Regelung zur Nutzung von zentralen IuK-Systemen der Hochschule Magdeburg Stendal

Wegen technischer und technologischer Änderungen wird die Regelung vom 12.11.2009 durch die Regelung 05/2017 ersetzt.

0 Präambel

Ziel dieser Betriebsregelung ist es, die Zusammenarbeit und Verantwortlichkeit der Benutzerinnen und Benutzer untereinander und zum zentralen Dienstleister Zentrum für Kommunikation und Informationsverarbeitung (ZKI) zu organisieren. Zur Erreichung dieses Ziels werden wesentliche Verhaltensregeln für einen optimalen und sicheren Umgang mit DV−Geräten, Netzressourcen und Kommunikationsdiensten, nachfolgend IuK-Systeme genannt, aufgestellt. Auch eine missbräuchliche Nutzung soll so vermieden werden.

IuK-Systeme bedürfen einer **sorgfältigen Planung und gegenseitigen Abstimmung**, da sie durch eine Vielzahl von **organisatorischen und funktionalen Prozessen** miteinander verbunden sind, z.B. der einheitlichen Verwaltungsstrategie, dem Datenaustausch und dem zentralen Datensicherungskonzept (Backup).

Der reibungslose Betrieb der IuK-Systeme im Hochschulbereich setzt ein **hohes Maß an Koordination** zwischen dem Betreiber und den Benutzerinnen und Benutzer voraus; insbesondere bei der **Planung von IT-Komponenten**, der **Konsistenzsicherung der Daten**, im **Havariefall,** bei der **Nutzung** der **Netzressourcen,** um nur einige zu nennen.

1 Geltungsbereich, Begriffsbestimmungen

1) Grundlage dieser Betriebsregelung sind die „Geschäftsordnung des ZKI“, die „Benutzerordnung für Informationsverarbeitungssysteme“ und die IT-Sicherheitsordnung der Hochschule Magdeburg-Stendal(FH)

2) Die Betriebsregelung bezieht sich auf alle IuK-Systeme der Hochschule Magdeburg-Stendal, nachfolgend Hochschule genannt, hier auch auf das interne Netz mit den Übergängen zum Wissenschaftsnetz und zu anderen Netzen.

3) **Betreiber** zentraler IuK-Systeme sowie der IuK-Systeme der Verwaltung[1] und zentralen Einrichtungen der Hochschule Magdeburg-Stendal (unter Beachtung gegebener Ausnahmeregelungen, wie auch Betriebstechnik) ist das ZKI

4) **Benutzerinnen und Benutzer** der IuK-Systeme sind im Wesentlichen die Mitglieder und die Angehörigen der Hochschule

1 Für die IuK (**I**nformation- **u**nd **K**ommunikation)-Systeme der Verwaltung gelten ergänzende Regelungen.

2 Betrieb von IuK-Systemen

1) Verfügbarkeitszeiten

Für alle online-Services des ZKI wird eine **Soll-Verfügbarkeit von 24*365 angenommen**. Während der Sollverfügbarkeit eines IuK-Systems gibt es i.d.R. jedoch **betriebsarme Zeiten**[2]. Das ZKI definiert für **Maßnahmen zum Erhalt oder Ausbau** der IT-Systeme entweder ein **Wartungsfenster** oder legt diese **nach Absprache mit den Benutzerinnen und Benutzern** in **betriebsarme Zeiten.**

Für Anfragen und bei Problemen stehen die KollegInnen des ZKI während der Geschäftszeiten, mindestens zu den Kernzeiten, zur Verfügung. Optimal ist eine Anfrage und Problemschilderung via Service-Mailadressen des ZKI

(https://www.hs-magdeburg.de/hochschule/einrichtungen/zki/personen.html) .

2) Abhängigkeiten der Verfügbarkeit

Die Verfügbarkeit der IuK-Systeme ist abhängig von der **Funktion des Datenkommunikationsnetzes**, welches ebenfalls durch das ZKI betrieben wird. Betriebsstörungen von IuK-Systemen müssen daher vom ZKI grundsätzlich in zwei unterschiedlichen Strukturen untersucht werden. Des Weiteren bestehen **Abhängigkeiten zur Elektroanlage**, zur **Klimatechnik** sowie zu **externen Netzen,** die außerhalb der Zuständigkeit des Betreibers liegen. Auch **bauliche Maßnahmen** können durch Umzug oder zeitweise Außerbetriebnahme von IuK-Technik Störungen in der Verfügbarkeit verursachen, die nicht durch das ZKI zu verantworten sind.

