Benutzungsordnung für die Informationsverarbeitungs- und Kommunikations-Infrastruktur der Universität Kassel (IT-Benutzungsordnung)

Präambel

§ 1 Geltungsbereich

§ 2 Benutzerkreis

§ 3 Benutzungsberechtigungen

§ 4 Gesetzliche Einbindung

§ 5 Rechte und Pflichten der Benutzer

§ 6 Aufgaben, Rechte und Pflichten des Systembetreibers

§ 7 Haftung des Systembetreibers und Haftungsausschluss

§ 8 Folgen einer rechtswidrigen Benutzung

§ 9 Sonstige Regelungen

§ 10 Inkrafttreten

Präambel

Die Universität Kassel, ihre Fachbereiche und Zentralen Einrichtungen betreiben eine Informationsverarbeitungs- und Kommunikationsinfrastruktur (IuK-Infrastruktur). Die IT-Systeme, IT-Dienstleistungen und hochschulinternen Kommunikationsnetze dienen zur Unterstützung der gesetzlich gemäß § 3 Hessisches Hochschulgesetz (HHG) festgelegten Aufgaben der Universität Kassel.

Die IuK-Infrastruktur ist an das Internet angeschlossen.

Die IT-Benutzungsordnung regelt die Bedingungen unter denen das Leistungsspektrum dieser Infrastruktur genutzt werden kann. Sie unterstützen insbesondere folgende Ziele:

- Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit der an der Universität Kassel eingesetzten IT-Systeme und den darauf verarbeiteten und vorgehaltenen Daten,
- Sicherstellung eines reibungslosen Lehr-, Forschungs- und Verwaltungsbetriebs,
- Sicherstellung eines ordnungsgemäßen Betriebs der IuK-Infrastruktur,
- Schutz zu wahrender Rechte Dritter und zu schützender Daten (Urheberrecht, Softwarelizenzen, Auflagen der Netzbetreiber, Datenschutzaspekte),
- Verpflichtung der Benutzer zu rechtmäßigem Verhalten und zum ökonomischen Gebrauch der angebotenen Ressourcen,
- Verpflichtung der Systembetreiber zum korrekten Systembetrieb,
- Verhinderung von Verstößen gegen die IT-Benutzungsordnung.

§ 1 Geltungsbereich

Diese IT-Benutzungsordnung gilt für die von der Universität Kassel betriebene IuK-Infrastruktur, bestehend aus Informationsverarbeitungssystemen, Kommunikationssystemen, weiteren Hilfseinrichtungen , den angebotenen IT-Dienstleistungen sowie bei Nutzung auf nicht universitätseigenen Geräten für Zwecke gemäß § 2 Absatz 1.

§ 2 Benutzerkreis

(1) Die in § 1 genannten Ressourcen stehen den Mitgliedern und Angehörigen der Universität Kassel gemäß § 32 Hessisches Hochschulgesetz (HHG) zur Erfüllung ihrer Aufgaben aus Forschung, Studium, Lehre, Verwaltung, Aus- und Weiterbildung und Öffentlichkeitsarbeit zur Verfügung.

(2) Anderen Personen und Institutionen kann die Nutzung durch das IT-Servicezentrum gestattet werden, wenn dies im Interesse der Universität Kassel liegt.

Als andere Personen und Institutionen gelten insbesondere:

a) Mitglieder und Angehörige anderer Hochschulen des Landes Hessen oder staatlicher Hochschulen außerhalb des Landes Hessen aufgrund besonderer Vereinbarungen;

b) sonstige staatliche Forschungs- und Bildungseinrichtungen und Behörden des Landes Hessen aufgrund besonderer Vereinbarungen und die zugehörigen Personen;

c) Mitglieder und Angehörige kooperierender Hochschulen;

d) kooperierende externe Einrichtungen (z.B. Studentenwerk, AStA) und die zugehörigen Personen.

§ 3 Benutzungsberechtigungen

(1) Die Benutzung der IuK-Infrastruktur bedarf einer formalen Benutzungsberechtigung (zum Beispiel Benutzerkennung, Netzanschluss, Netzzugang) des zuständigen Systembetreibers.

