

Nutzungsbedingungen WZL-IT

für die Lehrstühle Produktionssystematik und Werkzeugmaschinen

Version: 1.09

Stand: 30.08.2024

WZL der RWTH Aachen
Campus Boulevard 30

Andreas Borgmann
Abteilung Organisation und IT
3. Etage PCL Gebäudeteil A
+49 241 80-27599
WZL-Helpdesk@wzl.rwth-aachen.de

Dr. Michael Riesener
Geschäftsführender Oberingenieur PS

Dr. Werner Herfs
Geschäftsführender Oberingenieur WM

[Zitat aus dem Rundschreiben des Kanzlers Manfred Nettekoven vom 6.7.2023:]

*Sehr geehrte Kolleginnen und Kollegen,
die IT-Sicherheit steht weltweit im Fokus. In der jüngeren Vergangenheit hat sich bei zahlreichen Unternehmen, öffentlichen Einrichtungen und auch bei Hochschulen bereits medienwirksam gezeigt, dass unter anderem fehlendes Sicherheitsbewusstsein und daraus resultierende, auch unabsichtliche Handlungen einzelner Personen gefährliche Einfallstore für einen Cyberangriff darstellen können. Das Sicherheitsbewusstsein jedes einzelnen ist wichtig für einen bestmöglichen Schutz vor solchen Angriffen.
Die ZHV stellt ihren Beschäftigten Hard- und Software zur Verfügung, welche die entsprechenden Tätigkeiten der Personen unterstützen. Um einen sicheren IT-Betrieb zu gewährleisten, ist es notwendig, dass alle Nutzenden die IT-Systeme so benutzen, dass keine Schäden an Hardware oder Software entstehen und Daten nur in der dienstlich vorgegebenen Art und Weise verarbeitet werden.
Mit den „**Nutzungsbedingungen ZHV-IT**“ sollen die Beschäftigten unterstützt werden, wesentliche Regelungen für einen sicheren Umgang mit den zur Verfügung gestellten und genutzten IT-Systemen zu verinnerlichen. Unabsichtliche und auf Unwissenheit zurückzuführende Handlungen wie beispielsweise das Verbinden privater Endgeräte mit dem ZHV-Netz oder die Verwendung ungeeigneter Passwörter stellen ein sehr hohes Risiko dar und müssen verhindert werden.
Alle Beschäftigten sind durch die jeweiligen Vorgesetzten auf die Nutzungsbedingungen hinzuweisen. Zukünftig neu in der ZHV beginnende Beschäftigte sind ebenfalls durch die jeweiligen Vorgesetzten zu informieren. Fragen können an helpdesk@zhv.rwth-aachen.de gerichtet werden.*

Die Nutzungsbedingungen gelten ab sofort und sind im Intranet unter <https://intranet.rwth-aachen.de/nutzungsbedingungen-zhv-it> abrufbar.]

Für alle Einrichtungen der RWTH müssen entsprechende Regelungen in den Gremien abgestimmt werden. Da den Instituten diesbezüglich aktuell noch keine verbindlichen Handreichungen der RWTH vorliegen, gelten bis auf Weiteres die im Folgenden formulierten „**Nutzungsbedingungen WZL-IT**“. Diese basieren im Wesentlichen auf den o.g. ‚Nutzungsbedingungen ZHV-IT‘. An bestimmten Stellen (insbesondere im Kapitel „Dateiablage“) wurden die Regelungen für die Lehrstühle für Produktionssystematik und für Werkzeugmaschinen nochmals präzisiert.

Die „**Nutzungsbedingungen WZL-IT**“ gelten ab sofort und sind im Handbuch unter <http://handbuch.wzl.rwth-aachen.de/cms/handbuch/de/z-edv.htm> abgelegt.

Inhaltsverzeichnis

1 Einführung	4
2 Bereitstellung von WZL-IT-Equipment.....	4
3 Umgang mit Hard- und Software.....	4
4 Meldung von Störungen	5
5 Zugriffsschutz.....	6
6 Erhalt und Entzug Berechtigungen	6
7 Wechseldatenträger	7
8 Dateiablage.....	7
9 Elektronische Signaturen.....	10
10 Umgang mit dienstlichen Daten / Datenschutz.....	10
11 Verbindungen mit dem RWTH-Netzwerk.....	11
12 Aktualisierungen / Updates.....	11
13 Sicherer Zugang zu Systemen / Passwörter.....	12

1 Einführung

Um einen sicheren IT-Betrieb zu gewährleisten, ist es notwendig, dass Nutzende die IT-Systeme so benutzen, dass keine Schäden an Hardware oder Software entstehen und Daten nur in der dienstlich vorgegebenen Art und Weise verarbeitet werden. Die allgemeinen Regeln für die Nutzung der WZL-IT-Systeme sind deshalb im vorliegenden Dokument niedergeschrieben.

