IT-Sicherheitsrichtlinie der Universität Erfurt

Inhalt

Richtlinientext	Erläuterungen und Hinweise	
	Referenznummer	
	Titel	IT-Sicherheitsrichtlinie
	Letzte Änderung Richtlinientext	21.08.2019
	Letzte Änderung Erläuterungen und Hinweise	26.11.2019
	Zielgruppe	Mitglieder, Angehörige und Gäste der Universität Erfurt
	Autorinnen und Autoren	- IT-Sicherheitsbeauftragter (Frank Becker) - Leitung des URMZ (Frank Trefflich) - Datenschutzbeauftragte (Ute Winter) - Kanzler (Dr. Jörg Brauns) - Leitung des Rechtsamts (Christine Kneipel) - Organisationsentwicklung (Dr. Susanne In der Smitten)
	Verabschiedet durch	Präsidium
	Implementiert durch	IT-Sicherheitsbeauftragter
	Monitoring der Einhaltung	Bereichsleitungen
	Kommentare	

Richtlinientext	Erläuterungen und Hinweise
## 1. Präambel Der Betrieb einer Universität hängt in hohem und zunehmendem Maße von der Qualität ihrer IT-Dienstleistungen ab, da leistungsfähige Forschung, Lehre und Verwaltung auf eine funktionsfähige und sichere Informationstechnologie (IT) angewiesen sind. Viele Geschäftsprozesse der Universität sind bereits IT-basiert, weitere werden folgen. Im Rahmen eines integrierten Informationsmanagements werden Geschäftsprozesse und IT-Dienstleistungen immer enger miteinander verknüpft. Der Einsatz von IT-Systemen führt dabei zu einer Effizienzsteigerung von Arbeitsabläufen bei gleichzeitig deutlich verbessertem Dienstleistungsangebot. Daher ist die „Sicherheit in der Informationstechnik“ (IT-Sicherheit) für die Universität Erfurt eine elementare Voraussetzung für ihre Aufgabenerfüllung, auch im Hinblick auf die Erfüllung gesetzlicher Auflagen, z.B. im Bereich des Datenschutzes. Die vorliegende IT-Sicherheitsrichtlinie gilt daher im Zusammenhang mit der Datenschutzrichtlinie und weiteren Handreichungen zu IT-Sicherheit und Datenschutz an der Universität Erfurt.	
## 2. Ziele und Adressatenkreis Das Ziel dieser Richtlinie ist ein angemessener Schutz der IT-Infrastrukturen, -Systeme, -Anwendungen, -Verfahren und -Prozesse sowie der dabei verarbeiteten Daten und Informationen an der Universität Erfurt. Hierzu formuliert die Richtlinie Verantwortlichkeiten im Rahmen der IT-Sicherheit, Verpflichtungen zur Gewährleistung derselben sowie die Konsequenzen und das Verfahren bei Sicherheitsverstößen. Sie gilt für alle Bereiche und Einrichtungen, Mitglieder und Angehörigen der Universität Erfurt sowie für alle Personen, die IT-Systeme und IT-Verfahren der Universität Erfurt benutzen oder betreiben. Eine Leistungs- und Verhaltenskontrolle findet nicht statt.	

Richtlinientext	Erläuterungen und Hinweise
## 3. Begriffsbestimmungen und Verantwortlichkeiten ### 3.1 Begriffsbestimmungen *3.1.1 IT* IT ist die Abkürzung von Informationstechnologie und umfasst den gesamten Bereich der technischen Informations- und Datenverarbeitung und somit IT-Infrastruktur, IT-Systeme, IT-Verfahren und IT-Prozesse.	
3.1.2 IT-Infrastruktur IT-Infrastruktur ist die Gesamtheit aller Gebäude, Kommunikationsdienste (Netzwerk), Maschinen (Hardware) und Programme (Software), die einer übergeordneten Ebene durch eine untergeordnete Ebene (lat. infra „Unter“) zur automatisierten Informationsverarbeitung zur Verfügung gestellt werden.	
3.1.3 IT-System/ IT-Verfahren / IT-Prozesse IT-Systeme sind elektronisch datenverarbeitende Systeme und bezeichnen im Wesentlichen genutzte Hardware, wie z.B. Arbeitsstationen, Notebooks, Smartphones, Server oder Netzwerkkomponenten. IT-Verfahren stehen für das Zusammenwirken von IT-Systemen und Anwendungen. IT-Prozesse sind umfänglichere zusammenhängende Arbeitsabläufe, die IT-Verfahren integrieren und somit Informationen digital über einen längeren Zeitraum verarbeiten.	
3.1.4 Schützenswerte Daten Schützenswerte Daten sind insbesondere alle personenbezogenen Daten. Zu unterschiedlichen Graden der Schutzbedürftigkeit berät die/der Datenschutzbeauftragte.	Informationen zur/zum aktuellen Datenschutzbeauftragten der Universität Erfurt finden Sie im Internet unter https://www.uni-erfurt.de/datenschutz/datenschutzbeauftragte/
### 3.2 Verantwortlichkeiten Die Gesamtverantwortung für die IT-Sicherheit liegt beim Präsidium der Universität Erfurt.	
3.2.1 Chief Information Officer (CIO) Der Chief Information Officer (CIO) nimmt die Aufgaben der strategischen und operativen Führung der Informationstechnologie wahr. Die Bestellung des CIO erfolgt durch das Präsidium.	Gegenwärtig ist der CIO der Kanzler der Universität.

