
Präambel:

Die RBO vom 04.10.2016 unterscheidet sich von der "alten" RBO vom 07.02.2008 lediglich durch redaktionelle Anpassungen an die neue Fakultäts-struktur der Universität.
Das bedeutet insbesondere, dass die gegenüber der alten RBO eingegangenen Verpflichtungen uneingeschränkt weitergelten.

Universität des Saarlandes

Fakultät Mathematik und Informatik (MI)

Rechnerbenutzungsordnung (RBO)

[Stand: 04.10.2016]

Weitere Informationen:

---

1. Geltungsbereich der Benutzungsordnung

Die Rechnerbenutzungsordnung (RBO) regelt die Benutzung der Kommunikations- und Datenverarbeitungsinfrastruktur (DV-Ressourcen) der Fakultät MI (FakMI) durch studentische und andere Benutzer. Die RBO soll eine möglichst sichere, störungsfreie und ungehinderte Nutzung der Kommunikations- und Datenverarbeitungsinfrastruktur der FakMI ermöglichen. Die RBO regelt das Nutzungsverhältnis zwischen den einzelnen Benutzern untereinander und zur FakMI und stellt die Grundregeln für den ordnungsgemäßen Betrieb der Kommunikations- und Datenverarbeitungsinfrastruktur auf.

2. Zweckbestimmung der Anlagen

Die Kommunikations- und Datenverarbeitungsinfrastruktur der FakMI soll im Rahmen der Aufgaben der Universität in Forschung, Lehre und Studium genutzt werden.

Die Zweckbestimmung umfasst insbesondere alle Übungen und Praktika zu Lehrveranstaltungen, freies Üben zur Vertiefung, alle Arbeiten im Auftrage des Fachbereichs sowie die Benutzung der Kommunikationseinrichtungen im jeweils zugelassenen Rahmen.
Die einzelnen Verwendungszwecke können vom Betreiber mit Prioritäten und Beschränkungen versehen werden.
Die Nutzung für private und kommerzielle Zwecke ist ausgeschlossen.

3. Zulassung der studentischen Benutzer

Die Zulassung zur Rechnerbenutzung wird zu festgelegten Zeiten bei den durch Aushang bekanntgemachten Stellen beantragt. Der Antrag wird bei Studenten mit Hauptfach Informatik oder Mathematik durch Abgabe eines Formblattes und bei Nebenfachstudenten durch Eintrag in die Teilnehmerliste einer im FakMI abgehaltenen Lehrveranstaltung gestellt. Die Zulassung erfolgt durch Vergabe eines Benutzerkennzeichens unter Berücksichtigung der vorhandenen Kapazitäten. Sie kann mit einer Begrenzung von Betriebsmitteln und Diensten und weiteren Auflagen im Rahmen der Zweckbestimmung der Anlagen nach Ziffer 1 versehen werden. Die Zulassung setzt die schriftliche Anerkennung der RBO voraus.
Andere Personen und Einrichtungen können zu wissenschaftlichen Zwecken oder zur Erfüllung der Aufgaben der Hochschulen des Landes zur Nutzung oder zum Angebot von Diensten zugelassen werden, sofern hierdurch die Belange der in Abs.1 genannten Benutzer nicht beeinträchtigt werden.
Über die Zulassung bzw. Versagung der Zulassung entscheiden die Beauftragten der Fachrichtungen für den Rechnerbetrieb (BfR).

4. Pflichten der Benutzer

Der Benutzer verpflichtet sich,
a) die bereitgestellten Betriebsmittel sorgfältig, wirtschaftlich und der Zweckbestimmung entsprechend zu benutzen;
b) das Passwort des ihm zugeteilten Benutzerkennzeichens geheim zu halten und ihm bekannt gewordene Informationen über andere Benutzerkennzeichen nicht weiterzugeben und auch nicht selbst zu benutzen;
c) Maßnahmen zum Schutz vor unbefugter Benutzung seines Kennzeichens zu ergreifen. Der Anlagenbetreiber stellt den Benutzern Informationen über solche Maßnahmen zur Verfügung;
d) alles zu unterlassen, was den ordnungsgemäßen Ablauf der Anlage stört;
e) in den Arbeitsräumen sich so zu verhalten, dass andere Benutzer nicht gestört werden;
f) Störungen, Beschädigungen, Fehler und Sicherheitsmängel an den Anlagen, Geräten, Datenträgern und Programmen unverzüglich dem jeweiligen BfR zu melden und diese nicht auszunutzen;
g) in den Räumen des Anlagenbetreibers sowie bei Inanspruchnahme seiner Geräte, Datenträger und sonstigen Einrichtungen den Weisungen des Personals des Anlagenbetreibers Folge zu leisten;
h) die Rechte und die Person anderer Benutzer zu respektieren;
i) keine falschen Identitäten vorzutäuschen;
j) seine Identität bekannt zu geben, wenn Dienste diese anfordern;
k) dem jeweiligen BfR in begründeten Fällen auf Verlangen Auskünfte über Programme und benutzte Methoden zu Kontrollzwecken zu erteilen sowie Einsicht zu gewähren;
l) lizensierte Software nur nach Absprache mit dem jeweiligen BfR einzuspielen und zu verwenden;
m) von der FakMI oder der Universität des Saarlandes bereitgestellte Software, Dokumentationen oder Daten weder zu kopieren noch an Dritte weiterzugeben, sofern dies nicht ausdrücklich erlaubt