3) Kontakt mit Fremdfirmen

Fremdfirmen, mit denen das ZKI auf der Grundlage von Wartungsverträgen kooperiert, werden unter Wahrung des Datenschutzes in die Aufrechterhaltung eines reibungslosen Betriebes einbezogen.

4) Zugang zu DV-Räumen

Räume, in denen sich ausschließlich durch das ZKI zu betreuende IuK-Systeme befinden, liegen in der alleinigen Verantwortlichkeit des ZKI. Die Mitarbeiterinnen und Mitarbeiter des ZKI erhalten im Rahmen ihrer zu verrichtenden Tätigkeiten, differenziert nach der Schutzbedürftigkeit und der Sensibilität der verarbeitenden Daten den **Zutritt** zu den Räumen, in denen betreute IuK-Systeme untergebracht sind. Mitarbeiterinnen und Mitarbeiter aus anderen Organisationseinheiten der Hochschule, wie Dezernat IV Technik, Bau und Liegenschaften wird der Zugang nach Anmeldung im Sekretariat gewährt. Für Mitarbeiterinnen und Mitarbeiter von Serviceunternehmen, wie Reinigung, Wachdienst, Wartung, Instandhaltung kann der Zutritt (auf formlosen Antrag) durch die Leitung des ZKI gestattet werden. Zutritts- und Aufenthaltsbedingungen für datenschutztechnisch sensible IT-Räume sind gesondert und im Einzelfall geregelt.

5) Nutzung zentraler DV-Räume

Zentrale DV-Räume sind zweckgerichtet zu nutzen. PC-Pools dienen der Lehre und dem freien Üben an den dort verfügbaren PC-Systemen. In den Pools ist der Anschluß von privater Technik nicht erlaubt. Ausnahmen regelt der Dozent bzw. die ZKI-Leitung. Soweit technisch möglich, kann in anderen öffentlichen Räumen des ZKI private Technik angeschlossen werden. Die Infrastruktur des ZKI darf dabei nicht verändert werden (Kabel und Stecker verbleiben, wie vorgefunden). Dritte dürfen durch die Nutzung privater Technik nicht geschädigt werden. Die Verantwortung für die Nutzung privater Technik obliegt dem Eigentümer.

---

2 Zeiten außerhalb der Kernzeit, vorlesungsfreie Zeit

6) Konfiguration

Das ZKI übernimmt in seinem Verantwortungsbereich die **Konfiguration** der IuK-Systeme für eine **bestimmungsgerechte Verwendung**. Dies schließt sowohl die Hardware, als auch die Software-Komponenten ein. Voraussetzung ist eine gemeinsame Planung der Benutzerin bzw. des Benutzers mit dem ZKI. Werden Teile der Konfiguration von Fremdfirmen geleistet, koordiniert das ZKI diese Tätigkeiten. Hardware und Software eines IuK-Systems unterliegen im Laufe der Benutzung wechselnden Anforderungen, z.B. durch Datenzuwachs, Gesetzesänderungen oder geänderte Programmfunktionalitäten. Diesbezügliche **Installationsarbeiten, Updates, Patches** sowie **Stammdatenpflege** (soweit diese nicht von der Benutzerin bzw. vom Benutzer geleistet werden kann) werden vom ZKI durchgeführt oder organisiert.

7) Servicehotline

Das ZKI betreibt virtuelle Infrastrukturen mit einer **Vielzahl von Applikationen**, die auf **verschiedene Betriebssysteme** und **Datenbanken** aufbauen sowie ausgewählte Anwendungen auf unterschiedlichen Hardware-Plattformen. All diese Komponenten sind aufeinander abgestimmt und stellen in ihrer Summe einen planbaren Arbeitsaufwand für den Betreiber dar. Neue Hard- oder Software-Komponenten, die nicht zu geplanten IuK-Verfahren gehören (u.a. auch Projekte*)*, bedeuten hingegen eine außergewöhnliche personelle (und evtl. technische) Belastung für das ZKI. Die Servicehotline des ZKI für solche außerplanmäßigen Komponenten dezentraler Systeme kann nur bedingt erfolgen.