(2) Ein Festnetzanschluss der Rechner an das Hochschulnetz kann nur von Bediensteten beantragt werden. Andere Mitglieder oder Angehörige der Universität Kassel können den Anschluss eines Rechners nur beantragen, wenn die Übernahme der Kosten durch Angabe einer universitären Kostenstelle und durch die Unterschrift des Kostenstellenverantwortlichen gewährleistet ist.

(3) Systembetreiber

a) für zentrale Systeme und Dienste gemäß Anlage 1 dieser Benutzungsordnung sind das IT-Servicezentrum, die Universitätsbibliothek und das Service Center Lehre.

b) für dezentrale Systeme die jeweilige Organisationseinheit der Universität Kassel, in der das System betrieben wird (z.B. Fachbereich).

(4) Der Antrag auf Benutzungsberechtigung muss in einer Form erfolgen, die eine sichere Authentifizierung ermöglicht (z.B. Schriftform, de-mail, digitale Signatur, elektronischer Personalausweis) und folgende Angaben enthalten:

- Systembetreiber, bei dem die Benutzungsberechtigung beantragt wird,
- Systeme, für welche die Benutzungsberechtigung beantragt wird,
- Antragsteller (Name, Adresse und Telefon-/Faxnummer oder E-Mail-Adresse des Antragstellers, Zuordnung zu einer Organisationseinheit der Universität, bei Studierenden Immatrikulationsnummer),
- für eine Benutzungsberechtigung gemäß Abs. 2 zusätzlich die Kostenstelle und die Unterschrift des Kostenstellenverantwortlichen,
- Angaben zum Rechner bzw. Anschluss in der Universität, Anforderungen an das System, für das eine Benutzungsberechtigung beantragt wird,
- Sofern der Benutzer nicht Mitglied oder Angehöriger der Universität Kassel im Sinne von § 2 Absatz 1 ist, eine Erklärung, dass der Benutzer die Benutzungsordnung anerkennt und in die Erfassung und Bearbeitung der eigenen personenbezogenen Daten zum Zwecke der Benutzerverwaltung einwilligt.

(5) Über den Antrag entscheidet der zuständige Systembetreiber. Er kann die Erteilung der Benutzungsberechtigung vom Nachweis bestimmter Kenntnisse über die Benutzung des Systems abhängig machen.

(6) Die Erteilung der Benutzungsberechtigung kann versagt, widerrufen oder nachträglich beschränkt werden, wenn

a) nicht hinreichend wahrscheinlich ist, dass der Antragsteller seinen Pflichten als Benutzer nachkommen wird (vgl. § 8),

b) das System für die beabsichtigte Benutzung offensichtlich ungeeignet oder für spezielle Zwecke reserviert ist oder

c) die Kapazität des Systems, dessen Nutzung beantragt wird, wegen einer bereits bestehenden Auslastung nicht ausreicht.

§ 4 Gesetzliche Einbindung

(1) Die IuK-Infrastruktur darf nur in rechtlich korrekter Weise genutzt werden. Es wird ausdrücklich darauf hingewiesen, dass nach dem Strafgesetzbuch unter Strafe gestellt sind:

a) Ausspähen von Daten (§ 202a StGB),

b) rechtswidriges Verändern, Löschen, Unterdrücken oder Unbrauchbarmachen von Daten (§ 303a StGB),

c) Computersabotage (§ 303b StGB) und Computerbetrug (§ 263a StGB),

d) die Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§86 StGB) oder rassistischem Gedankengut (§ 130 StGB),

e) die Verbreitung pornographischer Darbietungen durch Medien- oder Teledienste (§ 184 d StGB),

f) Ehrdelikte wie Beleidigung oder Verleumdung (§ 185 ff. StGB), Beschimpfungen von Bekenntnissen, Religionsgesellschaften oder Weltanschauungsvereinigungen (§ 166 StGB),

g) Urheberrechtsverletzungen, z.B. durch urheberrechtswidrige Vervielfältigung von Software oder die Eingabe geschützter Werke in eine DV-Anlage (§§ 106 ff. UrhG)

(2) In einigen Fällen ist bereits der Versuch strafbar.

(3) Benutzer und Systembetreiber haben die Bestimmungen des Hessischen Datenschutzgesetzes zu beachten.