ist, noch zu anderen als den erlaubten Zwecken zu verwenden,
n) personenbezogene Daten nicht ohne gesetzliche Grundlage oder Einwilligung der Betroffenen zu speichern und dabei die gesetzlichen Vorschriften und sonstigen einschlägigen Vorschriften einzuhalten;
o) fremde Benutzerkennungen weder zu ermitteln noch zu nutzen
p) keinen unberechtigten Zugriff auf Informationen anderer Benutzer zu nehmen und bekannt gewordene Informationen anderer Benutzer nicht ohne Genehmigung weiterzugeben, selbst zu nutzen oder zu verändern.
Auf die einschlägige Gesetzgebung wird verwiesen (insbesondere betreffend: Urheberrechtsverletzungen (§§ 106ff. UrhG), Ausspähen von Daten (§ 202a StGB), Datenveränderung (§303a StGB), Computersabotage (§ 303b StGB), Computerbetrug (§ 263a StGB), Beleidigung und Verleumdung (§§ 185ff, StGB), Verbreitung pornographischer Schriften und Verbreitung pornographischer Darbietungen durch den Rundfunk, Medien- und Teledienste (§§ 184b, 184c StGB)).
(s.a. Anlage 1)
q) Ergänzend wird auf die Regelungen zur Benutzung von Rechenanlagen (Anlage 2) verwiesen, welche die hier dargestellten Pflichten ergänzen und konkretisieren.

5. Rechte der Benutzer

Der Benutzer hat das Recht,
a) die ihm von der FakMI zur Verfügung gestellten Betriebsmittel (Rechenzeit, Speicher, Geräte, Netze, Räume und Programme) im Rahmen der RBO zu nutzen;
b) auf Beratung und Betreuung durch den jeweiligen BfR im möglichen Rahmen;
c) sich mit Anregungen und Vorschlägen an die jeweiligen BfR zu wenden;
d) auf Beseitigung von auftretenden Störungen durch den jeweiligen BfR im möglichen Rahmen.

6. Spezielle Dienste

Für spezielle Dienste kann der Anlagenbetreiber ergänzende Regelungen treffen.

7. Verfahren bei Verstößen

Benutzer können vorübergehend oder dauerhaft in der Benutzung der DV-Ressourcen beschränkt oder ausgeschlossen werden, wenn sie

1. schuldhaft gegen die RBO insbesondere gegen die unter Nr. 5 aufgeführten Pflichten verstoßen (missbräuchliches Verhalten) oder
2. die Kommunikations- und Datenverarbeitungsinfrastruktur für strafbare Handlungen missbrauchen oder
3. der Fakultät MI oder der Universität des Saarlandes durch rechtswidriges Benutzerverhalten Nachteile entstehen.

Die Maßnahmen nach Abs. a) sollen erst nach vorheriger erfolgloser Abmahnung erfolgen. Den Betroffenen ist die Möglichkeit zur Stellungnahme zu geben. Die Entscheidung über den Ausschluss trifft der jeweilige BfR.

8. Widerspruch

Über Widersprüche gegen Entscheidungen des jeweiligen BfR nach Ziffern 3 und 7 entscheidet der Fakultätsrat.

9. Rechte und Pflichten der Fakultät MI

a) Die FakMI führt über die erteilten Benutzungsberechtigungen eine Nutzerdatei, in der die Benutzer- und Mailkennungen sowie der Name und die Matrikelnummer der zugelassenen Nutzer aufgeführt werden.
b) Soweit dies zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit sowie zum Schutz der Nutzerdaten erforderlich ist, kann die FakMI die Nutzung seiner Ressourcen vorübergehend einschränken oder einzelne Benutzerkennungen vorübergehend sperren. Sofern möglich, sind die betroffenen Benutzer hierüber im Voraus zu unterrichten.
Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass ein Nutzer auf den Servern der FakMI rechtswidrige Inhalte zur Nutzung bereithält, kann die FakMI die weitere Nutzung verhindern, bis die Rechtslage hinreichend geklärt ist.
c) Die FakMI ist nach Maßgabe der nachfolgenden Regelungen berechtigt, die Inanspruchnahme der Datenverarbeitungssysteme durch die einzelnen Nutzer zu dokumentieren und auszuwerten, jedoch nur soweit dies erforderlich ist

1. zur Gewährleistung eines ordnungsgemäßen Systembetriebs,
2. zur Ressourcenplanung und Systemadministration,
3. zum Schutz der personenbezogenen Daten anderer Nutzer,
4. zu Abrechnungszwecken,
5. für das Erkennen und Beseitigen von Störungen sowie
6. zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung.

Unter den Voraussetzungen von Absatz c) ist die FakMI auch berechtigt, unter Beachtung des Datengeheimnisses Einsicht in die Benutzerdateien zu nehmen, soweit dies erforderlich ist zur Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Missbräuchen, sofern hierfür tatsächliche Anhaltspunkte vorliegen.
Eine Einsichtnahme in die Nachrichten- und E-Mail-Postfächer ist jedoch nur zulässig, soweit dies zur Behebung aktueller Störungen im Nachrichtendienst unerlässlich ist. In jedem Fall ist die Einsichtnahme zu dokumentieren, und der betroffene Benutzer ist nach Zweckerreichung unverzüglich zu benachrichtigen.
Nach Maßgabe der gesetzlichen Bestimmungen ist die FakMI zur Wahrung des Telekommunikations- und Datengeheimnisses verpflichtet.

10. Haftung des Benutzers

a) Der Benutzer haftet für alle Nachteile, die der FakMI oder der Universität des Saarlandes durch missbräuchliche oder rechtswidrige Verwendung der DV-Ressourcen und der Nutzungsberechtigung oder dadurch entstehen, dass der Nutzer schuldhaft seinen Pflichten aus dieser Benutzungsordnung nicht nachkommt.
b) Der Benutzer haftet auch für Schäden, die im Rahmen der ihm zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn er diese Drittnutzung zu vertreten hat, insbesondere im Falle einer Weitergabe seiner Benutzerkennung an Dritte.
c) Der Nutzer hat die FakMI und die Universität des Saarlandes von allen Ansprüchen freizustellen, wenn Dritte die FakMI/Universität des Saarlandes wegen eines missbräuchlichen oder

rechtswidrigen Verhaltens des Benutzers auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen. Die FakMI/Universität des Saarlandes wird dem Benutzer den Streit verkünden, sofern Dritte gegen die FakMI/Universität des Saarlandes gerichtlich vorgehen.