Dieses Dokument gilt für alle Nutzerinnen und Nutzer von IT-Ressourcen (Soft- und Hardware), die vom WZL bereitgestellt und von der WZL-IT verwaltet / betreut werden.

2 Bereitstellung von WZL-IT-Equipment

Die WZL-EDV-Abteilung beschafft und pflegt alle für den Dienstbetrieb notwendige Hard- und - Software. Der WZL-EDV-Abteilung obliegt dabei unter anderem die Aufgabe, den lizenzrechtlich einwandfreien Einsatz von dienstlich zu nutzender Software sicherzustellen.

Bei Fragen zum Thema WZL-IT wenden Sie sich daher per Helpdesk-Ticket, per Mail an wzl-helpdesk@wzl.rwth-aachen.de oder telefonisch unter 80-27599 an die Mitarbeitenden der WZL-EDV-Abteilung.

3 Umgang mit Hard- und Software

Dienstlich überlassene Hardware der WZL-IT ist stets sorgsam zu behandeln. Es ist darauf zu achten, dass die Hardware nicht durch mechanische, stoffliche oder thermische Einflüsse zu Schaden kommt.

Für mobile Endgeräte sind entsprechende Schutzhüllen zu nutzen. Notebooks sind zum Transport in die dienstlich gelieferten Transporttaschen zu verpacken. Die Nutzung privater Transporttaschen, Rucksäcke etc. ist gestattet, sofern ein gleichwertiger Schutz gewährleistet wird.

Standort- / Hauptbenutzerwechsel von WZL-Hardware sollen stets vom WZL-Helpdesk durchgeführt werden, sind im Vorfeld aber zumindest mit diesem abzustimmen. Weiterhin ist dienstliche Hardware vor Diebstahl zu schützen. Sollte es dennoch zu einem Diebstahl kommen, ist dieser unverzüglich dem WZL-Helpdesk zu melden.

Auf dienstlichen Endgeräten, welche vom Helpdesk der WZL-IT verwaltet werden, darf nur von der WZL-IT freigegebene Software betrieben werden. Die allgemeinen Lizenzbestimmungen für dienstliche Software sind stets einzuhalten. Bestehen Zweifel an der legalen Nutzung einer Software, so ist umgehend das WZL-Helpdesk zu kontaktieren.

Von der WZL-IT zur Verfügung gestellte Standardsoftwareprodukte werden per Softwareverteilung automatisch installiert und aktualisiert. Die Installation weiterer Softwareprodukte, die im WZL-Softwareportfolio zur Verfügung stehen, kann ggfs. vom Nutzenden selbst initiiert oder per Ticket im WZL-Helpdesk veranlasst werden. Anderweitige Änderungen der Softwareausstattung oder der Endgerätehardware sind per Helpdesk-Ticket bei der WZL-IT zu beantragen.

Installationen und Deinstallationen von Software werden grundsätzlich nur durch die WZL-IT bzw. vom

WZL-Helpdesk durchgeführt. Eine eigenmächtige Installation / Deinstallation durch die Nutzenden ist nicht zulässig.

Für neue Beschäftigte erfolgt die Benutzerkontenerstellung und die Bereitstellung der ‚IT-Grundausrüstung‘ im Rahmen des WZL-Onboarding-Prozess. Die dazu nötigen Informationen, die über die vom WZL-Personalbüro bereitgestellten Daten hinausgehen, werden vom Abteilungsleiter oder Obergeringenieur mit dem nötigen Vorlauf als formloses Ticket im WZL-Helpdesk eingereicht.

4 Meldung von Störungen

IT-Systemverhalten, welches von der anwendenden Person nicht erwartet wurde und ihrem Verständnis nach ein Fehler oder eine Störung darstellen könnte, ist dem WZL-Helpdesk unmittelbar zu melden, sofern dieses nicht bereits durch eine entsprechende Störungsmeldung der WZL-IT oder durch die Auflistung auf der [Störungsseite des ITC der RWTH Aachen](#) als ‚bekannt‘ gilt.

Bei der Kommunikation einer Störung an das WZL-Helpdesk ist darauf zu achten, so genau wie möglich zu beschreiben, wie und wann es zur Störung kam oder wie sie entdeckt wurde. Wenn möglich und sinnvoll, sind Screenshots mitzusenden.

