Ansprechpartner in Fachbereichen

Bei Fragen können Sie sich an die zuständigen Mitarbeiterinnen und Mitarbeiter Ihres Fachbereichs wenden, deren Kontaktadressen finden Sie unter:

www.hs-fulda.de/it-sicherheit
→ Ansprechpartner → 5. Ansprechpartner in Fachbereichen.

Ansprechpartner in Verwaltung und zentralen Einrichtungen

Knut Merz
IT-Sicherheitsbeauftragter in der Verwaltung
Telefon 0661 9640-1301
E-Mail Knut.Merz@rz.hs-fulda.de

Hendrik Wesner
IT-Sicherheitsbeauftragter in der Hochschul- und Landesbibliothek
Telefon 0661 9640-9803
E-Mail Hendrik.Wesner@hlb.hs-fulda.de

Bei speziellen Problemen, wie zum Beispiel mit dem E-Mail-Client oder der WLAN/VPN-Verbindung wenden Sie sich an die Ansprechpartner im Rechenzentrum:

www.hs-fulda.de/it-sicherheit
→ Ansprechpartner → 6. Ansprechpartner im Rechenzentrum.

IT-Sicherheit

Hochschule Fulda

02|21

Zentrale Ansprechpartner

Prof. Dr. Siegmar Groß
IT-Sicherheitsbeauftragter der Hochschule Fulda
Telefon 0661 9640-3333
E-Mail IT-Sicherheitsbeauftragter@hs-fulda.de

Sonja Redweik
Datenschutzbeauftragte
Telefon 0661 9640-1051
E-Mail Datenschutzbeauftragte@hs-fulda.de

Knut Merz
IT-Sicherheitsbeauftragter des Rechenzentrums
Telefon 0661 9640-1301
E-Mail Knut.Merz@rz.hs-fulda.de

IT-Sicherheitsrichtlinien der Hochschule Fulda

Internet www.hs-fulda.de/it-sicherheit

Hochschule Fulda
University of Applied Sciences

IT-Sicherheit

Hochschule Fulda

Hochschule Fulda
University of Applied Sciences

IT-Sicherheit

Hochschule Fulda

Liebe Studierende,

um Ihnen, Ihren Kommilitoninnen und Ihren Kommilitonen sowie anderen Nutzern ein effizientes und ungestörtes Arbeiten an den Hochschulcomputern und -netzwerken zu ermöglichen, hat die Hochschule Fulda eine **IT-Sicherheitsrichtlinie (einsehbar unter www.hs-fulda.de/it-sicherheit)** verabschiedet und hält alle Nutzer an, sich an diese zu halten.

Auf diesem Flyer finden Sie die wichtigsten Informationen sowie Links, die Ihnen den Zugang zur Rechnernutzung erleichtern sollen.

Benutzungsordnung

Die wichtigsten Rechte und Pflichten der Benutzer:

- Nutzen Sie die zur Verfügung gestellten Mittel verantwortungsvoll und ökonomisch sinnvoll.
- Vermeiden Sie alles, was den Betrieb stört, Schaden an der IT-Infrastruktur oder für andere Benutzer verursacht.
- Es ist verboten, die Computer oder Netzwerke missbräuchlich zu benutzen.
- Die Weitergabe von Benutzerkennungen und Passwörtern ist nicht gestattet.
- Melden Sie sich nach Benutzung eines Computers ab.
- Halten Sie sich an Copyright und Urheberrechte.
- Halten Sie sich an die in Lizenzverträgen vereinbarten Bedingungen bei der Benutzung von Programmen.
- Software, Dokumentationen und Daten dürfen nicht für gewerbliche Zwecke genutzt, kopiert o. weitergegeben werden.
- Es ist verboten, die Konfiguration der Betriebssysteme, Programme oder des Netzwerks zu verändern.
- Sie tragen die volle Verantwortung für alle Aktionen, die unter Ihrer Benutzerkennung vorgenommen werden.

Gute Passwörter

erfüllen 3 wichtige Eigenschaften:

1. Sie enthalten mindestens einen Groß- und einen Kleinbuchstaben sowie eine Ziffer und ein Sonderzeichen.
2. Sie sind mindestens 8 Zeichen lang.
3. Das Passwort ist kein Wort (auch nicht fremdsprachig), wenn man die Ziffern und Sonderzeichen weglässt.

Tipp:

- Denken Sie sich einen Merksatz aus, z. B.: „Ich wohne seit 12 Jahren in Deutschland“. Benutzen Sie die Anfangsbuchstaben der Wörter und zum Beispiel Sonderzeichen nach Ziffern, also: Iws1;2.JiD
- Ändern Sie sofort Ihr Passwort, wenn es in fremde Hände geraten ist oder Sie den Verdacht haben, dass es unautorisierten Personen bekannt geworden ist.

Weitere Hinweise finden Sie auf:

www.hs-fulda.de/it-sicherheit → Grundschutz

www.hs-fulda.de/it-sicherheit → Passwörter

E-Mail

Eine E-Mail sollte immer nur als normaler Text versendet und angezeigt werden, da HTML-Code Schad-Software enthalten kann. Klicken Sie nie auf einen "Link" in einer E-Mail und öffnen Sie nie HTML- oder Office-Dokumente im Anhang von unbekannten Mail-Adressen. Denken Sie daran, dass Absender gefälscht sein können.

Tipps zur richtigen Einstellung von Thunderbird, Outlook und Novell GroupWise finden Sie auf:

www.hs-fulda.de/it-sicherheit → E-Mail.

Web-Browser

Schalten Sie grundsätzlich die Funktion der Pop-Up-Fenster aus, denn diese sind zum einen lästig und zum anderen ein Sicherheitsrisiko, wenn Sie versehentlich in einen Bereich des Fensters klicken.

Sie sollten niemals Passwörter in Programmen oder Dateien speichern. Dies ist zwar praktisch, lädt aber Hacker geradezu ein, Ihre Benutzerkennungen zu missbrauchen. Phishing bezeichnet ein Verfahren, mit dem man Benutzerdaten (Benutzername, Passwort, Kontonummer, ...) erlangen will. Schalten Sie einen Phishing-Filter ein, falls der Browser dies unterstützt.

Weitere Einstellungsempfehlungen zu den Browsern Firefox, Internet Explorer, Edge, Safari, Chrome und Opera finden Sie auf:

www.hs-fulda.de/it-sicherheit → Web-Browser.

Office-Programme

Schalten Sie "Makros" in Office-Programmen aus, da sie zur Installation und Verbreitung von Schad-Software benutzt werden können.

Ausführliche Hinweise finden Sie auf:

www.hs-fulda.de/it-sicherheit → Office-Makros deaktivieren.

Stand der Informationen Februar 2021