8) Kompetenzcenter

Das ZKI sammelt und stellt online Empfehlungen zu fachübergreifenden IuK-Systemen und deren Anwendung zur Verfügung (Hardware, Betriebssysteme, Standardsoftware, Zubehör).

9) Private Hard- und Software

Das ZKI betreut keine private Hard- und Software und haftet nicht für Schäden, die infolge deren Benutzung auftreten. Ähnliche **Sicherheitsrisiken** wie der Anschluss von Notebooks, stellt jede Art von **Datenübertragung** von außen an IuK-Technik im Datenkommunikationsnetz der Hochschule dar -gleich, ob die Quelle ein **Datenspeicher** oder ein **Internet-Download** ist. **Private Software** unterliegt den **urheber- und lizenzrechtlichen Bestimmungen**, für deren Einhaltung **jede Benutzerin und jeder Benutzer selbst** zu sorgen hat.

10) Benutzerverwaltung und Zugriffsrechte

Das **ZKI** übernimmt die **zentrale Nutzerverwaltung** der IuK-Systeme. Benutzernamen werden vom ZKI hochschulweit abgestimmt (federführend HIS-Datenbanken). In der zentralen Benutzerdatenbank werden Name, Vorname, Struktureinheit, Benutzeridentifikation und Telefonnummer gespeichert.

11) Netz- und Kommunikationsdienste

Das ZKI betreibt alleinig sowohl das Campus-Netz als auch das WLAN der Hochschule. Es werden folgende zentralen Dienste ausschließlich durch das ZKI erbracht: E-Mail, List-Server, DNS (Domain-Name-System), NTP (Zeit-Server), Zugang zum Internet, Backup/Archiv, Remote Access. Das ZKI betreut das lokale Netz der Zentralverwaltung.

Das ZKI gewährleistet die Verfügbarkeit und Sicherheit der Netze und der zentralen Dienste entsprechend den aktuellen Anforderungen. Die Administration der für die Netze und zentralen Dienste notwendigen Komponenten obliegt dem ZKI.

12) Datensicherung (Backup)

Das ZKI trifft auf Anforderung geeignete Maßnahmen, um die **Daten betreuter IuK-Systeme automatisch** zu **sichern**. Dies geschieht in **IT-üblicher Verfahrensweise** entsprechend dem aktuellen Stand der Technik, sofern mit den Benutzerinnen und Benutzern keine anderen, **speziellen Sicherungsverfahren/-algorithmen** vereinbart wurden. Im **Backup-Regime** wird unterschieden zwischen **Systemdaten** (z.B. Betriebssystem etc.), die weniger häufigen Änderungen unterliegen, und **Daten/ Dateien die durch die Benutzerinnen und Benutzer selber erstellt** werden und sich häufiger ändern können. (Der spezielle Umfang einer Datensicherung ist an die geforderte Verfügbarkeit des jeweiligen IuK-Systems angepasst.) Das ZKI übernimmt und organisiert **außerplanmäßige Datensicherungen** bei Wartungsmaßnahmen bzw. auf Anfrage von Benutzerinnen und Benutzern bei applikationsbedingten Anforderungen. Das Backup erfüllt die Funktion der **Sicherung des Betriebes** eines IuK-Systems. Es ist **kein Ersatz für die Archivierung** entsprechend den **gesetzlichen Aufbewahrungsfristen**.

13) Dokumentation

Das ZKI stellt sicher, dass **Zugriffsberechtigungen** für zentrale IuK-Systeme dokumentiert sind. Des Weiteren werden **Fehler- und Problemmeldungen von Benutzerinnen und Benutzern** und **Tätigkeiten der ZKI-Mitarbeiterinnen und ZKI-Mitarbeiter im Rahmen dieser Meldungen und deren Lösung** dokumentiert.

Tätigkeiten des ZKI, die **über den Rahmen der kontinuierlichen Dienstleistungen hinausgehen,** werden mit den entsprechenden Benutzerinnen und Benutzern **gesondert vereinbart** und in sog. **Projektdokumentationen** festgehalten.