§ 5 Rechte und Pflichten der Benutzer

(1) Die in § 1 genannten Ressourcen dürfen nur zu den in § 2 Abs. 1 genannten Zwecken genutzt werden.

(2) Der Benutzer ist verpflichtet, die Vorgaben dieser IT-Benutzungsordnung zu beachten und die Grenzen der jeweiligen Benutzungserlaubnis einzuhalten, insbesondere

a) den ordnungsgemäßen Arbeitsablauf,

b) den Schutz der IT-Systeme vor unbefugter, unsachgemäßer und missbräuchlicher Benutzung,

c) den ordnungsgemäßen Gebrauch von Passwörtern (die jeweilige Passwordpolicy wird durch den Systembetreiber festgelegt),

d) die Ermittlung oder Nutzung fremder Benutzerkennungen und Passwörter zu unterlassen,

e) den ausschließlichen Einsatz freigegebener gültiger Programme und Betriebssysteme.

(3) Der Benutzer ist darüber hinaus verpflichtet,

a) bei der Benutzung von Software, Dokumentationen und anderen Daten die gesetzlichen Regelungen (Urheberrechtsrechtsschutz) einzuhalten und

b) die Lizenzbedingungen, unter die im Rahmen von Lizenzverträgen erworbene Software, Dokumentation oder Daten zur Verfügung gestellt werden, zu beachten.

(4) Dem Benutzer ist es untersagt, ohne Zustimmung des Systembetreibers

a) Eingriffe in die Hardware- und Software-Installationen vorzunehmen oder

b) die Konfiguration der Betriebssysteme, des Netzwerks und der Software zu verändern.

(6) Der Benutzer ist verpflichtet, Vorhaben zur automatisierten Verarbeitung personenbezogener Daten der bzw. dem Datenschutzbeauftragten der Universität Kassel zu melden und mit dem jeweiligen Systembetreiber abzustimmen.

(7) Der Benutzer ist verpflichtet,
   a) dem Systemverantwortlichen auf Verlangen in begründeten Einzelfällen – insbesondere bei begründetem Missbrauchsverdacht und zur Störungsbeseitigung – zu Kontrollzwecken Auskünfte über Programme und benutzte Methoden zu gewähren.
   b) vor einer Installation von Software sich über die jeweiligen örtlichen und systemtechnischen Gegebenheiten und Regelungen zu informieren und diese zu befolgen.

(8) Hinsichtlich der Haftung des Benutzers gelten folgende Regelungen:
   a) Der Benutzer haftet für alle Nachteile, die der Universität durch missbräuchliche oder rechtswidrige Verwendung der DV-Ressourcen und Nutzungsberechtigung oder dadurch entstehen, dass der Benutzer schuldhaft seinen Pflichten aus dieser Benutzungsordnung nicht nachkommt. Die Universität kann verlangen, dass missbräuchlich genutzte Ressourcen und weitere Kosten nach Maßgabe der Entgeltordnung vom Benutzer zu erstatten sind.
   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 oder des Passworts an Dritte. In diesem Fall kann die Universität vom Benutzer nach Maßgabe der Entgeltordnung ein Nutzungsentgelt für die Drittnutzung verlangen.
   c) Der Benutzer hat die Universität von allen Ansprüchen freizustellen, wenn Dritte die Universität wegen eines missbräuchlichen oder rechtswidrigen Verhaltens des Benutzers auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen. Hierzu zählt insbesondere auch die Haftung für rechtswidrige Drittinhalte, die sich der Benutzer zu eigen macht.

   Soweit der Benutzer in einem Beamten-, Arbeits- oder Ausbildungsverhältnis zur Universität steht, richtet sich die Heranziehung zum Schadensersatz nach den einschlägigen beamten- bzw. tarifrechtlichen Regelungen.

§ 6 Aufgaben, Rechte und Pflichten des Systembetreibers

(1) Der Systembetreiber darf über die erteilten Benutzungsberechtigungen eine Nutzerdatei mit den Bestandsdaten der Benutzer führen. Die Antrags-Unterlagen zur Erteilung der Benutzerberechtigungen sind nach Auslaufen der Berechtigung zwei Jahre aufzubewahren.