11. Haftung der FakMI/Universität des Saarlandes

a) Die FakMI übernimmt keine Garantie dafür, dass das System fehlerfrei und jederzeit ohne Unterbrechung läuft. Eventuelle Datenverluste infolge technischer Störungen sowie die Kenntnisnahme vertraulicher Daten durch unberechtigte Zugriffe Dritter können nicht ausgeschlossen werden.
b) Die FakMI übernimmt keine Verantwortung für die Richtigkeit der zur Verfügung
gestellten Programme. Die Hochschule haftet auch nicht für den Inhalt, insbesondere für die Richtigkeit, Vollständigkeit und Aktualität der Informationen, zu denen sie lediglich den Zugang zur Nutzung vermittelt.
c) Im Übrigen haftet die FakMI nur bei Vorsatz und grober Fahrlässigkeit ihrer Mitarbeiter, es sei denn, dass eine schuldhafte Verletzung wesentlicher Kardinalpflichten vorliegt. In diesem Fall ist die Haftung der Hochschule auf typische, bei Begründung des Nutzungsverhältnisses vorhersehbare Schäden begrenzt, soweit nicht vorsätzliches oder grob fahrlässiges Handeln vorliegt..

12.Inkrafttreten

Die RBO tritt mit Eilentscheid des Dekans vom 04.10.2016 sofort in Kraft.

Anlage 1 zur Rechnerbenutzungsordnung der Fakultät MI

Universität des Saarlandes
Fakultät MI – Mathematik und Informatik

Wichtige Gesetzestexte

[Stand: 07.02.08]

Ziel

Dies ist eine Sammlung von Auszügen aus geltenden deutschen Gesetzestexten. Sie erhebt keinen Anspruch auf Richtigkeit und Vollständigkeit.

Strafgesetzbuch

§202a Ausspähen von Daten
(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder

1. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,
2. herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

§ 303a Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.
(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er

1. eine Tat nach §303a Abs.1 begeht oder
2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§185 Beleidigung

Die Beleidigung wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe und, wenn die Beleidigung mittels einer Tätigkeit begangen wird, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§186 Üble Nachrede

Wer in Beziehung auf einen anderen eine Tatsache behauptet oder verbreitet, welche denselben verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen geeignet ist, wird, wenn nicht diese Tatsache erweislich wahr ist, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe und, wenn die Tat öffentlich oder durch Verbreiten von Schriften begangen ist, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§187 Verleumdung

Wer wider besseres Wissen in Beziehung auf einen anderen eine unwahre Tatsache behauptet oder verbreitet, welche denselben verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen oder dessen Kredit zu gefährden geeignet ist, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe und, wenn die Tat öffentlich, in einer Versammlung oder durch Verbreiten von Schriften begangen ist, mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

§263a Computerbetrug
(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Saarländisches Datenschutzgesetz

§ 4 Zulässigkeit der Datenverarbeitung; Datenvermeidung und Datensparsamkeit
(1) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn
a) dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder
b) der Betroffene eingewilligt hat.
Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist der Betroffene auf die Einwilligungserklärung schriftlich besonders hinzuweisen. Der Betroffene ist in geeigneter Weise über die Bedeutung der Ein-willigung, insbesondere über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung an Dritte über diese aufzuklären; er ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann.
(2) .....

§ 6 Datengeheimnis
Denjenigen Personen, die bei öffentlichen Stellen oder ihren Auftragnehmern dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, solche Daten unbefugt zu verarbeiten; dies gilt auch nach Beendigung ihrer Tätigkeit. Diese Personen sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten.

§ 19 Unabdingbarkeit der Rechte des Betroffenen
Die in den §§ 20 bis 24 aufgeführten Rechte können durch Rechtsgeschäft weder ausgeschlossen noch beschränkt werden.

§ 20 Auskunft
(1) Dem Betroffenen ist von der verantwortlichen Stelle auf Antrag unentgeltlich Auskunft zu erteilen über
1. die zu seiner Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung sowie
3. die Herkunft der Daten und die Empfänger von Übermittlungen, soweit dies gespeichert ist.
Dies gilt nicht für Daten, die gesperrt sind, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.
(2) In dem Antrag soll die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung nach pflichtgemäßem Ermessen; sind die Daten in Akten gespeichert, ist dem Betroffenen auf Verlangen Einsicht zu gewähren. Auskunft aus Akten oder Akteneinsicht ist zu gewähren, soweit der Betroffene Angaben macht, die das Auffinden der Daten mit angemessenem Aufwand ermöglichen, und soweit sich aus § 29 Saarländisches Verwaltungsverfahrensgesetz nichts anderes ergibt.

(3) Die Verpflichtung zur Auskunftserteilung oder zur Gewährung der Akteneinsicht entfällt, soweit
a) dies die ordnungsgemäße Erfüllung der Aufgaben der verantwortlichen Stelle gefährden würde,
b) dies die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder
c) die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der berechtigten Interessen eines Dritten, geheim gehalten werden müssen.
(4) Einer Begründung für die Verweigerung der Auskunft oder Akteneinsicht bedarf es nur dann nicht, wenn durch die Mitteilung der Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall sind die wesentlichen Gründe für die Entscheidung aufzuzeichnen. Der Betroffene ist in jedem Fall darauf hinzuweisen, dass er sich an den Landesbeauftragten für Datenschutz wenden kann.
(5) Bezieht sich die Auskunftserteilung oder die Akteneinsicht auf die Herkunft personenbezogener Daten von Behörden des Verfassungsschutzes, der Staatsanwaltschaft und der Polizei, von Finanzbehörden, soweit diese personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, sowie von den in § 19 Abs. 3 Bundesdatenschutzgesetz genannten Behörden, ist sie nur mit Zustimmung dieser Stellen zulässig. Gleiches gilt für die Übermittlung personenbezogener Daten an diese Behörden. Für die Versagung der Zustimmung gelten, soweit dieses Gesetz auf die genannten Behörden Anwendung findet, die Absätze 3 und 4 entsprechend.