Richtlinientext	Erläuterungen und Hinweise
3.2.2 IT-Sicherheitsbeauftragte/r IT-Sicherheitsbeauftragte/r ist die Person, die von der Universitätsleitung dazu bestimmt wurde, die Hochschulleitung und den CIO bei der Wahrnehmung ihrer Aufgaben bezüglich der IT-Sicherheit zu beraten und bei deren Umsetzung zu unterstützen. Der/Die IT-Sicherheitsbeauftragte nimmt damit die Verantwortung für die IT-Sicherheit fachlich wahr.	Informationen zur/zum aktuellen IT-Sicherheitsbeauftragten der Universität Erfurt finden Sie im Internet unter https://www.uni-erfurt.de/urmz/it-sicherheit/
3.2.3 IT-Personal Das IT-Personal umfasst zentrale oder dezentrale Administratorinnen und Administratoren, die für die technische Bereitstellung und Betreuung von Hard- und Software (insbesondere Wartung, Installation, Konfiguration) zuständig sind und die IT-Nutzerinnen und -Nutzer beraten und unterstützen. An der Universität Erfurt ist das IT-Personal im Wesentlichen am Universitätsrechen- und Medienzentrum (URMZ) verortet. Das URMZ ist insbesondere verantwortlich für • die Beschaffung und Bereitstellung von Hard- und Software für alle Bereiche und Einrichtungen, Mitglieder und Angehörigen der Universität Erfurt • die Erfassung und Registrierung der Geräte • Registrierung mobiler dienstlicher Endgeräte und Unterweisung der IT-Nutzerinnen und -Nutzer (vgl. Ziff. 4.1) • die Einrichtung und Aufhebung von Netzzugängen und Benutzerkonten sowie ggf. die vorübergehende Sperrung des Zugangs zur Gefahrenintervention • die Beratung und Unterstützung der IT-Nutzerinnen und -Nutzer • die Organisation regelmäßiger Schulungen für die IT-nutzenden Beschäftigten der Universität (vgl. Ziff. 4.3) • die Sicherung der Geräte vor unbefugten Zugriffen (vgl. Ziff. 4.2) durch entsprechende bauliche Vorkehrungen in Absprache mit dem zuständigen Dezernat für Gebäudemanagement, durch Unterstützung von Maßnahmen zum Diebstahlschutz (z.B. Aushändigen von geeigneten Schlössern zur Sicherung mobiler Endgeräte an IT-Nutzerinnen und -Nutzer) und durch eine entsprechende Sensibilisierung aller Nutzergruppen über Hinweisblätter und Schulungen • die Ausstattung der Rechnersysteme mit Zugriffschutz (vgl. Ziff. 4.4) • die Einrichtung von Virenschutzprogrammen auf Arbeitsplatzrechnern und mobilen Geräten (vgl. Ziff. 4.5)	Geeignete Schlösser zur Sicherung mobiler Endgeräte sind beispielsweise Kensington-Schlösser.