(2) Der Systembetreiber gibt die Systemverantwortlichen für die Betreuung seiner Systeme bekannt. Der Systembetreiber und die Systemverantwortlichen sind zur Vertraulichkeit verpflichtet. Insbesondere sind alle Passwörter nach den aktuellen Sicherheitsstandards zu verarbeiten.

(3) Der Systembetreiber kann die Nutzung seiner Ressourcen vorübergehend einschränken oder einzelne Nutzerkennungen vorübergehend sperren, soweit es zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit sowie zum Schutze der Daten der Benutzer erforderlich ist. Die betroffenen Benutzer sind hierüber unverzüglich zu unterrichten.

(4) Sofern begründete Anhaltspunkte dafür vorliegen, dass ein Benutzer auf den Systemen des Systembetreibers rechtswidrige Inhalte zur Nutzung bereithält, kann der Systembetreiber die weitere Nutzung verhindern, bis die Rechtslage hinreichend geklärt ist.

(5) Der Systembetreiber ist berechtigt, die Sicherheit der Benutzerpasswörter und der Nutzerdaten durch regelmäßige manuelle oder automatisierte Maßnahmen zu überprüfen und notwendige Schutzmaßnahmen, zum Beispiel Änderungen leicht zu erratender oder veralteter Passwörter, durchzuführen, um die DV-Ressourcen und Benutzerdaten vor unberechtigten Zugriffen Dritter zu schützen. Über erforderliche Änderungen der Benutzerpasswörter, der Zugriffsberechtigungen auf Benutzerdateien und über sonstige nutzungsrelevante Schutzmaßnahmen ist der Benutzer unverzüglich in Kenntnis zu setzen.

(6) Der Systembetreiber ist berechtigt, für die nachfolgenden Zwecke die Verkehrsdaten der einzelnen Benutzer zu dokumentieren und auszuwerten:
   a) zur Gewährleistung eines ordnungsgemäßen Systembetriebs,
   b) zur Ressourcenplanung und Systemadministration,
   c) zum Schutz der personenbezogenen Daten anderer Benutzer,
   d) zu Abrechnungszwecken,
   e) für das Erkennen und Beseitigen von Störungen sowie
   f) zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung.

(7) Für die in Abs. 6 aufgeführten Zwecke ist der Systembetreiber auch berechtigt, Einsicht in die Inhaltsdaten zu nehmen, soweit dies zur Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Verstößen gegen die Benutzungsordnung erforderlich ist und hierfür tatsächlich Anhaltspunkte vorliegen. Das Datengeheimnis und das Vieraugenprinzip sind dabei zu beachten. In jedem Fall ist die Einsichtnahme zu dokumentieren, und der betroffene Benutzer ist nach Zweckerreichung unverzüglich zu benachrichtigen.
   Eine Einsichtnahme in die E-Mail-Postfächer ist jedoch nur zulässig, soweit dies zur Behebung aktueller Störungen im Nachrichtendienst unerlässlich ist. Eine Einsichtnahme in die Inhalte der E-Mails erfolgt nicht.
   Bei begründeten Hinweisen auf Straftaten handelt der Systembetreiber nach Abstimmung mit der Hochschulleitung in Absprache mit den zuständigen Behörden und wird - falls erforderlich - beweissichernde Maßnahmen einsetzen.

(8) Nach Maßgabe der gesetzlichen Bestimmungen ist der Systembetreiber zur Wahrung des Telekommunikations- und Datengeheimnisses verpflichtet. Das Protokollieren von Verbindungsdaten (z.B. Zugriffe auf den Datenbestand eines WWW-Servers) darf nur während der Zeit zur Behebung einer Störung personenbezogene Daten enthalten.

§ 7 Haftung des Systembetreibers und Haftungsausschluss

(1) Der Systembetreiber übernimmt keine Garantie dafür, dass das System fehlerfrei und jederzeit ohne Unterbrechung läuft. Der jeweilige Systembetreiber kann nicht für die Unversehrtheit (bzgl. Zerstörung, Manipulation) und Vertraulichkeit der bei ihm gespeicherten Daten garantieren.

(2) Der Systembetreiber haftet nicht für Schäden gleich welcher Art, die dem Benutzer aus der Inanspruchnahme der IuK-Ressourcen nach § 1 entstehen, soweit sich nicht aus den gesetzlichen Bestimmungen zwingend etwas anderes ergibt.