§ 21 Berichtigung, Sperrung und Löschung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Sind personenbezogene Daten, die nicht automatisiert verarbeitet werden, zu berichtigen, so ist in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt und aus welchem Grund diese Daten unrichtig waren oder geworden sind.
(2) Personenbezogene Daten sind zu sperren, wenn
a) ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt,
b) eine Löschung nach Absatz 3 Satz 2 nicht in Betracht kommt und der Betroffene die Sperrung beantragt,
c) der Betroffene an Stelle der Löschung nach Absatz 3 Satz 1 Buchstabe a die Sperrung beantragt,
d) wenn Grund zu der Annahme besteht, dass durch die Löschung der Daten berechtigte Interessen des Betroffenen beeinträchtigt werden,
e) sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind oder
f) sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen.

In den Fällen nach Satz 1 Buchstabe d sind die Gründe aufzuzeichnen. Bei automatisierten Verfahren ist die Sperrung grundsätzlich durch technische Maßnahmen sicherzustellen; im Übrigen ist ein entsprechender Vermerk anzubringen. Gesperrte Daten dürfen über die Speicherung hinaus nicht mehr weiterverarbeitet werden, es sei denn, dass dies zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist oder der Betroffene eingewilligt hat.
(3) Personenbezogene Daten sind zu löschen, wenn
a) ihre Speicherung unzulässig ist oder
b) ihre Kenntnis für die verantwortliche Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

Sind personenbezogene Daten in Akten gespeichert, ist die Löschung nach Satz 1 Buchstabe b nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist; soweit

hiernach eine Löschung nicht in Betracht kommt, sind die Daten auf Antrag des Betroffenen zu sperren.
(4) Abgesehen von den Fällen des Absatzes 3 Satz 1 Buchstabe a ist von einer Löschung abzusehen, soweit die gespeicherten Daten aufgrund von Rechtsvorschriften einem Archiv zur Übernahme anzubieten oder von einem Archiv zu übernehmen sind.
(5) Über die Berichtigung unrichtiger Daten, die Sperrung bestrittener Daten und die Löschung oder Sperrung unzulässig gespeicherter Daten sind unverzüglich die Stellen zu unterrichten, denen die Daten übermittelt worden sind. Die Unterrichtung kann unterbleiben, wenn sie einen erheblichen Aufwand erfordern würde und nachteilige Folgen für den Betroffenen nicht zu befürchten sind.

§ 22 Einwendungsrecht des Betroffenen
Betroffene können gegenüber der verantwortlichen Stelle auch gegen eine durch Rechtsvorschrift erlaubte Verarbeitung ihrer personenbezogenen Daten unter Hinweis auf ein schutzwürdiges besonderes persönliches Interesse im Einzelfall schriftlich Einwände vorbringen. In diesen Fällen bleibt die Verarbeitung nur dann zulässig, wenn eine Prüfung ergibt, dass das öffentliche Interesse an der Verarbeitung überwiegt. Betroffene sind über das Ergebnis der Prüfung schriftlich zu unterrichten. Wird dem Einwand nicht entsprochen, ist der Betroffene darauf hinzuweisen, dass er sich an den Landesbeauftragten für Datenschutz wenden kann. Das Einwendungsrecht besteht nicht, wenn eine Rechtsvorschrift zur Verarbeitung verpflichtet.

§ 23 Anrufungsrecht des Betroffenen
(1) Jedermann hat das Recht, sich unmittelbar an den Landesbeauftragten für Datenschutz zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine der Kontrolle des Landesbeauftragten unterliegende Stelle in seinen Rechten verletzt zu sein; dies gilt auch für Bedienstete der öffentlichen Stellen.
(2) Niemand darf deswegen benachteiligt oder gemaßregelt werden, weil er sich an den Landesbeauftragten für Datenschutz wendet.

§ 24 Schadensersatz
(1) Wird dem Betroffenen durch eine nach den Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung seiner personenbezogenen Daten ein Schaden zugefügt, so ist ihm die verantwortliche Stelle un-abhängig von einem Verschulden zum Schadensersatz verpflichtet. In schweren Fällen kann der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen. Der Ersatzpflichtige haftet jedem Betroffenen nach den Sätzen 1 und 2 für jedes schädigende Ereignis bis zu einem Betrag von 125.000 Euro.
(2) Soweit die unzulässige oder unrichtige Verarbeitung personenbezogener Daten nicht automatisiert erfolgt, haftet die verantwortliche Stelle nur bei Verschulden. Die verantwortliche Stelle haftet nicht, wenn sie nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihr nicht zur Last gelegt werden kann.
(3) Auf das Mitverschulden des Betroffenen und auf die Verjährung des Entschädigungsanspruchs sind die §§ 254, 839 Abs. 3 und 852 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden.
(4) Weitergehende sonstige Schadensersatzansprüche bleiben unberührt.

Straf- und Bußgeldvorschriften; Übergangsvorschriften

§ 35 Straftaten
(1) Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind, gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen

zu schädigen,

1. erhebt, speichert, verändert, weitergibt, zur Einsichtnahme oder zum Abruf bereithält, löscht oder nutzt,
2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlasst,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.
(2) Absatz 1 findet nur Anwendung, soweit die Tat nicht nach anderen Vorschriften mit Strafe bedroht ist.