14) Bekanntmachen von Dienstleistungen

Das **ZKI** sorgt für die **Bekanntmachung** seiner Dienstleistungen. Diese werden **im Intranet der Hochschule Magdeburg-Stendal zugänglich** gemacht und sind **verbindlich**.

15) Virenschutz

IuK-Systeme, deren Betrieb und Wartung nicht in die Zuständigkeit des ZKI gehören und nicht vom ZKI sicherheitstechnisch überprüft wurden, sind **nicht als völlig autark** anzusehen. Gleiches gilt für private PCs. Neben betriebsbedingten Beeinflussungen gibt es auch unbeabsichtigte Datenströme bzw. Beeinflussungen, vor denen sowohl die genannten, wie auch alle übrigen IuK-Systeme geschützt werden müssen. Ein wirksamer Schutz vor Viren, Trojanern und ähnlichen Programmen, die den Routinebetrieb behindern oder auf lange Zeit stilllegen können, ist nur möglich, wenn **auf allen potentiellen Angriffszielen gleiche Maßnahmen** ergriffen werden. Das ZKI bietet deshalb die **Leistung „Virenschutz“** sowohl für betreute als auch die o.g. IuK-Systeme an. Der Virenschutz ist von allgemeinem Interesse für die Hochschule.

Folgende Vorgaben sind bindend für DV-Systeme, die das ZKI betreibt bzw. für DV-Systeme in Bereichen mit sensiblen Daten:

- Betriebssystem muss auf dem aktuellsten Stand sein und ständig auf diesen gehalten werden, vor allem hinsichtlich verfügbarer Sicherheitsupdates
- Virenscanner muss installiert und aktiv sein und über aktuelle Viren-Signaturen verfügen, und diese auch ständig aktualisieren
- es wird empfohlen, **Outlook** bzw. Outlook-Express und den I**nternet Explorer nicht** zu verwenden, sondern Alternativen wie Thunderbird und Firefox
- es wird empfohlen, die Ausführung von **ActivX nicht** zu erlauben.

Jede Ausnahme von dieser Liste stellt eine Sicherheitslücke dar, die den verwaltungstechnischen Routinebetrieb bedroht.

16) Administration

Zur Administration sicherheitsrelevanter Funktionen durch Mitarbeiterinnen und Mitarbeiter des ZKI, nachfolgend Administratorinnen und Administratoren genannt, werden unterschiedliche Zugriffsprivilegien, wie die Berechtigung zum Verwalten von Authentisierungsdaten (Benutzerkennwörter, Passwörter, Zugriffsrechte), zur Verwaltung der Protokollierung und Auswertung sicherheitsrelevanter Ereignisse erteilt. Die Zugangskontrolle erfolgt mit Benutzerkennung und dazugehörigen Passwort. Für die Administratorinnen und Administratoren sind diese Angaben bei der Leiterin des ZKI gesichert aufzubewahren (Safe), damit bei plötzlicher Abwesenheit einer Administratorin bzw. eines Administrators deren/dessen Anmeldeprozedur von einer Vertreterin bzw. einem Vertreter nachvollzogen werden kann.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist **nur im Rahmen der Dienstaufgabe** durch Mitarbeiterinnen und Mitarbeiter des ZKI zulässig und setzt die aktenkundige Verpflichtung auf das Datengeheimnis voraus. Eine Nutzung dadurch erlangter Kenntnisse, auf **Weisungen** von Vorgesetzten oder anderen Personen, **Daten von Dritten zu beschaffen oder zugänglich zu machen, sind unzulässig**. Entsprechende Aufforderungen sind durch die Mitarbeiterinnen und Mitarbeiter zu verweigern. Eine Einsichtnahme in die Daten Dritter ist nur auf Antrag und unter Einbeziehung des Personalrates und des Datenschutzbeauftragten statthaft.