§ 8 Folgen einer rechtswidrigen Benutzung

Bei Vorliegen tatsächlicher Anhaltspunkte bzw. Verstößen gegen gesetzliche Vorschriften oder gegen Bestimmungen dieser IT-Benutzungsordnung, insbesondere die Rechte und Pflichten der Benutzer gemäß § 5, kann die Benutzungsberechtigung eingeschränkt oder widerrufen werden. Es ist dabei unerheblich, ob der Verstoß einen materiellen Schaden zur Folge hatte oder nicht. Maßnahmen zur Ein-

schränkung oder zum Entzug der Nutzungsberechtigung sollen erst nach vorheriger erfolgloser Abmahnung erfolgen. Dem Benutzer ist Gelegenheit zur Stellungnahme zu geben. Über Maßnahmen zur Einschränkung oder zum Entzug der Nutzungsberechtigung entscheidet nach Stellungnahme des jeweiligen Vorgesetzten der Kanzler.

§ 9 Sonstige Regelungen

(1) Für die Nutzung der IuK-infrastruktur können Entgelte oder Gebühren festgelegt werden.

(2) Für einzelne Systeme können bei Bedarf ergänzende oder abweichende Nutzungsregeln festgelegt werden.

§ 10 Inkrafttreten

(1) Diese IT-Benutzungsordnung wurde durch das CIO-Gremium am 25.10.2011 beraten und vom Präsidium der Universität Kassel am 23.04.2012 beschlossen.

(2) Die IT-Benutzungsordnung tritt am 01.02.2013 in Kraft. Sie wird in das Online-Informationsangebot der Universität Kassel aufgenommen.

Kassel, den 30.01.2013

In Vertretung

gez.