§ 36 Ordnungswidrigkeiten
(1) Ordnungswidrig handelt, wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, verändert, weitergibt, zur Einsichtnahme oder zum Abruf bereithält, löscht oder nutzt,
2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlasst.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50.000 Euro geahndet werden.

Urheberrechtsgesetz

§15 Allgemeines
(1) Der Urheber hat das ausschließliche Recht, sein Werk in körperlicher Form zu verwerten; das Recht umfasst insbesondere
1. das Vervielfältigungsrecht,
2. das Verbreitungsrecht,
3. das Ausstellungsrecht.

§16 Vervielfältigungsrecht
(1) Das Vervielfältigungsrecht ist das Recht, Vervielfältigungsstücke des Werkes herzustellen, gleichviel in welchem Verfahren und in welcher Zahl.

§17 Verbreitungsrecht
(1) Das Verbreitungsrecht ist das Recht, das Original oder Vervielfältigungsstücke des Werkes der Öffentlichkeit anzubieten oder in Verkehr zu bringen.
(2) Sind das Original oder Vervielfältigungsstücke des Werkes mit Zustimmung des zur Verbreitung im Geltungsbereich dieses Gesetzes Berechtigten im Wege der Veräußerung in Verkehr gebracht worden, so ist ihre Weiterverbreitung zulässig.

§23 Bearbeitungen und Umgestaltungen
Bearbeitungen oder andere Umgestaltungen des Werkes dürfen nur mit Einwilligung des Urhebers des bearbeiteten oder umgestalteten Werkes veröffentlicht oder verwertet werden.

§24 Freie Benutzung

1. Ein selbständiges Werk, das in freier Benutzung des Werkes eines anderen geschaffen worden ist, darf ohne Zustimmung des Urhebers des benutzten Werkes veröffentlicht und verwertet werden.
2. .....

§ 53 Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch
(1) Zulässig sind einzelne Vervielfältigungen eines Werkes durch eine natürliche

Person zum privaten Gebrauch auf beliebigen Trägern, sofern sie weder unmittelbar noch mittelbar Erwerbszwecken dienen, soweit nicht zur Vervielfältigung eine offensichtlich rechtswidrig hergestellte oder öffentlich zugänglich gemachte Vorlage verwendet wird. Der zur Vervielfältigung Befugte darf die Vervielfältigungsstücke auch durch einen anderen herstellen lassen, sofern dies unentgeltlich geschieht oder es sich um Vervielfältigungen auf Papier oder einem ähnlichen Träger mittels beliebiger photomechanischer Verfahren oder anderer Verfahren mit ähnlicher Wirkung handelt.

(2) Zulässig ist, einzelne Vervielfältigungsstücke eines Werkes herzustellen oder herstellen zu lassen

1. zum eigenen wissenschaftlichen Gebrauch, wenn und soweit die Vervielfältigung zu diesem Zweck geboten ist und sie keinen gewerblichen Zwecken dient,
2. zur Aufnahme in ein eigenes Archiv, wenn und soweit die Vervielfältigung zu diesem Zweck geboten ist und als Vorlage für die Vervielfältigung ein eigenes Werkstück benutzt wird,
3. zur eigenen Unterrichtung über Tagesfragen, wenn es sich um ein durch Funk gesendetes Werk handelt,
4. zum sonstigen eigenen Gebrauch,
    a) wenn es sich um kleine Teile eines erschienenen Werkes oder um einzelne Beiträge handelt, die in Zeitungen oder Zeitschriften erschienen sind,
    b) wenn es sich um ein seit mindestens zwei Jahren vergriffenes Werk handelt.

    Dies gilt im Fall des Satzes 1 Nr. 2 nur, wenn zusätzlich

    1. die Vervielfältigung auf Papier oder einem ähnlichen Träger mittels beliebiger photomechanischer Verfahren oder anderer Verfahren mit ähnlicher Wirkung vorgenommen wird oder
    2. eine ausschließlich analoge Nutzung stattfindet oder
    3. das Archiv im öffentlichen Interesse tätig ist und keinen unmittelbar oder mittelbar wirtschaftlichen oder Erwerbszweck verfolgt.

Dies gilt in den Fällen des Satzes 1 Nr. 3 und 4 nur, wenn zusätzlich eine der Voraussetzungen des Satzes 2 Nr. 1 oder 2 vorliegt.

(3) Zulässig ist, Vervielfältigungsstücke von kleinen Teilen eines Werkes, von Werken von geringem Umfang oder von einzelnen Beiträgen, die in Zeitungen oder Zeitschriften erschienen oder öffentlich zugänglich gemacht worden sind, zum eigenen Gebrauch

1. zur Veranschaulichung des Unterrichts in Schulen, in nichtgewerblichen Einrichtungen der Aus- und Weiterbildung sowie in Einrichtungen der Berufsbildung in der für die Unterrichtsteilnehmer erforderlichen Anzahl oder
2. für staatliche Prüfungen und Prüfungen in Schulen, Hochschulen, in nichtgewerblichen Einrichtungen der Aus- und Weiterbildung sowie in der Berufsbildung in der erforderlichen Anzahl herzustellen oder herstellen zu lassen, wenn und soweit die Vervielfältigung zu diesem Zweck geboten ist. Die Vervielfältigung eines Werkes, das für den Unterrichtsgebrauch an Schulen bestimmt ist, ist stets nur mit Einwilligung des Berechtigten zulässig.