Richtlinientext	Erläuterungen und Hinweise
3.2.4 IT-Verantwortliche/r IT-Verantwortliche sind diejenigen, die über Zwecke, den Einsatz und die Mittel eines IT-Verfahrens oder -Prozesses entscheiden. Sie tragen die Verantwortung für die technische und organisatorische Sicherheit des Verfahrens.	
3.2.5 Bereichsleitung Bereichsleitung ist diejenige Person, die einer Einrichtung, einem Dezernat usw. vorsteht. Als Fachvorgesetzte sind die Bereichsleitungen für die erforderlichen aufgabenspezifischen Schulungen ihrer Mitarbeiterinnen und Mitarbeiter verantwortlich. Sie tragen dafür Sorge, dass ihre Mitarbeiterinnen und Mitarbeiter an den angebotenen Schulungen des URMZ und der Datenschutzbeauftragten zur IT-Sicherheit und zum Datenschutz teilnehmen.	
3.2.6 IT-Nutzer/in IT-Nutzerinnen und -Nutzer im Sinne dieser Richtlinie sind alle Personen, die IT-Systeme und -Verfahren der Universität Erfurt benutzen oder betreiben. Sie tragen die Verantwortung, die in dieser Richtlinie und ergänzenden Handreichungen formulierten Pflichten und getroffenen Regelungen für IT-Nutzerinnen und -Nutzer (vgl. Abschnitt 5) einzuhalten.	

Richtlinientext	Erläuterungen und Hinweise
## 4. Grundsätze und Prinzipien der IT-Sicherheit Der IT-Sicherheit an der Universität Erfurt liegen folgende Grundsätze und Prinzipien zugrunde: • IT-Sicherheit wird als strategische Aufgabe begriffen, und Maßnahmen zu ihrer Gewährleistung werden durch das Präsidium unterstützt • IT-Systeme werden durch kompetentes Personal langfristig betreut • IT-Systeme werden in einer sicheren Umgebung betrieben und insbesondere auch vor Diebstahl geschützt • IT-Systeme werden auf einem adäquaten Versionsstand gehalten • IT-Systeme werden vor schädlicher Software (sog. „Malware“) geschützt • Die administrative Arbeit auf IT-Systemen wird sicher und nachvollziehbar gestaltet • Informationen werden ihrem Schutzbedarf entsprechend angemessen sicher verarbeitet und adäquat vor unberechtigten Zugriffen geschützt • IT-nutzende Beschäftigte werden geschult, so dass in der Breite ein Grundverständnis für Belange der IT-Sicherheit gewährleistet werden kann; hinzu kommen aufgabenspezifische Schulungen (vgl. Ziffer 4.3). • IT-Sicherheitszwischenfälle werden dokumentiert und kommuniziert • Die IT-Sicherheitsrichtlinie wird regelmäßig, mindestens jedoch einmal pro Jahr auf ihre Aktualität, Wirksamkeit und Angemessenheit hin überprüft und bei Bedarf weiterentwickelt.	
### 4.1 Registrierung mobiler dienstlicher Endgeräte und Unterweisung der IT-Nutzerinnen und -Nutzer Alle dienstlichen mobilen Geräte (Smartphones, Tablets, Notebooks, usw.), auch solche, die nicht vom URMZ betreut werden, sind vom URMZ/zuständigen IT-Personal in einer Liste zu erfassen und zu registrieren. Die IT-Nutzerinnen und -Nutzer werden bei der Übergabe durch ein entsprechendes Hinweisblatt über den Umgang mit dem mobilen Gerät informiert und bestätigen die Kenntnisnahme und Einhaltung der Regeln durch Unterschrift.	Verantwortlich für die Initiierung: CIO, Bereichsleitung Verantwortlich für die Umsetzung: URMZ, IT-Nutzerinnen und -Nutzer Das Hinweisblatt zur Vergabe von Administrationsrechten für PC-, Notebooknutzer an der Universität Erfurt finden Sie im Intranet unter https://www.uni-erfurt.de/mitarbeiterservice/mein-arbeitsplatz/it-service/selbstadministration/