Dr. Robert Kuhn

- Kanzler -

Serviceebene	IT-Service-erbringer	Servicebaustein	Unterstützte Produkte	Unterstützte Standorte
Zugangsgerät	ITS	PoolPC	Vom ITS aufgestellte Arbeitsplätze	ITS-Pool-Räume
	ITS	Druckdienst	Vom ITS aufgestellte Drucker	ITS-Pool-Räume
	ITS	Desktoprechner	PC, Mac; gemäß ITS-Katalog	Vom ITS unterstützte Arbeitsplätze
	ITS	Notebook	Gemäß ITS-Katalog	Vom ITS unterstützte Arbeitsplätze
	ITS	Tablet	iOS (iPad), Android; gemäß ITS-Katalog	Vom ITS unterstützte Arbeitsplätze
	ITS	Smartphone	iOS (iPhone), Android, Symbian; gemäß ITS-Katalog	Vom ITS unterstützte Arbeitsplätze
	ITS	IP-Telefone	Siemens	Vom ITS unterstützte Arbeitsplätze
	UB	Nutzer-PCs	Von der UB aufgestellte Arbeitsplätze	UB-Räume
	UB	MMT-Pool	Von der UB aufgestellte Arbeitsplätze	UB-Räume
	UB	Druckdienst	Von der UB aufgestellte Drucker	UB-Räume
	SCL/ITS	E-Klausur	E-Klausur Laptops	E-Klausur-Center
PoolPC-Software	ITS	Standardsoftware	Wie unter http://cms.uni-kassel.de/unicms/index.php?id=its-software veröffentlicht	ITS-PoolPC
	ITS	Schulungssoftware	Auf schulungsspezifische Anfrage	ITS-PoolPC
	UB	Standardsoftware	Kiosksysteme, OPAC, bei MMT s. http://www.ub.uni-kassel.de/939.html	UB-PoolPC
	SCL	Standard- und E-Klausursoftware	Auf klausurspezifische Anfrage	E-Klausur Laptop
Desktopsoftware	ITS	Betriebssystem	MS Windows, Linux, MacOS	auf ITS-Endgerät
	ITS	Officeanwendungen	MS Office, OpenOffice	auf ITS-Endgerät
	ITS	Browser	Firefox, IE, Safari	auf ITS-Endgerät
	ITS	Skript- und Programmiersprachen	C, C++, php, Perl, Java	auf ITS-Endgerät
	ITS	Groupware	Lotus Notes, Communigate	auf ITS-Endgerät
	ITS	email Client	Thunderbird, Lotus Notes, Apple Mail, Outlook, Webmail	auf ITS-Endgerät
	ITS	VPN Client	Cisco	auf ITS-Endgerät
	ITS	Verwaltungsanwendung	SAP-GUI, SAP-Web-GUI	auf ITS-Endgerät
	ITS	Backup Client	Tivoli Storage Manager (TSM)	auf ITS-Endgerät
	ITS	Kommunikation	Jabber-Client, Instant Messaging	auf ITS-Endgerät
	ITS	PC-Videokommunikation	DFN-VC, Polycom, Adobe-Connect	auf ITS-Endgerät
	ITS	Virenschutz	Sophos	auf ITS-Endgerät
	ITS	Textverarbeitung	Tex, Latex, PDF-Reader	auf ITS-Endgerät
	ITS	Literaturverwaltung	Citavi	auf ITS-Endgerät
	ITS	Computeralgebra	Matlab, Mathematica, Maple	auf ITS-Endgerät
	ITS	Statistikprogramme	SPSS, R	auf ITS-Endgerät
	UB	Nutzer-PCs	Von der UB aufgestellte Arbeitsplätze	auf UB-Endgerät
	UB	MMT-Pool	Von der UB aufgestellte Arbeitsplätze	auf UB-Endgerät
	UB	Mitarbeiter-PCs und Thinclients	Von der UB aufgestellte Arbeitsplätze	auf UB-Endgerät
	UB	Druckdienst	Von der UB aufgestellte Drucker	auf UB-Endgerät
	UB	Betriebssystem	MS Windows, Linux, MacOS	auf UB-Endgerät
	UB	Officeanwendungen	MS Office, OpenOffice	auf UB-Endgerät
	UB	Browser	SeaMonkey, Firefox, IE, Safari	auf UB-Endgerät
	UB	email Client	SeaMonkey, Apple Mail, SquirrelMail	auf UB-Endgerät
	UB	Bibliothekssoftware	WinIBW, Transferprogramm	auf UB-Endgerät
	SCL	E-Assessment	Questionmark Authoring Manager	auf betreuten Clients
Serversoftware	ITS	Content Management System	Typo3	ITS-Maschinenraum
	ITS	Runtime Environments	C, C++, Fortran, php, Perl, Java	ITS-Maschinenraum
	ITS	Homepages	HTML, Typo3, php/MySQL	ITS-Maschinenraum
	ITS	Videokonferenzsystem	Tandberg	ITS-Maschinenraum
	ITS	Studierendenmanagement System	HIS - ZUL/SOS/LSF/POS/QIS, MOVEON	ITS-Maschinenraum
	ITS	ERP-System	SAP HCM, -CO, -FI, -FIAA, -FM, -REFX, -PM, -MM, -SRM	ITS-Maschinenraum
	ITS	eLearning-System	Moodle, Mahara, Wordpress, Questionmark Perception	ITS-Maschinenraum
	ITS	Identity Management System	Novell Identity Manager	ITS-Maschinenraum
	ITS	Trouble Ticket System	OTRS	ITS-Maschinenraum
	ITS	Lizenz-Server	Flexlm, etc.	ITS-Maschinenraum
	ITS	Forschungsinformationssystem	CONVERIS	ITS-Maschinenraum
	ITS	Business Intelligence	MicroStrategy	ITS-Maschinenraum
	UB	Content Management System	Typo3	UB-Räume
	UB	Homepage	HTML, Typo3, php/MySQL	UB-Räume
	UB	Publikationsmanagement	PUMA	UB-Räume
	UB	Bibliothekssystem	PICA-LBS	ITS-Maschinenraum
	UB	Institutional Repository)(Kobra)	DSpace	UB-Räume
	UB	Open Repository (Orka)	Goobi	ITS-Maschinenraum
	UB	Web-DB-Auto-Login-Server	HAN (Hidden Automatic Navigator)	UB-Räume
	UB	Universitätsweite Multifunktionskarte	Apache, PostgreSQL	UB-Räume
	ITS	Telefonanlage(VoIP)	Siemens	ITS-Maschinenraum
	ITS	Installations- und Konfigurationsverteilung	Rembo, Matrix42	ITS-Maschinenraum
	ITS	Virenschutz	Sophos	ITS-Maschinenraum
	ITS	Web Server	Apache	ITS-Maschinenraum
	ITS	Application Server	Tomcat	ITS-Maschinenraum
	ITS	Mail Server	Communigate, Lotus Notes, Traveller	ITS-Maschinenraum
	ITS	DB Server	MySql, MS-SQL-Server, PostgreSQL	ITS-Maschinenraum