(4) Die Vervielfältigung

    a) graphischer Aufzeichnungen von Werken der Musik,
    b) eines Buches oder einer Zeitschrift,

wenn es sich um eine im wesentlichen vollständige Vervielfältigung handelt, ist, soweit sie nicht durch Abschreiben vorgenommen wird, stets nur mit Einwilligung des Berechtigten zulässig oder unter den Voraussetzungen des Absatzes 2 Satz 1 Nr. 2 oder zum eigenen Gebrauch, wenn es sich um ein seit mindestens zwei Jahren vergriffenes Werk handelt.

(5) Absatz 1, Absatz 2 Satz 1 Nr. 2 bis 4 sowie Absatz 3 Nr. 2 finden keine Anwendung auf Datenbankwerke, deren Elemente einzeln mit Hilfe elektronischer Mittel zugänglich sind. Absatz 2

Satz 1 Nr. 1 sowie Absatz 3 Nr. 1 finden auf solche Datenbankwerke mit der Maßgabe Anwendung, dass der wissenschaftliche Gebrauch sowie der Gebrauch im Unterricht nicht zu gewerblichen Zwecken erfolgen.
(6) Die Vervielfältigungsstücke dürfen weder verbreitet noch zu öffentlichen Wiedergaben benutzt werden. Zulässig ist jedoch, rechtmäßig hergestellte Vervielfältigungsstücke von Zeitungen und vergriffenen Werken sowie solche Werkstücke zu verleihen, bei denen kleine beschädigte oder abhanden gekommene Teile durch Vervielfältigungsstücke ersetzt worden sind.
(7) Die Aufnahme öffentlicher Vorträge, Aufführungen oder Vorführungen eines Werkes auf Bild- oder Tonträger, die Ausführung von Plänen und Entwürfen zu Werken der bildenden Künste und der Nachbau eines Werkes der Baukunst sind stets nur mit Einwilligung des Berechtigten zulässig.

§106 Unerlaubte Verwertung urheberrechtlich geschützter Werke
(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder eine Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.

Besondere Bestimmungen für Computerprogramme

§69a Gegenstand des Schutzes

(1) Computerprogramme im Sinne dieses Gesetzes sind Programme in jeder Gestalt, einschließlich des Entwurfsmaterials.
(2) Der gewährte Schutz gilt für alle Ausdrucksformen eines Computerprogrammes. Ideen und Grundsätze, die einem Element eines Computerprogrammes zugrundeliegen, einschließlich der den Schnittstellen zugrundeliegenden Ideen und Grundsätze, sind nicht geschützt.
(3) Computerprogramme werden geschützt, wenn sie individuelle Werke in dem Sinne darstellen, daß sie das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers sind.
Zur Bestimmung ihrer Schutzfähigkeit sind keine anderen Kriterien, insbesondere nicht qualitative oder ästhetische, anzuwenden.
(4) Auf Computerprogramme finden die für Sprachwerke geltenden Bestimmungen Anwendung, soweit in diesem Abschnitt nichts anderes bestimmt ist.

§69b Urheber in Arbeits- und Dienstverhältnissen
(1) Wird ein Computerprogramm von einem Arbeitnehmer in Wahrnehmung seiner Aufgaben oder nach den Anweisungen seines Arbeitgebers geschaffen, so ist ausschließlich der Arbeitgeber zur Ausübung aller vermögensrechtlichen Befugnisse an dem Computerprogramm berechtigt, sofern nichts anderes vereinbart ist.
(2) Absatz 1 ist auf Dienstverhältnisse entsprechend anzuwenden.

§69c Zustimmungsbedürftige Handlungen
Der Rechtsinhaber hat das ausschließliche Recht, folgende Handlungen vorzunehmen oder zu gestalten:
1. die dauerhafte oder vorübergehende Vervielfältigung, ganz oder teilweise, eines Computerprogramms mit jedem Mittel und in jeder Form. Soweit das Laden, Anzeigen, Ablaufen, Übertragen oder Speichern des Computerprogramms eine Vervielfältigung erfordert, bedürfen diese Handlungen der Zustimmung des Rechtsinhabers;
2. die Übersetzung, die Bearbeitung, das Arrangement und andere Umarbeitungen eines Computerprogramms sowie die Vervielfältigung der erzielten Ergebnisse. Die Rechte derjenigen, die

das Programm bearbeiten, bleiben unberührt;
3. jede Form der Verbreitung des Originals eines Computerprogramms oder von Vervielfältigungsstücken, einschließlich der Vermietung. Wird ein Vervielfältigungsstück eines Computerprogramms mit Zustimmung des Rechtsinhabers im Gebiet der Europäischen Gemeinschaften oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum im Wege der Veräußerung in Verkehr gebracht, so erschöpft sich das Verbreitungsrecht in bezug auf dieses Vervielfältigungsstück mit Ausnahme des Vermietrechts.

§69d Ausnahmen von den zustimmungsbedürftigen Handlungen
(1) Soweit keine besonderen vertraglichen Bestimmungen vorliegen, bedürfen die in §69c Nr. 1 und 2 genannten Handlungen nicht der Zustimmung des Rechtsinhabers, wenn sie für eine bestimmungsgemäße Benutzung des Computerprogramms einschließlich der Fehlerberichtigung durch jeden zur Verwendung eines Vervielfältigungsstückes des Programms Berechtigten notwendig sind.
(2) Die Erstellung einer Sicherungskopie durch eine Person, die zur Benutzung des Programms berechtigt ist, darf nicht vertraglich untersagt werden, wenn sie für die Sicherung künftiger Benutzung erforderlich ist.
(3) Der zur Verwendung eines Vervielfältigungsstücks eines Programms Berechtigte kann ohne Zustimmung des Rechtsinhabers das Funktionieren dieses Programms beobachten, untersuchen oder testen, um die einem Programmelement zugrundeliegenden Ideen und Grundsätze zu ermitteln, wenn dies durch Handlungen zum Laden, Anzeigen, Ablaufen, Übertragen oder Speichern des Programms geschieht, zu denen er berechtigt ist.