Richtlinientext	Erläuterungen und Hinweise
4.2 Sicherung der IT-Infrastruktur Die IT-Infrastruktur der Universität Erfurt ist gegen unbefugten Zugang zu schützen. Dies ist durch technische und organisatorische Maßnahmen sicherzustellen, die den Zugang zu schützenswerten Daten verhindern oder zumindest erschweren. Das Nähere regelt das IT-Sicherheitskonzept des URMZ.	Verantwortlich für die Initiierung: CIO, Bereichsleitung Verantwortlich für die Umsetzung: URMZ
4.3 Schulungen Die IT-nutzende Beschäftigte sind grundsätzlich aufgabenspezifisch zu schulen und dürfen erst dann mit IT-Verfahren arbeiten. Dabei sind sie insbesondere auch mit den für sie geltenden Sicherheitsmaßnahmen und den Erfordernissen des Datenschutzes vertraut zu machen. Diese Schulung hat prinzipiell das allgemeine Sicherheitsbewusstsein und die Einsicht in die Notwendigkeit von IT-Sicherheitsmaßnahmen zu entwickeln. Die Schulung sollte auch eine realistische Selbsteinschätzung fördern. Die IT-Nutzerinnen und -Nutzer sollen in die Lage versetzt werden zu erkennen, wann IT-Personal sowie IT-Sicherheits- und Datenschutzbeauftragte/r hinzugezogen werden müssen. Zusätzlich organisiert das URMZ (vgl. Ziff. 3.2.3) Schulungen für IT-nutzende Beschäftigte zu den Grundlagen der IT-Sicherheit und des Datenschutzes, die von den IT-nutzenden Beschäftigten einmal jährlich verpflichtend wahrzunehmen sind.	Verantwortlich für die Initiierung: URMZ, Bereichsleitung Verantwortlich für die Umsetzung: URMZ, Bereichsleitung

Richtlinientext	Erläuterungen und Hinweise
### 4.4 Zugriffschutz Alle Rechnersysteme sind so einzurichten, dass nur berechtigte Nutzerinnen und Nutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist zunächst eine Anmeldung mit Benutzerkennung und einem Kennwort oder anderen eindeutigen Merkmalen erforderlich. Die Vergabe von Benutzerkennungen für die Arbeit an IT-Systemen erfolgt grundsätzlich personenbezogen. In den Fällen, in denen aus dienstlichen Gründen ein Account ohne Personenbezug erforderlich ist, kann ein Funktions-Account eingerichtet werden. Der Kreis der Nutzerinnen und Nutzer solcher Funktions-Accounts ist unbedingt auf das Notwendigste zu beschränken und regelmäßig zu überprüfen. Die Nutzerinnen und Nutzer dürfen nur mit den Zugriffsrechten ausgestattet werden, die unmittelbar für die Erledigung ihrer Aufgaben vorgesehen sind. Insbesondere sind alltägliche Arbeiten nicht mit privilegierten Benutzerkonten (Administrator, root o. a.) vorzunehmen. Bei allen administrativen Anwendungen (z.B.: ERP-System), die gesetzlichen Anforderungen genügen müssen (Datenschutz, Handelsgesetzbuch, u. a.), erfolgt die Vergabe bzw. Änderung der Zugriffsrechte für die einzelnen Nutzerinnen und Nutzer auf schriftlichen Antrag mit Zustimmung der Bereichsleitung. In allen anderen Bereichen sind die dort geltenden Regelungen zu beachten. In der Regel ist auch hier für die Vergabe der Zugriffsrechte ein schriftlicher Antrag erforderlich. Bei der Vergabe von Zugriffsrechten ist die Funktionstrennung zu beachten.	Verantwortlich für die Initiierung: CIO, Bereichsleitung Verantwortlich für die Umsetzung: IT-Personal, IT-Nutzerinnen und -Nutzer
### 4.5 Virenschutz Auf allen Arbeitsplatzrechnern und mobilen Geräten, ist, soweit technisch möglich, ein aktueller Virenscanner einzurichten, der automatisch alle eingehenden und zu öffnenden Dateien überprüft. Damit soll bereits das Eindringen von schädlichen Programmen erkannt und verhindert werden.	Verantwortlich für die Initiierung: CIO, Bereichsleitung Verantwortlich für die Umsetzung: IT-Personal

