden Protokolle und informiert die Anstellungsinstanz bzw. die zuständige Studiengangleiterin/Institutsleiterin, den zuständigen Studiengangleiter/Institutsleiter, sowie den Vizepräsidenten (Leiter Services).

5 Bei Missbrauch durch Mitarbeitende der FHNW verfügt die Anstellungsinstanz der betroffenen Person die im GAV vorgesehenen Massnahmen.

6 Bei Missbrauch durch Studierende der FHNW verfügt die Hochschule die in der Studien- und Prüfungsordnung vorgesehenen Massnahmen.

7 Schwerwiegender Missbrauch wird bei der Strafverfolgungsbehörde angezeigt.

IV. Schlussbestimmungen

9. Inkrafttreten

1 Die Mitwirkung wurde beiden Parteien gemäss GAV Ziff. 4.9 der Mitwirkungsstufe "Mitentscheidung paritätisch" gewährt.

2 Dieses Reglement tritt am 1.6.2017 in Kraft und ersetzt die Weisung betreffend Nutzung von Informatikmitteln vom 1.11.2013.