Universität Bamberg

10 goldene Regeln

zur Informationssicherheit an der Universität Bamberg

1. Vorsicht bei der mobilen Nutzung und mit Datenträgern von Dritten!

Mobilgeräte, wie Laptops oder Smartphones, und mobile Datenträger, wie USB-Sticks, können leicht verloren gehen. Daher haben kritische Daten auf solchen Systemen nichts zu suchen oder sie müssen (beispielsweise durch die Verschlüsselung der Festplatte oder des Datenträgers) besonders geschützt werden. Behalten Sie Ihren Laptop in öffentlichen Bereichen im Auge. Achten Sie darauf, dass beim Arbeiten im Zug oder Flugzeug keine unerwünschten Blicke auf vertrauliche Unterlagen fallen können.

Seien Sie kritisch bei der Verwendung mobiler Datenträger anderer Personen (z.B. USB-Sticks, Speicherkarte, mobile Festplatte, CD, DVD) und schließen Sie diese nicht einfach an Ihren Computer an. Mobile Datenträger können Schadsoftware enthalten, die gezielt Passwörter ausforschen, Systeme fernsteuern, Schutzsoftware deaktivieren und Daten ausspionieren, um gegebenenfalls Geräte, Zubehör, Schriftstücke und Datenträger zu manipulieren oder zu zerstören.

Überprüfen Sie einen mobilen Datenträger immer auf Viren. Schließen Sie keinen mobilen Datenträger mit unbekannter Herkunft an Ihren Rechner an.

2. Halten Sie Ihr System aktuell und beachten Sie Systemhinweise!

Ein Betriebssystem benötigt regelmäßig Updates. Führen Sie diese Updates regelmäßig durch. Meistens werden Sie dazu vom System aufgefordert, zum Beispiel dazu, den Rechner neu zu starten, damit die Updates installiert werden können. Erledigen Sie dies am besten immer sofort, wenn Sie über ein Symbol oder eine entsprechende Systemnachricht dazu aufgefordert werden! Denn: Mit Updates werden oftmals auch Sicherheitslücken des Systems geschlossen.

3. Trennen Sie Dienstliches und Privates!

Wenn Sie dienstlich eine E-Mail verfassen, nutzen Sie eine E-Mail-Adresse der Universität Bamberg – entweder Ihre persönliche E-Mail-Adresse *vorname.nachname@uni-bamberg.de* oder eine aufgabenbezogene E-Mail-Adresse *bezeichnung.kürzel@uni-bamberg.de*. Schreiben Sie aber eine private E-Mail, dann nutzen Sie dazu Ihre private E-Mail-Adresse bei gmx, web.de, gmail, t-online etc.

Es ist grundsätzlich untersagt, dienstliche E-Mails an Postfächer von anderen Anbietern, wie gmx, web.de, gmail, t-online etc., weiterzuleiten.

Für dienstliche Daten nutzen Sie ausschließlich dienstlichen Speicherplatz, wie z.B. das Netzlaufwerk auf dem Fileserver an der Universität Bamberg. Für private Daten verwenden Sie ausschließlich privaten Datenspeicher.

4. Nutzen Sie Cloud-Dienste achtsam!

Grundsätzlich dürfen ausschließlich Informationen, die als öffentlich deklariert sind, in einem Cloud-Dienst gespeichert werden, der nicht von der Universitätsleitung und dem Rechenzentrum empfohlen wird. Verwendbare Cloud-Dienste für dienstliche Zwecke sind die von der Universität zentral bereitgestellten Fileserver (Netzlaufwerke) und TeamDrive.

Bei allen anderen Cloud-Diensten, wie Dropbox, Google Drive etc., achten Sie unbedingt darauf, dass dort ausschließlich unkritische Daten abgelegt werden, keine dienstlichen, keine persönlichen, keine vertraulichen oder gar geheimen Daten.