Richtlinientext	Erläuterungen und Hinweise
### 4.6 Konsequenzen bei Sicherheitsverstößen Die IT-Infrastruktur ist im zugelassenen Rahmen so zu nutzen, dass nicht gegen die an der Universität geltenden IT-Sicherheitsvorgaben verstoßen wird, welche in dieser Richtlinie, der Benutzungsordnung des URMZ sowie in den sie ergänzenden Durchführungsbestimmungen und weiteren, vom Leiter des URMZ auf der Grundlage der Benutzungsordnung oder vom Kanzler als CIO erlassenen Regeln für die Nutzung der Datenverarbeitungs-Anlagen der Universität geregelt sind. IT-Sicherheitsverstöße können z.B. dazu führen, dass • die Sicherheit der Mitarbeiter*innen, Nutzer*innen, Vertragspartner*innen sowie des Vermögens der Universität Erfurt in erheblichem Umfang beeinträchtigt wird, • durch Kompromittierung der Sicherheit von Daten oder Geschäftsinformationen die Universität Erfurt erheblichen finanziellen Verlust erleidet, • der unberechtigte Zugriff auf Systeme und Informationen zu deren unerwünschter Preisgabe und/oder Änderung führt, • die Informationstechnik der Universität Erfurt für illegale Zwecke genutzt wird oder • der unbefugte Zugriff auf personenbezogene Daten ermöglicht wird. Verstöße gegen IT-Sicherheitsvorgaben werden nach den geltenden rechtlichen Bestimmungen geahndet. Auf folgende Vorschriften des Strafgesetzbuchs (StGB) und des Thüringer Datenschutzgesetzes (ThürDSG) wird in diesem Zusammenhang besonders hingewiesen: • Ausspähen von Daten (§ 202a StGB) • Verletzung von Privatgeheimnissen (§ 203 StGB) • Verletzung des Post- oder Fernmeldegeheimnisses (§ 206 StGB) • Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB) • Ordnungswidrigkeiten und Strafbestimmungen (§ 61 ThürDSG) Darüber hinaus können IT-Sicherheitsverstöße dienst- oder arbeitsrechtliche Konsequenzen nach sich ziehen. Zur Gefahrenintervention können vom URMZ Netzzugänge oder Benutzerkonten vorübergehend deaktiviert werden.	Verantwortlich für die Initiierung: IT-Sicherheitsbeauftragter Verantwortlich für die Umsetzung: Universitätsleitung Die Benutzungsordnung des Universitätsrechen- und Medienzentrums der Universität Erfurt finden Sie im Internet unter https://www.uni-erfurt.de/fileadmin/public-docs/Hochschulrecht/Satzungsrecht_UE/Benutzungs-O/Benutzerordnung_URMZ.pdf

Richtlinientext	Erläuterungen und Hinweise
## 5. Pflichten der IT-Nutzerinnen und IT-Nutzer ### 5.1 Sicherung der IT-Infrastruktur Die IT-Nutzerinnen und -Nutzer haben innerhalb ihres Aufgabenbereichs dafür Sorge zu tragen, dass unbefugter Zugang zur IT-Infrastruktur der Universität Erfurt und die unbefugte Nutzung verhindert werden. Büroräume sind beim Verlassen zu verschließen, Bildschirme zu sperren, Arbeitsplatzrechner und mobile Geräte nach Dienstschluss auszuschalten. Bei längerer Abwesenheit sollen leicht zu transportierende Geräte in Schränken verschlossen aufbewahrt oder durch andere geeignete Maßnahmen (z.B. Schlösser zur Sicherung mobiler Endgeräte) vor Diebstahl gesichert werden. Bei der Anordnung und Verwendung der Geräte ist darauf zu achten, dass schützenswerte Daten nicht von Unbefugten eingesehen werden können. Beim Ausdrucken oder Faxempfang derartiger Daten muss das Entnehmen der Ausdrucke durch Unbefugte verhindert werden.	Abschnitt 5 dieser Richtlinie umfasst solche Regelungen, deren Einhaltung von jeder IT-Nutzerin und jedem IT-Nutzer unmittelbar selbst verantwortet wird. Verantwortlich für die Initiierung: CIO, Bereichsleitung Verantwortlich für die Umsetzung: IT-Nutzerinnen und -Nutzer Geeignete Schlösser zur Sicherung mobiler Endgeräte sind beispielsweise Kensington-Schlösser; Sie können Sie beim IT-Personal des URMZ erhalten.
### 5.2 Nutzung und Sicherung mobiler dienstlicher Geräte Bei der Nutzung mobiler dienstlicher Geräte sind von den IT-Nutzerinnen und -Nutzern die vom URMZ erteilten Hinweise zum Umgang mit mobilen Geräten zu beachten. Die mobilen Geräte sind durch geeignete Maßnahmen (Kennwort-Schutz, nur Einsatz legitimierter Software (siehe 5.4), regelmäßige Updates, keine Verwendung von nichtlegitimierten externen Cloud-Diensten, etc.) entsprechend zu schützen. Die weiteren unter Ziffer 5 getroffenen Regelunge (insbesondere zum Schutz durch Kennwörter usw.) sind entsprechend zu beachten. Sofern die jeweilige Applikation eigene Schutzmechanismen anbietet (Verschlüsselung, Kennwörter, etc.) sind diese zu verwenden. Bei der Speicherung von schützenswerten Daten auf mobilen Geräten (Smartphones, Tablets, Notebooks, usw.) sind besondere Vorkehrungen zum Schutz der Daten zu treffen. Mobile Geräte sind möglichst verschlossen aufzubewahren. Auf regelmäßige Datensicherung ist besonderer Wert zu legen.	Verantwortlich für die Initiierung: CIO, Bereichsleitung Verantwortlich für die Umsetzung: IT-Nutzerinnen und -Nutzer Hinweise zur Datensicherung finden Sie auf den Webseiten der Universität Erfurt unter https://www.uni-erfurt.de/computerhilfe/windows-10/tipps/datensicherung-mit-dateiversionsverlauf/