§69e Dekompilierung
(1) Die Zustimmung des Rechtsinhabers ist nicht erforderlich, wenn die Vervielfältigung des Codes oder die Übersetzung der Codeform im Sinne des §69c Nr. 1 und 2 unerlässlich ist, um die erforderlichen Informationen zur Herstellung der Interoperabilität eines unabhängig geschaffenen Computerprogramms mit anderen Programmen zu erhalten, sofern folgende Bedingungen erfüllt sind:
1. Die Handlungen werden von dem Lizenznehmer oder von einer anderen zur Verwendung eines Vervielfältigungsstücks des Programms berechtigten Person oder in deren Namen von einer hierzu ermächtigten Person vorgenommen;
2. die für die Herstellung der Interoperabilität notwendigen Informationen sind für die in Nr. 1 genannten Personen noch nicht ohne weiteres zugänglich gemacht;
3. die Handlungen beschränken sich auf die Teile des ursprünglichen Programms, die zur Herstellung der Interoperabilität notwendig sind.
(2) Bei Handlungen nach Absatz 1 gewonnene Informationen dürfen nicht
1. zu anderen Zwecken als zur Herstellung der Interoperabilität des unabhängig geschaffenen Programms verwendet werden,
2. an Dritte weitergegeben werden, es sei denn, dass dies für die Interoperabilität des unabhängig geschaffenen Programms notwendig ist,
3. für die Entwicklung, Herstellung oder Vermarktung eines Programms mit im wesentlichen ähnlicher Ausdrucksform oder für irgendwelche anderen das Urheberrecht verletzenden Handlungen verwendet werden.
(3) Die Absätze 1 und 2 sind so auszulegen, daß ihre Anwendung weder die normale Auswertung des Werkes beeinträchtigt noch die berechtigten Interessen des Rechtsinhabers unzumutbar verletzt.

§69f Rechtsverletzungen
(1) Der Rechtsinhaber kann von dem Eigentümer oder Besitzer verlangen, dass alle rechtswidrig hergestellten, verbreiteten oder zur rechtswidrigen Verbreitung bestimmten Vervielfältigungsstücke vernichtet werden. [...]
(2) Absatz 1 ist entsprechend auf Mittel anzuwenden, die allein dazu bestimmt sind, die unerlaubte Beseitigung oder Umgehung technischer Programmschutzmechanismen zu erleichtern.

§69g Anwendung sonstiger Rechtsvorschriften; Vertragsrecht

(1) [...]
(2) Vertragliche Bestimmungen, die in Widerspruch zu §69d Absatz 2 und 3 und §69e stehen, sind nichtig.

Anlage 2 zur Rechnerbenutzungsordnung der Fakultät MI

Universität des Saarlandes
Fakultät MI – Mathematik und Informatik

Regeln zur Benutzung der Rechenanlagen

[Stand: 12.06.13]

Zum Selbstverständnis dieser Regeln

Der vorliegende Katalog stellt eine nicht abgeschlossene Sammlung von Regeln für die Benutzung der Rechner und Netze in der Fachrichtung Informatik dar. Diese Regeln ergänzen die RBO und geben Hinweise zur Benutzung.

A) Achtung von Zugangs- / Zugriffsrechten

1. Versuchen Sie nicht, ohne Autorisierung Zugang zu anderen Kennzeichen, insbesondere zu `root', zu erlangen.
2. Versuchen Sie nicht, Passwörter anderer Kennzeichen zu brechen.
3. Entdeckte Sicherheitsmängel sind dem Anlagenbetreiber mitzuteilen. Sie dürfen nicht ausgenutzt werden.
4. Versuchen Sie nicht, elektronische Post oder ausdrücklich geschützte Daten anderer Benutzer ohne deren Einwilligung zu lesen oder zu kopieren.
5. Mit Copyright geschützte Software darf nur in Übereinstimmung mit der Lizenz verwendet werden.

B) Verantwortung der Benutzer

1. Der Benutzer ist verantwortlich für sämtliche Handlungen unter seinem Kennzeichen.
2. Der Benutzer ist für die Wahl eines sicheren Passwortes und für den Schutz seiner Daten verantwortlich. (d.h.: als Passwörter keine Namen, Wörter, die in Lexika vorkommen (deutsch oder englisch), Geburtstage, Konto-, Pass- oder ähnliche Nummern; verwenden Sie Groß- und Kleinschreibung).
3. Passwörter sind geheim zu halten.
4. Lassen Sie Ihre Workstation niemals unbeaufsichtigt.

C) Benutzung der Rechner

1. Stören Sie andere Benutzer nicht bei der Arbeit.
2. Unternehmen Sie keine unautorisierten Versuche der Modifikation von Geräten, Programmen oder Daten. Insbesondere dürfen Virus-Programme weder eingebracht noch angewendet werden.
3. Erstellen Sie keine nicht autorisierten Kopien von Programmen und Daten.
4. Die bereitgestellten Betriebsmittel sind nicht für kommerzielle oder parteipolitische Zwecke zu nutzen.
5. Versuche, nicht zugelassene Dienste zu benutzen, sind untersagt.
6. Ausdrücklich untersagt ist die Erzeugung von BitCoins.

D) Regeln zur Verwendung von News und Mail

1. Senden Sie keine Nachricht mit verletzendem, beleidigendem oder obszönem Inhalt.
2. Senden Sie keine Nachrichten mit kommerziellem Inhalt (z.B. Werbung für Firmen); erlaubt sind private `Kleinanzeigen'.
3. Der Absender von Nachrichten muß sich einwandfrei identifizieren. Insbesondere sind Täuschungen über den wahren Absender untersagt.