5. Gehen Sie bewusst mit sensiblen Daten um!

Personenbezogene Daten und Daten, die vertraulich sind, müssen Sie mit besonderer Sorgfalt behandeln. So haben Daten der Studierenden nichts bei Dropbox, Google und Co. zu suchen und auch nichts auf Ihrem privaten Rechner.

Speichern Sie sensible Daten sicher vor dem Zugriff von Unbefugten!

6. Geben Sie Zugangsdaten niemals weiter!

Geben Sie niemals – auch nicht Mitarbeiterinnen und Mitarbeitern des Rechenzentrums! – das Kennwort Ihres Benutzernamens (BA-Nummer) weiter. Nach der BA-Nummer werden Sie gegebenenfalls gefragt. Das Kennwort dürfen nur Sie wissen und nicht weitergeben.

7. Verwenden Sie sichere Kennwörter!

a. So sieht ein sicheres Kennwort aus: $EI8sam!

   1. Mindestens 8 Zeichen
   2. Phantasiewörter, keine Namen, Geburtstage etc.
   3. Zahlen, Buchstaben und Sonderzeichen

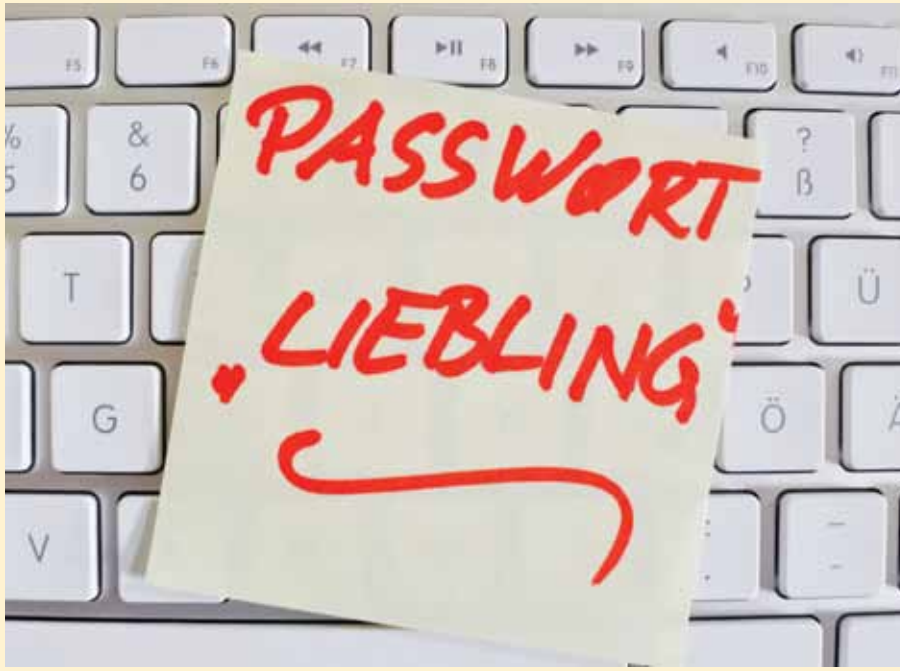
   An der Universität Bamberg verwenden Sie mit Ihrer BA-Nummer nur ein Kennwort für mehrere IT-Dienste. Verwenden Sie dieses Kennwort nicht für andere Dienste, z.B. für Ihr privates E-Mail-Postfach oder für einen externen IT-Dienst, bei dem Sie Ihre E-Mail-Adresse der Uni Bamberg hinterlegen.

b. Verwenden Sie unterschiedliche Kennwörter!

   Verwenden Sie im Internet unbedingt unterschiedliche Kennwörter für verschiede Dienste! Schon das Anhängen einer dienstspezifischen Buchstabenfolge an ein gutes Grundpasswort hilft und erschwert das Merken kaum.
   Aus „$EI8sam!“ wird bspw. „$EI8sam!AM“ für einen Dienst und „$EI8sam!EB“ für einen anderen.

c. Ändern Sie in regelmäßigen Abständen Ihr Kennwort/Ihre Kennwörter!

d. Verwenden Sie entweder Kennwörter, die Sie sich merken können, oder nutzen Sie einen Kennwort-Safe.