Störungsmeldungen erfolgen bevorzugt direkt als Ticket im **WZL-Ticket-Tool** oder **per E-Mail** an wzl-helpdesk@wzl.rwth-aachen.de. Sollte beides nicht möglich oder nicht sinnvoll sein, so kann die **Störung telefonisch** unter **0241-80-27599** gemeldet werden.

Die Meldung hat unmittelbar zu erfolgen, um evtl. Folgeschäden zu vermeiden. Davon ausgenommen sind bereits bekannt gemachte Störungen, Fehler oder Nicht-Verfügbarkeiten.

Anweisungen zur Behebung einer Störung und zur Schadensbegrenzung sind unverzüglich zu befolgen!

Wenn eine Störung Relevanz für andere Anwenderinnen und Anwender oder Hochschulbereiche außerhalb des WZL hat, informiert die WZL-IT die jeweils zuständige(n) Abteilungen des Dezernats 5 (Organisation und IT) und des ITC der RWTH Aachen.

5 Zugriffsschutz

- Die genutzten IT-Systeme des WZLs sind stets vor unberechtigtem Zugriff zu schützen.
- Berechtigungen sind i.d.R. personenbezogen vergeben.
- Es ist nicht gestattet, andere Personen mit den eigenen Benutzerdaten arbeiten zu lassen.
- Endgeräte sind bei Nichtbenutzung / Verlassen des Arbeitsplatzes zu sperren.
- Bei Windows-Geräten ist eine Sperrung gegen unberechtigten Zugriff durch die Tastenkombination (Windows-Taste) + L (wie Lock) möglich.
- Es ist empfehlenswert, einen Bildschirmschoner mit automatischer Sperrung und einer nicht zu langen Inaktivitätsfrist zu aktivieren.

6 Erhalt und Entzug Berechtigungen

Die Erteilung von Zugriffsrechten auf WZL-IT-Systeme erfolgt i.d.R. durch eine von drei unterschiedlichen Methoden:

- Berechtigungen über institutseigene Benutzerverzeichnisse (Windows-AD ,WZL-RWTH' und HCL Domino Benutzerverzeichnis ,WZL-Benutzerverzeichnis')
- Berechtigungen aus der Rollenverwaltung des Identity-Managements der RWTH oder
- Individuelle Berechtigungen (Spezialsoftware)

Berechtigungen aus der Rollenverwaltung der WZL-Benutzerverwaltung oder des Identity-Managements der RWTH finden meist dort Anwendung, wo Zugriffsberechtigungen auf RWTH-Ressourcen in Abhängigkeit von der Lehrstuhl- bzw. Abteilungs- oder Einrichtungszugehörigkeit benötigt werden.

Die mit der Rollenverwaltung beauftragten Mitarbeitenden der jeweiligen Hochschuleinrichtung

- mit EDV-/IT-Bezug über die WZL-IT und mit
- Buchhaltungsbezug über die Personalabteilung in der WZL-Buchhaltung 1

können die Berechtigungen vergeben, ohne dass die Berechtigungsadministration des jeweiligen Zielsystems im konkreten Fall tätig werden muss. Wichtig ist, dass Rollen immer nur in Abstimmung mit der Lehrstuhlleitung vergeben werden dürfen. Der Entzug der jeweiligen Rolle erfolgt ebenfalls durch die Rollenverwalter – oder durch Ablauf einer Rollenbedingung.

Individuelle Berechtigungen in WZL-IT-Systemen oder Zugriffsrechte auf spezifische HCL-Datenbanken müssen per Helpdesk-Ticket bei der WZL-IT beantragt werden. Eine „Selbstberechtigung“ ist nicht vorgehen.

Individuell vergebene Berechtigungen müssen auch individuell zurückgenommen werden – zum Beispiel, wenn Beschäftigte die Hochschuleinrichtung verlassen oder die Tätigkeit, für die die Berechtigung benötigt wurde, nicht mehr ausüben. Hierfür ist ebenfalls ein Ticket an das WZL-Helpdesk erforderlich.

WZL-spezifische Nutzungsberechtigungen erlöschen spätestens mit Beendigung der WZL-Anstellung.

7 Wechseldatenträger

Wechseldatenträger sind leicht transportierbare und über Schnittstellen an Computer anschließbare Datenträger mit digitalen Daten. Dazu gehören neben reinen Datenträgern wie externen Festplatten, USB-Sticks, Speicherkarten, CDs und DVDs auch smarte IOT-Geräte wie Kameras, Messsystemen, IPCs und andere Geräte, die über interne Datenspeicher verfügen.