Infrastruktursoftware	ITS	File Server	Samba, WebDAV, GPFS	ITS-Maschinenraum
	ITS	Backup Server	Tivoli Storage Manager (TSM)	ITS-Maschinenraum
	ITS	Name Server	BIND	ITS-Maschinenraum
	ITS	Directory Server	OpenLDAP, MS Active Directory, Novell eDirectory	ITS-Maschinenraum
	ITS	Authentification Server	NIS, Kerberos, Radius, Shibboleth	ITS-Maschinenraum
	ITS	Groupware Server	Communigate, Lotus Notes, Traveller	ITS-Maschinenraum
	ITS	Unified Messaging Server	MRS (Cycos)	ITS-Maschinenraum
	ITS	Wiki Server	Moin Moin	ITS-Maschinenraum
	ITS	Virtualisation Server	VMWare, KVM	ITS-Maschinenraum
	ITS	Time Server	ntp	ITS-Maschinenraum
	ITS	Mailing List Server	Majordome	ITS-Maschinenraum
	ITS	Discussion Server	Forensoftware PHPBB	ITS-Maschinenraum
	ITS	Video Server	Helix	ITS-Maschinenraum
	ITS	GoTo-Server (URL-Umleitung)	php	ITS-Maschinenraum
	ITS	News Server	DFN Service	DFN-Verein
	ITS	Compute-Server	Linux-Cluster	ITS-Maschinenraum
	UB	Installations- und Konfigurationsverteilung	Rembo (MMT-Server)	UB-Räume
	UB	Web Server	Apache	UB-Räume
	UB	Application Server	Tomcat	UB-Räume
	UB	Mail Server	Cyrus-IMAP	UB-Räume
	UB	DB Server	MySql, PostgreSQL, Sybase	ITS-Maschinenraum/UB-Räume
	UB	File Server	MS Windows, Linux	UB-Räume
	UB	Directory Server	OpenLDAP, MS Active Directory	UB-Räume
	UB	Virtualisation Server	Citrix Xen	UB-Räume
	UB	Universitätsweite Druck- und Kopierdienste (in Zus. mit Fa. Ricoh)	Q-Pilot-Server	UB-Räume
	UB	Terminalserver	MS Windows, Citrix XenApp	UB-Räume
Maschinensaal-Infrastruktur	ITS	Betriebssystem	Unix, Linux, Windows	ITS-Maschinenraum
	ITS	SAN	IBM	ITS-Maschinenraum
	ITS	Rechner-Hardware	Intel, AMD	ITS-Maschinenraum
	ITS	Rechnerarchitekturen	x86, Opteron, RS6000	ITS-Maschinenraum
	UB	Betriebssystem	Unix, Linux, Windows	ITS-Maschinenraum
	UB	Rechner-Hardware	Intel, AMD, Oracle	ITS-Maschinenraum
	UB	Rechnerarchitekturen	x86, Opteron, Sparc	ITS-Maschinenraum
Netzwerk-Infrastruktur	ITS	Festnetzanschluss	Analog, ISDN	Vom ITS unterstützte Arbeitsplätze
	ITS	WLAN	EDUROAM, VPN	Universitäre WLANs
	ITS	VPN	Cisco	ITS-Maschinenraum
	ITS	Internet	X-Win	ITS-Maschinenraum
	ITS	Firewall	Cisco Catalyst 6500 Series Firewall Services Modules, Sonicwall	ITS-Maschinenraum
	UB	LAN	Netgear, KTI	UB-Räume

Dienstanweisung zur Verarbeitung von schützenswerten dienstlichen Daten in mobilen Endgeräten und Cloud-Diensten

Anwendungsbereich

Die vorliegende Dienstanweisung gilt ab dem 01.08.2019 für alle Universitätsangehörigen, die schützenswerte dienstliche Daten auf mobilen Endgeräten (Smartphones, Tablets, Notebooks, etc.) verarbeiten. Sie gilt außerdem für alle Universitätsangehörigen, die für die Verarbeitung schützenswerter dienstlicher Daten Cloud-Dienste nutzen. Sie ergänzt die IT-Benutzungsordnung der Universität Kassel vom 30.01.2013.

