

**für Computer,
Tablets und Smartphones**

Passwörter

Umgang mit Zugangsdaten

- › Geben Sie Passwörter niemals weiter.
- › Wenn Ihr Passwort anderen bekannt geworden ist, ändern Sie es sofort oder lassen Sie Ihren Zugang vorübergehend sperren.
- › Verwenden Sie möglichst unterschiedliche Passwörter für die Anmeldungen bei verschiedenen Diensten.

Erzeugen von sicheren Passwörtern

- › Achten Sie auf ein ausreichend komplexes Passwort (mindestens acht Zeichen mit Sonderzeichen).
- › Vermeiden Sie sich ähnelnde Passwörter sowie Passwörter mit persönlichem Bezug.
- › Sichere Passwörter können leicht durch einen Passwortgenerator oder durch die Anfangsbuchstaben von Merksätzen erzeugt werden.
- › Passwörter können an einem sicheren Ort z.B. in einem Passwortsafe hinterlegt werden.



Sicherheit beim Arbeiten

Arbeitskennung

- › Arbeiten Sie bei der täglichen Arbeit ohne Administratorrechte, damit keine Systemdateien ohne Ihre Kenntnis geändert werden können.
- › Sperren Sie den PC bei Arbeitspausen.

Betriebssystem- und Programmaktualisierungen

- › Installieren Sie regelmäßig Updates.
- › Aktivieren Sie automatische Update-Funktionen und überprüfen Sie ggf. selbst, ob neue Updates für Ihre Programme vorhanden sind.
- › Achten Sie auf eine aktive Firewall.

Virenschutz

- › Installieren Sie ein Antivirenprogramm, um sich vor Schadsoftware (u.a. Viren und Trojaner) zu schützen. Das ZIV bietet eine entsprechende Software zum kostenlosen Download an und unterstützt Sie auch bei der Installation.
- › Führen Sie nach einem Virenbefall eine Neuinstallation des PCs durch.



Schutz und Sicherung Ihrer Daten

Weitergabe persönlicher Daten

- › Wählen Sie sorgfältig aus, wem Sie persönliche Daten wie Kontoinformationen oder Adressen geben.
- › Achten Sie bei öffentlichen PCs und mobilen Internetverbindungen darauf, sensible Daten verschlüsselt und zertifiziert zu übertragen.

Datensicherung

- › Fertigen Sie regelmäßig Backups an, um Datenverlust zu vermeiden. Das ZIV bietet für universitätsbezogene Dateien einen persönlichen Speicherplatz an.
- › Speichern Sie Sicherungskopien nicht auf Ihrem PC, sondern auf externen Datenträgern.

Verschlüsselung von sensiblen Daten

- › Verschlüsseln Sie Ihre Daten und mobile Datenträger, damit Unbefugte nicht darauf zugreifen können.