Richtlinientext	Erläuterungen und Hinweise
### 5.3 Telearbeit Bei der Telearbeit verlassen Daten den räumlich eingegrenzten Bereich der datenverarbeitenden Stelle. Die telearbeitenden IT-Nutzerinnen und -Nutzer haben die entsprechenden Vereinbarungen zum Schutz der bearbeiteten Daten und verwendeten Systeme einzuhalten (IT-Sicherheits- und Datenschutzrichtlinie für Telearbeitsplätze an der Universität Erfurt).	Verantwortlich für die Initiierung: Bereichsleitung Verantwortlich für die Umsetzung: IT-Nutzerinnen und -Nutzer Hinweise zu IT-Sicherheit und Datenschutz bei der Telearbeit finden Sie auf den Webseiten der Universität Erfurt unter https://www.uni-erfurt.de/datenschutz/datenschutz-im-bueroalltag/telearbeit/
### 5.4 Kontrollierter Software-Einsatz Auf allen Rechnersystemen der Universität Erfurt darf zum Zweck des Schutzes von universitätseigener Hardware und dem Universitätsnetz nur Software installiert werden, die zur Erfüllung der dienstlichen Aufgaben erforderlich ist. Dies gilt insbesondere auch für nicht vom URMZ betreute Geräte (Selbstadministration). Im Zweifelsfall ist die Zustimmung der Bereichsleitung und des URMZ einzuholen.	Verantwortlich für die Initiierung: CIO, Bereichsleitung Verantwortlich für die Umsetzung: IT-Nutzerinnen und -Nutzer, URMZ
### 5.5 Nutzung privater Hard- und Software Die Benutzung von privater Hard- und Software (Bring Your Own Device, BYOD) in Verbindung mit technischen Einrichtungen der Universität Erfurt und deren Netzen ist grundsätzlich nicht gestattet. Dies betrifft insbesondere auch die Speicherung dienstlicher Daten auf privaten Geräten. Allgemeine Ausnahmen gelten für den Einsatz von privaten Computern für Lehrveranstaltungen und Vorträge sowie in speziell gekennzeichneten Bereichen, wie zum Beispiel in Bibliotheken oder in Studierendenarbeitsbereichen, und im Funknetz eduroam. Auch ist der Abruf dienstlicher Emails über private Geräte gestattet, wenn dies über Webmail erfolgt. Die Bereichsleitung kann weitere Ausnahmen in Abstimmung mit dem URMZ gestatten.	Verantwortlich für die Initiierung: CIO, Bereichsleitung Verantwortlich für die Umsetzung: IT-Nutzerinnen und -Nutzer