Die Nutzung von Wechseldatenträgern und / oder smarten IOT-Geräten an mehreren Computern stellt grundsätzlich ein potenzielles Sicherheitsrisiko für IT-Systeme dar und „sollte“ wenn möglich vermieden werden. Hier gilt ganz bewusst „sollte“, da dieser Weg zum Datenaustausch im dienstlichen Kontext teilweise nicht oder nur äußerst aufwendig zu ersetzen ist. Alternative Wege des Datentransfers wie WZL-Interne Netzlaufwerke, GIGAMOVE, SCIEBO, oder (bei kleinen Datenmengen !!) auch E-Mail sind stets zu bevorzugen, wenn dem keine anderen (datenschutz- bezogenen) Bedenken im Wege stehen. Smarte IOT-Geräte und/oder Wechseldatenträger sind nur zu verwenden, wenn ein Anschluss oder Datenaustausch auf anderem Wege nicht möglich ist.

Es dürfen nur Datenträger an die dienstlichen Endgeräte angeschlossen werden, deren Quelle bekannt und vertrauenswürdig ist. Die installierte Anti-Virensoftware (derzeit Sophos) kann und soll zum Prüfen vom Wechseldatenträgern verwendet werden. Sofern die Quelle eines notwendigerweise zu verbindenden Wechseldatenträgers unsicher erscheint, ist vorab Kontakt zum WZL-Helpdesk aufzunehmen, um eine sichere Überprüfung durchzuführen.

Defekte Wechseldatenträger werden über die WZL-IT fachgerecht und datenschutzkonform entsorgt.

8 Dateiablage

Bedingt durch zahlreiche Digitalisierungsprojekte der vergangenen Jahre, wie auch durch den allgemeinen Fortschritt der Informationstechnologie, gibt es mittlerweile zahlreiche Möglichkeiten, Dateien von einem lokalen Endgerät aus zu speichern. Allgemein lässt sich sagen, dass bei der Auswahl der jeweiligen Dateiablage insbesondere Datensicherheit, Datenschutz, Aspekte der Zusammenarbeit und nachrangig natürlich auch der persönliche Komfort zu berücksichtigen sind.

Im WZL stehen **für die Dateiablage in der Regel die Netzlaufwerke W:\, U:\, T:\ und L:** zur Verfügung. Die auf diesen Laufwerken abgelegten Daten werden innerhalb des WZLs gespeichert und täglich zentral für beide Lehrstühle gesichert. Auch sensible Daten können hier unter Beachtung der entsprechenden Berechtigungsstrukturen abgelegt werden.

Das **Laufwerk W:** beherbergt WZL-weit relevante Daten und die über die zentrale „**WZL-Projektabwicklung**“ verwalteten WZL-Projektverzeichnisse. Der Datenzugriff erfolgt gemäß der Zugriffsregelungen für die unterschiedlichen Datenbereiche.

Laufwerk L: beinhaltet **lehrstuhlspezifische Daten**. Zugriff ist nur für Lehrstuhlangehörige möglich.

Auf dem **Laufwerk U:** sollen / dürfen **persönliche Dateien und Konfigurationsdaten** der Mitarbeitenden gespeichert werden. Zugriff ist jeweils nur für die Mitarbeitenden selbst möglich. Daher hier bitte keine Projektdaten ablegen!

Für die gemeinsame Datenablage und den Datenaustausch im **persönlichen Team** steht jedem fest angestellten Mitarbeitenden außerdem das **Laufwerk T:** zur Verfügung. Hier haben automatisch alle studierenden Mitarbeitenden und der User selbst Zugriff.

Darüber hinaus besteht die Möglichkeit, **Cloudspeicher** zu nutzen, **solange nicht mit personenbezogenen Daten gearbeitet wird**.

Dabei wird zwischen **SCIEBO**, **OneDrive** und sonstigen Angeboten zu unterscheiden.