So nicht: Schreiben Sie keinesfalls ein Kennwort auf einen Zettel und bewahren ihn an Ihrem Rechner oder in seiner Nähe auf.

8. Nutzen Sie sichere Datenspeicher!

Speichern Sie Ihre Daten auf einem sicheren Datenspeicher. An der Universität Bamberg sind dies vor allem die aufgabenbezogenen Fileserver (Netzlaufwerk). Die auf den Fileservern abgelegten Daten werden täglich vom Rechenzentrum zusätzlich in einem Backup gesichert.

Wenn Sie Ihre Daten lokal auf Ihrem PC oder Laptop speichern, müssen Sie sich selbstständig um eine regelmäßige Datensicherung auf einem zusätzlichen Datenträger kümmern!

9. Seien Sie kritisch bis misstrauisch!

a. Prüfen Sie in E-Mails angegebene Links, bevor Sie diese anklicken.

b. Seien Sie auch dann misstrauisch, wenn eine E-Mail vermeintlich von einem Ihnen bekannten Absender stammt (Kollegin, Kollege, Lieferanten ...). Fragen Sie im Zweifel bei der Absenderin oder dem Absender nach, bevor Sie Anhänge von E-Mails öffnen, die Ihnen auch nur leicht seltsam vorkommen.

c. Speichern Sie angehängte Dateien und überprüfen Sie diese vor dem Öffnen mit dem Virenscanner.

d. Geben Sie niemals Ihr Kennwort oder andere vertrauliche Daten weiter.

e. Lesen Sie eine E-Mail aufmerksam; oftmals ist schon an Formulierungen die Echtheit und Vertrauenswürdigkeit des Absenders erkennbar.

10. Wenden Sie sich bei Unsicherheit oder mit Ihren Fragen an Fachleute!

Wenn Sie sich unsicher sind, ob eine E-Mail echt ist, ein Link vertrauenswürdig oder ein Datenträger nutzbar, wenden Sie sich einfach ans Rechenzentrum. Der IT-Support kann Ihnen entweder direkt helfen oder an entsprechendes Fachpersonal weiterleiten.

Telefon: +49 951 863-1333
E-Mail: it-support@uni-bamberg.de

Informationssicherheit geht uns alle an!

Der Schutz von Informationen hat an der Universität Bamberg eine wichtige Bedeutung, da deren Missbrauch zu großen materiellen und immateriellen Schäden führen kann. Deshalb führt die Universität Bamberg ein Information Security Management System (ISMS, engl. für „Managementsystem für Informationssicherheit“) ein. Die in diesem ISMS aufgestellten Verfahren und Regeln helfen, Informationssicherheit zu steuern, zu kontrollieren und aufrechtzuerhalten sowie zu verbessern.

Eine Aufgabe des ISMS ist auch die Sensibilisierung der Anwenderinnen und Anwender für das Thema „Informationssicherheit“. Dieses Faltblatt soll Ihre Aufmerksamkeit für einem umsichtigen Umgang mit Daten, Datenträgern, Kennwörtern etc. gewinnen.

Weiterführende Informationen im Internet

– Fileserver: *www.uni-bamberg.de/rz/fileserver*

– TeamDrive: *www.uni-bamberg.de/rz/teamdrive*

– Kennwort: *www.uni-bamberg.de/rz/kennwort*

– SPAM und Phishing: *www.uni-bamberg.de/rz/spam*

Otto-Friedrich-Universität Bamberg
Rechenzentrum
Feldkirchenstraße 21 • 96052 Bamberg
Tel. +49 951 863-1333
it-support@uni-bamberg.de • www.uni-bamberg.de/rz

V. 01/02/19 | Fotos: colourbox.de