Richtlinientext	Erläuterungen und Hinweise
5.6 Virenschutz Per E-Mail erhaltene Anhänge sind nur dann zu öffnen, wenn ihre Herkunft bekannt und Ungefährlichkeit wahrscheinlich ist. Auch auf nicht vom URMZ betreuten Geräten (selbstadministrierten Geräten) ist, soweit technisch möglich, ein aktueller Virenscanner einzurichten, der automatisch alle eingehenden und zu öffnenden Dateien überprüft. Bei Verdacht auf Vireninfektion ist das zuständige IT-Personal zu informieren.	Verantwortlich für die Initiierung: CIO, Bereichsleitung Verantwortlich für die Umsetzung: IT-Nutzerinnen und -Nutzer
5.7 Zugriffsschutz Beim Verlassen des Arbeitsplatzes müssen der Arbeitsplatzrechner und mobile Geräte (Notebooks, Tabletts, Smartphones, usw.) durch einen Kennwortschutz gesperrt werden. Grundsätzlich sind die Arbeitsplatzsysteme nach Dienstschluss auszuschalten, dabei sollte die Spannungszuführung durch schaltbare Steckdosenleisten nicht unterbrochen werden (Gewährleistung der nächtlichen Update-Funktion). Von diesen Regelungen kann nur abgewichen werden, soweit es die Arbeitsorganisation dringend erfordert und/oder andere Sicherheitsmaßnahmen es ermöglichen. IT-Nutzerinnen und -Nutzer haben ihr Passwort geheim zu halten. Idealerweise sollte das Passwort nicht notiert werden. Die Arbeit unter der Kennung einer anderen Person ist unzulässig. Den IT-Nutzerinnen und –Nutzern ist untersagt, Kennungen und Passwörter weiterzugeben. Dies gilt für alle genutzten Systeme und Dienste. Ausgenommen von dieser Regelung sind Systeme, die für allgemeine öffentliche Zugänge bestimmt sind (z. B. Kiosksysteme, Abfragestationen für Bibliothekskataloge). Erhalten IT-Nutzerinnen und -Nutzer beim Anmelden mit dem persönlichen Passwort temporär keinen Zugriff auf das System, besteht die Gefahr, dass das Passwort durch Ausprobieren ermittelt wurde, um illegal Zugang zum System zu erhalten. Solche Vorfälle sind dem IT-Personal zu melden. Vergisst eine IT-Nutzerin oder ein IT-Nutzer ihr bzw. sein Passwort, hat sie bzw. er beim IT-Personal ohne vorheriges Ausprobieren das Zurücksetzen zu veranlassen, da ansonsten eine temporäre Sperrung des Zugangs droht.	Verantwortlich für die Initiierung: CIO, Bereichsleitung Verantwortlich für die Umsetzung: IT-Nutzerinnen und -Nutzer Empfehlungen zur Gestaltung der Passwörter werden im Intranet der Universität unter https://www.uni-erfurt.de/mitarbeiterservice/mein-arbeitsplatz/it-service/it-sicherheit/ bereitgestellt. Spezielle Regelungen und Hinweise für Zertifikate findet man im Intranet der Universität auf der Seite https://www.uni-erfurt.de/mitarbeiterservice/mein-arbeitsplatz/it-service/it-sicherheit/

Richtlinientext	Erläuterungen und Hinweise
### 5.8 Netzzugang Der Anschluss von Systemen an das Datennetz der Universität Erfurt hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Switches, Hubs o. ä.) sowie die eigenmächtige Einbringung aktiver und passiver Netzwerkkomponenten (z.B.: WLAN-Router) ist unzulässig. Ausnahmen darf nur das URMZ in Absprache mit der Bereichsleitung und ggf. mit der/dem Datenschutzbeauftragten einrichten. Das Netz wird durch geeignete Maßnahmen geschützt, die nicht umgangen werden dürfen.	Verantwortlich für die Initiierung: CIO, Bereichsleitung Verantwortlich für die Umsetzung: IT-Nutzerinnen und -Nutzer
### 5.9 Sichere Netzwerknutzung Der Einsatz von verschlüsselten Kommunikationsdiensten (z.B.: https://) ist nach Möglichkeit den unverschlüsselten Diensten vorzuziehen. Die Übertragung schützenswerter Daten muss verschlüsselt erfolgen oder durch andere geeignete Maßnahmen (z. B. Verwendung isolierter eigener interner Netze – sogenannte VLANs, die keinen Zugang zum Internet haben) gesichert werden.	Verantwortlich für die Initiierung: CIO, Bereichsleitung Verantwortlich für die Umsetzung: IT-Nutzerinnen und -Nutzer, IT-Personal