1. Begriffsklärung

Schützenswerte dienstliche Daten

Schützenswerte dienstliche Daten im Sinne dieser Dienstanweisung sind Daten, die aufgrund einer Rechtsvorschrift, eines Vertrages oder einer sonstigen Regelung als vertraulich anzusehen sind. Hierunter fallen personenbezogene Daten wie z.B. Prüfungsergebnisse oder solche, wie sie z.B. in Bewerbungsunterlagen, dienstlichen E-Mails sowie in gespeicherten Dateien enthalten sind oder sein können. Nicht schützenswert im Sinne dieser Dienstanweisung sind Daten, die ohnehin für die Öffentlichkeit bestimmt sind (z.B. wiss. Veröffentlichungen, Lehrmaterialien, etc.).
Im Zweifel ist von einer Schutzwürdigkeit dienstlicher Daten auszugehen.

Datenverarbeitung

Datenverarbeitung im Sinne dieser Dienstanweisung ist jede Speicherung, Bearbeitung, Zugänglichmachung oder Übermittlung von Daten.

2. Zu treffende Maßnahmen

Schützenswerte dienstliche Daten dürfen mit mobilen Endgeräten nur dann verarbeitet werden, wenn

- der Zugriff auf das Gerät durch eine Bildschirmsperre geschützt ist, die nicht einfach zu umgehen ist.
- Dritten die Nutzung des Geräts nicht gestattet ist, sofern es diesen dadurch ermöglicht würde, auf die Daten zuzugreifen.
- der Benutzer die Möglichkeit aktiviert, selbst eine Fernlöschung der Daten auf dem Gerät vornehmen zu können (sofern das Gerät diese Funktionalität aufweist).
- der Zugriff auf die Daten auf diejenigen Anwendungen ("Apps") beschränkt ist, die diese nur für dienstliche Zwecke nutzen (sofern das Gerät diese Funktionalität aufweist).
- die Geräteverschlüsselung aktiviert ist (oder zumindest die Daten auf dem Gerät verschlüsselt gespeichert sind).
- bei der Nutzung "offener" (unverschlüsselter) WLANs (z.B. in Hotels) die Übertragung der Daten verschlüsselt erfolgt (z.B. durch die Verwendung eines VPN).

Im Sinne der Datensparsamkeit sollen auf mobilen Endgeräten so wenig wie möglich schützenswerte dienstliche Daten verarbeitet werden.
Vor der Außerbetriebnahme eines mobilen Endgeräts (z.B. wegen Veräußerung) sind alle Daten sicher zu löschen und das Gerät auf Werkseinstellungen zurückzusetzen. Defekte Geräte, bei denen dies nicht mehr möglich ist, können über die Universität datenschutzgerecht entsorgt werden.

3. Cloud-Dienste

Schützenswerte dienstliche Daten dürfen in Cloud-Diensten nur dann verarbeitet werden, wenn es sich um Cloud-Dienste der Universität Kassel oder deren Vertragspartner handelt. Es ist nicht erlaubt, schützenswerte dienstliche Daten bei externen Cloud-Anbietern (z.B. "Dropbox") zu verarbeiten. Dies gilt auch, wenn für die Nutzung eines Cloud-Dienstes kein mobiles Endgerät verwendet wird. Schützenswerte dienstliche Daten, die bei externen Cloud-Anbietern gespeichert wurden, sind dort zu löschen und auf erlaubte Cloud-Dienste zu migrieren.

Bei Fragen zur technischen Umsetzung der o. g. Maßnahmen sehen Sie bitte die Handreichung des ITS ein: http://www.uni-kassel.de/go/byod

Kassel, den 24.07.2019

Der Präsident
In Vertretung

gez. im Original Dr. N. Fischer

Dr. Oliver Fromm
Kanzler