17) Erweiterung von Funktionalitäten

Wird es im Rahmen der Arbeitsaufgabe eines Bereiches oder einer Benutzerin bzw. eines Benutzers erforderlich, den **Funktionsumfang** eines zentralen DV-Systems zu ändern bzw. zu erweitern, muss dies **beim ZKI beantragt** werden. Jede **Funktionserweiterung muss geplant** und die damit verbundene Dienstleistung innerhalb des ZKI untersetzt werden[3]. Hierzu klassifiziert das ZKI die Anträge nach „**Projekten**“ (endlicher Arbeitsaufwand mit Projektziel) und „**Einführung neuer Dienstleistungen**“ (neuer Bestandteil der ZKI-Leistungen). In beiden Fällen werden **Verantwortlichkeiten, Arbeitsaufgaben** und **Ziele** schriftlich fixiert und vom Bereich sowie dem ZKI abgezeichnet.

3 Störungen der Verfügbarkeit

1) Informationen über den akuten Ausfall von Ressourcen

Das ZKI schafft im **Intranet der Hochschule** eine Möglichkeit, mit der sich **jede Benutzerin und jeder Benutzer** eines netzwerkfähigen PCs über **aktuelle Ausfälle oder Störungen** in IuK-Systemen informieren kann. An gleicher Stelle gibt das ZKI **wichtige Hinweise** für weitere Aktivitäten der Benutzerinnen und Benutzer im konkreten Fall. Diese Anzeige wird ständig aktuell gehalten. Die Benutzerin bzw. der Benutzer ist auch nach allgemeinen Arbeitsgrundsätzen dazu aufgefordert, sich dieser Informationsmöglichkeit zu bedienen.

Des Weiteren **informiert das ZKI** bei Ausfall einer IuK-Ressource **aktiv** die Leiterin bzw. den Leiter der Struktureinheit, die/der den entsprechenden IuK-Dienst dezidiert als Arbeitsmittel nutzt. Diese sind ggf. verpflichtet, nachgeordnete Einrichtungen zu informieren. Ist eine der angegebenen Personen nicht erreichbar, erfolgt die Meldung an das Sekretariat.

3 Das ZKI muss, wie jede Abteilung, technische, finanzielle und personelle Ressourcen planen. Eine neue Dienstleistung dauerhaft und zuverlässig zur Verfügung zu stellen, bedeutet fast immer eine Umverteilung dieser Ressourcen, die Beantragung oder Beschaffung neuer Ressourcen (Personal nicht möglich) sowie das sinnvolle Einbetten in bestehende Konzepte (Backup, Hardware- u. Softwareverwaltung, Schnittstellen etc.).

2) Voraussehbare Stillstandszeiten, Wartung

Voraussehbare Stillstandszeiten sind **keine Systemausfälle**. Sie sind **notwendigen Wartungs-, Reparatur- oder Erweiterungsleistungen** vorbehalten und werden i.d.R. langfristig mit den Benutzerinnen und Benutzern geplant. Diese Stillstandszeiten werden in das sog. **Wartungsfenster** (Zeit außerhalb der Soll-Verfügbarkeit) gelegt. Verfügt ein IuK-System nicht über ein Wartungsfenster, wird mit den Benutzerinnen und Benutzern eine Stillstandszeit innerhalb der **betriebsarmen Zeit** vereinbart.

Wird eine Stillstandszeit **kurzfristig** nötig, etwa um wesentliche Funktionalitäten einer Applikation zu gewährleisten oder um Schaden vom System abzuwenden, **erfolgt nach Rücksprache mit den Benutzerinnen und Benutzern eine Wartung** auch, wenn sie in der Hauptbetriebszeit liegt, jedoch von allen Beteiligten als notwendig erachtet wird.

Wie bereits die Informationen bei Ausfall von Ressourcen werden auch **voraussehbare Stillstandszeiten** an gleicher Stelle im **Intranet der Hochschule** vom ZKI veröffentlicht. Das ZKI aktualisiert diese Anzeige ständig. Die Benutzerin bzw. der Benutzer von IuK-Systemen sind angehalten, sich aktiv an dieser Stelle zu informieren.

3) Fehlerverfolgung / -behebung, extern

Muss die Verfolgung und Behebung von Fehlern an eine externe Firma übergeben werden, sorgt das ZKI bei zentralen IuK-Systemen für die Verpflichtung der Firma zur **Einhaltung des Datenschutzes**; insbesondere bei der Übertragung von Daten nach außen. Bei Fernwartung (Wartungsarbeiten über Modem oder Internet) sind die betei- ligten Firmen per Wartungsvertrag zur Einhaltung von **Datenschutzbestimmungen** und zur **Geheimhaltung** verpflichtet.