E) Allgemeine Hinweise

1. Man verlässt seinen Arbeitsplatz so, wie man ihn vorgefunden hat.
2. In den Arbeitsräumen sind Gespräche mit gedämpfter Lautstärke geboten.
3. Die Rechte und die Person anderer Benutzer sind zu respektieren.
4. Essen, Trinken und Rauchen ist in den Arbeitsräumen ausdrücklich untersagt.

F) Sonstiges

1. In allen Zweifelsfällen ist der Anlagenbetreiber einzuschalten.

Anlage 3 zur Rechnerbenutzungsordnung der Fakultät MI

Universität des Saarlandes
Fakultät MI – Mathematik und Informatik

Verbote beim Umgang mit der Rechnerausstattung der Studentenrechnerpools der Fachrichtung Informatik (FRI).

[Stand: 16.02.2006 bzw. 04.10.2016]

Ausdrücklich verboten ist:

- Anschliessen von Hardware, die nicht zur Ausstattung der Rechnerräume gehört.*
- Abziehen und Einstöpseln von Steckern gleich welcher Art.*
- Manipulation an Geräten (auch das Öffnen).

- Ab-/Einschalten bzw. Rebooten der Geräte.**
- Die Betätigung der Notausschalter, ohne dass ein echter Notfall vorliegt.
- Demontage der Möblierung.
- Essen und Trinken in den Rechnerräumen.
- Unnötige Störungen und Belästigungen der übrigen in den Räumen anwesenden Personen.

* Ausnahme: Datenelektranten in der vordersten Bankreihe in Raum 012.
** Notfälle dem zuständigen Personal der FRI melden. Bei Anwesenheit der Aufsicht direkt dort melden, oder eine email mit kurzer Beschreibung des Zustandes der Maschine an operator@studcs.uni-saarland.de.

Anlage 4 zur Rechnerbenutzungsordnung der Fakultät MI

Universität des Saarlandes
Fakultät MI – Mathematik und Informatik

Hinweise zur Systemsicherheit

[Stand: 21.4.1995 bzw. 03.04.2000 bzw. 04.10.2016]

Die Systemsicherheit erfordert, dass jeder Account im System so gut wie möglich gegen unberechtigte Benutzung geschützt wird. Jeder Benutzer muss sich dabei für die Sicherheit seines Accounts verantwortlich fühlen. Denn ist erst einmal ein Einbruch in einen schlecht gesicherten Account gelungen, können nicht nur die Systemressourcen im Namen dieses Benutzers missbraucht werden, sondern es sind auch alle anderen Benutzer durch die neuen Möglichkeiten des Einbrechers bedroht. Diese Checkliste soll dem Benutzer Hinweise geben, mit welchen Massnahmen er zur Verbesserung der Systemsicherheit beitragen kann:

- erkannte Sicherheitsmängel dem Anlagenbetreiber melden und nicht ausnutzen
- Regeln für den Umgang mit Passworten beachten:
  - das Passwort soll 8 Zeichen lang sein
  - das Passwort soll kein Wort mit einer Bedeutung sein
  - das Passwort soll kein Wort aus einem Wörterbuch sein
  - das Passwort soll nicht aus persönlichen Daten hergeleitet sein
  - das Passwort soll nicht aus bekannten Abkürzungen gebildet werden
  - das Passwort soll Gross- und Kleinbuchstaben, Ziffern, Satzzeichen enthalten Beispiel: Wahl eines Satzes mit einer Bedeutung, den man sich merken kann. Der Reihe nach den ersten Buchstaben jedes Wortes und die Satzzeichen als Passwort nehmen.
  - das Passwort ist geheimzuhalten
  - das Passwort ist regelmässig zu ändern (ca. alle 3 Monate)
  - auf verschiedenen Sicherheitsclustern * sind unterschiedliche Passworte zu wählen
  - keine Passworte im Klartext im Rechner (in Scripts, etc.) ablegen
- die Nutzung des eigenen Accounts auch keinem "guten Freund" erlauben
- nach Sitzungsende abmelden (ausloggen)
- auch bei kurzzeitiger Abwesenheit möglichst das Terminal sperren oder den Raum abschliessen
- kein World-Write-Zugriff auf das Home directory und alle eigenen Files
- kein World-Zugriff auf Punkt-Files wie .login, .cshrc, .profile, usw.
- kein World-Exec-Zugriff auf eigene Programme (Risiko für den Aufrufer)
- World-Read-Zugriff auf eigene Files nur in Ausnahmefällen
- keine set-UID Programme mit World Exec-Zugriff

- keine set-UID oder set-GID Scripts
- umask auf Wert 077 setzen
- eigene Dateien mittels "ls -alc" von Zeit zu Zeit auf Plausibilität (Name, Eigentümer, Zugriffsschutz, Datum) überprüfen
- nur sichere Directories in die Definition des Kommandosuchpfades (CSH-Variable path, SH-Variable PATH, Environment-Variable PATH) aufnehmen
- Current-Directory (".") als letztes Directory in PATH bzw. path eintragen
- kein "+" im .rhosts-File
- kein Rechner und User aus anderem Sicherheitscluster im .rhosts-File
- kein Eintrag ohne Userangabe im .rhosts File
- keine "alten" Einträge (Hosts , User) im .rhosts-File
- in .netrc-File nur Einträge für Zugang zu anonymous FTP, keine Passworte
- Vorsicht bei der Ausführung von Programmen aus anderen User-Directories (unerwünschte Nebenwirkung, Trojanisches Pferd)
- kein Kommando "xhost +" oder "xhost +Rechnername" geben
- Passwort-Eingaben über xterm nur im Secure-Mode machen (Option Secure-Keyboard oder secureonpwd)
- ein Sicherheitscluster bilden z.B. die Aus bildungsrechner oder die Anlagen eines Lehrstuhls.