Richtlinientext	Erläuterungen und Hinweise
5.10 Datensicherung Regelmäßig durchgeführte Datensicherungen sollen vor Verlust durch Fehlbedienung, technische Störungen o.ä. schützen. Grundsätzlich sind Daten auf zentralen Servern zu speichern. Ist die Speicherung auf zentralen Servern vorübergehend oder dauerhaft nicht möglich, sind die der IT-Nutzerinnen und _Nutzer für die Sicherung ihrer Daten selbst verantwortlich, dies gilt besonders bei selbstadministrierten Geräten. Die zentrale Datensicherung durch das URMZ erfolgt für einen Zeitraum von drei Monaten rückwirkend. Die IT-Nutzerinnen und -Nutzer sollten sich über ggf. hiervon abweichende in den jeweiligen Bereichen geltende Regelungen zu Rhythmus und Verfahrensweise für die Datensicherung informieren. Das Speichern schützenswerter Daten auf der Festplatte von Arbeitsplatzrechnern (insbesondere von Notebooks) oder anderer lokaler Speicher- oder Übertragungsmedien und deren Übertragung ist nur zulässig, wenn die für den jeweiligen Schutzbedarf (die für die jeweilige Schutzstufe) erforderlichen Sicherheitsmaßnahmen getroffen wurden. Bei Unsicherheiten ist die/der Datenschutzbeauftragte zu konsultieren. Zur Datenspeicherung in der Cloud ist der DFN-Cloud-Dienst zu verwenden. Der Antrag auf Nutzung durch IT-Nutzerinnen und -Nutzer ist beim URMZ zu stellen. Für die Speicherung, insbesondere von schützenswerten Daten, in der Cloud sind besondere Regelungen zu beachten (u.a. sind schützenswerte Daten immer verschlüsselt abzulegen). Datenträger sind an gesicherten Orten aufzubewahren. Ggf. sind Datenträgertresore zu beschaffen. Weiterhin sind Datenträger zu kennzeichnen, falls die Identifikation des Datenträgers nicht durch ein anderes technisches Verfahren erfolgt. Datenträger müssen beim Transport vor Beschädigungen geschützt sein. Bei schützenswerten Daten ist eine Verschlüsselung erforderlich.	Verantwortlich für die Initiierung: IT-Verantwortlicher Verantwortlich für die Umsetzung: IT-Personal, IT-Nutzerinnen und -Nutzer Hinweise zum Umgang mit schützenswerten Daten finden sich - beispielsweise im Leitfaden zur Basisabsicherung nach IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI), online unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf - auf den Seiten zur IT-Sicherheit an der Universität Erfurt im Intranet unter https://www.uni-erfurt.de/mitarbeiterservice/meinarbeitsplatz/it-service/it-sicherheit/ - sowie auf den Seiten zum Datenschutz an der Universität Erfurt im Internet unter https://www.uni-erfurt.de/datenschutz/

Richtlinientext	Erläuterungen und Hinweise
5.11 Datenlöschung Datenträger mit schützenswerten Daten müssen vor einer Weitergabe an nicht autorisierte Personen physisch gelöscht werden. Das kann mit geeigneten Programmen oder mit einem Gerät zum magnetischen Durchflutungslöschen erfolgen. Auszusondernde oder defekte Datenträger müssen, sofern sie schützenswerte Daten enthalten (oder enthalten haben), vollständig unlesbar gemacht werden. Die betreffenden Datenträger sind im URMZ zur Aussonderung abzugeben. Das URMZ leitet sie einer professionellen Datenvernichtung zu. Weitere Informationen zu Aufbewahrungsfristen und zum Löschen von Datenträgern finden sich in der „Dienstanweisung Datenabfall“ und den zugehörigen Anlagen unter. Darüber hinaus geben das URMZ sowie die Datenschutzbeauftragten der Universität Auskunft.	Verantwortlich für die Initiierung: IT-Verantwortlicher Verantwortlich für die Umsetzung: IT-Personal, IT-Nutzerinnen und -Nutzer Die „Dienstanweisung Datenabfall“ und die zugehörigen Anlagen sind im Intranet der Universität Erfurt unter https://www.uni-erfurt.de/mitarbeiterservice/aktuelles/aktuelle-meldungen/news-detail/news-show/dienstanweisung-datenabfall-rundschreiben-des-praesidenten/ hinterlegt.
5.12 Meldung von Sicherheitsproblemen und Datenpannen Auftretende Sicherheitsprobleme aller Art (Systemabstürze, fehlerhaftes Verhalten von bisher fehlerfrei laufenden Anwendungen, Hardwareausfälle, Eindringen Unbefugter, Manipulationen, Virenbefall u. a.) sind dem zuständigen IT-Personal mitzuteilen. In Abhängigkeit vom Schutzbedarf der betreffenden Anwendung ist jeder schwerwiegende Vorfall vom zuständigen IT-Personal zu dokumentieren und dem IT-Sicherheitsbeauftragten zu melden. Jede Datenpanne (Verlust oder nicht autorisierter Zugriff auf personenbezogenen Daten) muss unverzüglich der/dem Datenschutzbeauftragten angezeigt werden.	Verantwortlich für die Initiierung: Bereichsleitung Verantwortlich für die Umsetzung: IT-Nutzerinnen und -Nutzer, IT-Personal Weitere Informationen zum Erkennen und Erfassen von Sicherheitsvorfällen stellt das Bundesamt für Sicherheit in der Informationstechnik unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/DER/DER_2_1_Behandlung_von_Sicherheitsvorf%C3%A4llen.html bereit.