4) IT-Sicherheit

In Übereinstimmung mit Absatz 1 dieses Abschnittes werden an zentraler Stelle im **Intranet der Hochschule** im Bedarfsfall **Hinweise** veröffentlicht, die sich auf Möglichkeiten der Vermeidung des Ausfalls von DV-Ressourcen beziehen. Diese Hinweise erwachsen aus der genauen Kenntnis der Datenstruktur, der technischen Hintergründe und der langjährigen Erfahrungen seitens des ZKI.

Die aufgeführten Handlungsanweisungen sind Bestandteil des hochschulweiten IT-Sicherheitsprozesses (siehe IT-Sicherheitsordnung), denen Folge geleistet werden soll. Sie dienen dem größtmöglichen **Schutz der Daten** vor Verlust oder Beschädigung bei bestmöglicher **Aufrechterhaltung des Routinebetriebes**. Das ZKI ist sowohl über das IT-Sicherheitsmanagement-Team (SMT) als auch über die Gruppe der dezentralen IT-Sicherheitsbeauftragten in diesen Sicherheitsprozess involviert.

Alle Nutzerinnen und Nutzer, die Zugang zu geschützten Bereichen des Intranets der Hochschule wünschen, müssen die Sicherheitsvorgaben des Netzbetreibers (ZKI) akzeptieren und umsetzen.

5) Datensicherheit/ Datenschutz

Die **Benutzerinnen und Benutzer** von IuK-Systemen tragen die Verantwortung für die Maßnahmen der Datensicherheit und des Datenschutzes, wie die Integrität (Unversehrtheit), die Vertraulichkeit, die Verfügbarkeit der Daten zu wahren und die zu deren Verarbeitung eingesetzten technischen Einrichtungen zu erhalten. Dazu gehören unter anderem die Sicherheit vor Verlust, vor fahrlässiger oder vorsätzlicher Veränderung, vor Löschung, vor unbefugten Zugriff und vor missbräuchlicher Benutzung sowie die **Korrektheit der Datenerfassung**, die **ordnungsgemäße Bedienung der Software** sowie die **Prüfung der Ergebnisse** auf Sinnfälligkeit.

6) Meldepflicht

Bei Verdacht auf Viren, Trojaner und ähnliche Programme, die den **Routinebetrieb stören** und/oder **Daten ausspionieren** können, ist das ZKI zu informieren.

4 Fehlerbehandlungsroutinen

1) Fehlermeldungen der Benutzerinnen und Benutzer an das ZKI

Treten bei der Benutzung eines zentralen IuK-Systems (im Sinne Abschnitt 1 dieser Regelung) **Störungen oder Fehler** auf, so kann die Benutzerin bzw. der Benutzer – bevorzugt über die beiden folgenden Wege – eine **Meldung an das ZKI** absetzen:

a) Der Arbeitsplatz-PC (oder ein beliebiger anderer PC) funktioniert und ist netzwerk- fähig eine Mail an zki-md@hs-magdeburg.de und/oder zki-sdl@hs-magdeburg.de absetzen. Die Leitung des ZKI liest beide Mailadressen und sichert im Zweifel die Erfüllung der Meldung.

b) Wenn kein netzwerkfähiger PC zur Verfügung steht, kann ein Fax an die **Hotline des ZKI unter 0391 886 4364 abgesetzt** werden. Das gilt auch für den Standort Stendal. Informationen wie Geräte-ID-Nummer und DV-System bzw. zu fehlerhafte Hardware/Software sind mitzugeben.

2) Havarieplan

Es ist davon auszugehen, dass seitens des ZKI alle möglichen Schritte unternommen werden, um einen ausfallsicheren Betrieb von IuK-Systemen zu gewährleisten. Sollte es trotz aller Vorkehrungen zu einem unerwarteten **Teil- oder Totalausfall** einer IuK- Ressource kommen, der das **zeitliche Limit einer tolerierbaren Nichtverfügbarkeit** für einen Bereich überschreitet, so muss auf einen **Havarieplan** zurückgegriffen werden. Das ZKI steht auf Anforderung beratend zur Seite.