- **SCIEBO** ist ein Cloudspeicher, der nur öffentlichen Einrichtungen des Landes NRW zur Verfügung steht. Die Daten werden DSGVO-konform abgelegt und verbleiben an Speicherstandorten in NRW. SCIEBO kann daher für **die Ablage und Bearbeitung von Forschungsdaten** genutzt werden, sofern **keine bilateralen Vereinbarungen mit etwaigen Forschungspartnern** bestehen, die dies untersagen. Die Nutzung von **SCIEBO** hat nach den WZL-Regeln für die Nutzung dieses Angebots zu erfolgen.
(Siehe WZL Handbuch)
- **OneDrive** gewinnt mit der Einführung von **M365** an Bedeutung. Es ist als Microsoft-eigener Cloud-Dienst tief in M365 integriert. Daten können aktuell nicht datenschutzkonform (DSGVO) gespeichert werden. **Die Ablage von personenbezogenen und/oder sensiblen Informationen (wie zum Beispiel Dokumenten, die in Drittmittelprojekten entstehen oder ausgetauscht werden sollen) ist daher auch im RWTH-Tenant nicht statthaft!** Bei der Nutzung von projektbezogenen Tenants, die von Projektpartnern bereitgestellt werden, dürfen ausschließlich projektbezogene Daten gespeichert bzw. abgelegt werden.
- **Andere Cloudspeicher-Anbieter (Dropbox, Google-Drive, etc.) sind im RWTH-Dienstgeschäft von der Nutzung ausgeschlossen!**
Ausnahmen gelten für Cloudspeicher, die im Rahmen öffentlicher Projekte oder im Rahmen bilateralen Projekte von Projektpartnern explizit für das Projektgeschäft bereitgestellt und zur Nutzung freigegeben wurden. Hier dürfen Projektunterlagen abgelegt werden. **Darüber hinaus gilt aber ein Verbot ausschließlich RWTH-interne Daten in diesen Bereichen abzulegen!**

Abschließend ein Überblick über die erwähnten Ablagemöglichkeiten:

<p>1. Speicherung auf dem lokalen Endgerät</p> <p>Nicht empfohlen, nur für persönliche, temporäre Dateien sinnvoll</p> <ul style="list-style-type: none"> - einfache Ablage, schnell (z.B. Messdatenerfassung) - Kein zentrales Backup - Zugriff nur auf diesem Endgerät
<p>2. Speicherung auf den WZL-Netz-Laufwerken T:, W: und L:</p> <p>Ort für die Standard-Dateiablage am WZL // Speicherplatz wird über Projektabwicklung geregelt</p> <ul style="list-style-type: none"> - Abteilungsstrukturen nutzbar, auch einheitenübergreifende Strukturen möglich - unter Berücksichtigung der Berechtigungsstruktur auch für sensible / geschäftskritische Daten geeignet - Zugriff durch andere Teammitglieder (Zusammenarbeit / Vertretung) - zentrales Backup
<p>3. Speicherung auf dem Netz-Laufwerk U:</p> <ul style="list-style-type: none"> - Ablage sehr persönlicher Daten, z.B. Nutzerzertifikate, Verträge, persönliche dienstl. Dokumente, pers. Konfigurationsdateien - zentrales Backup - Geringe Speicherplatz-Quotierung (aktuell initial: 5GB/25GB je nach Anstellungsverhältnis)
<p>4. Speicherung in SCIEBO (Cloudspeicher)</p> <ul style="list-style-type: none"> - gemeinsamer Cloudspeicher der NRW-Hochschulen (3 Speicherstandorte in NRW) - Teilen / Zusammenarbeit möglich (innerhalb & außerhalb der NRW-Hochschulen) - Primär für den Austausch und die gemeinsame Bearbeitung von Forschungsdaten gedacht - Synchronisation in Windows möglich (Softwarepaket s. WZL Software Portfolio) - Daten verlassen die RWTH - nicht für personenbezogene oder sehr sensible Daten (wie z.B. Daten aus bilateralen bzw. Drittmittel-Projekten) ausgelegt - kein Backup, nur Versionierung <= 6 Monate - Im Falle von Zugriffsproblemen oder Datenverlust ist kein direkter Zugriff über WZL-IT möglich
<p>5. Speicherung in OneDrive (Cloudspeicher)</p> <ul style="list-style-type: none"> - Integriert in M365 - Teilen möglich (auch mit Externen) - Daten verlassen die RWTH, aktuell keine DSGVO-konforme Speicherung - Verbot, personenbezogene oder sehr sensible Daten von Projektpartnern oder aus der RWTH hier abzulegen - Kein zentrales Backup
<p>6. Speicherung in anderen Cloud-Diensten</p> <ol style="list-style-type: none"> Dienstliche Daten der RWTH dürfen nicht in anderen Cloud-Speichern abgelegt werden Daten, die im Rahmen von Projektergebnissen aus Drittmittelprojekten heraus entstehen, dürfen in vom Auftraggeber frei gegebenen Cloud-Diensten abgelegt werden

9 Elektronische Signaturen

Aktuell können in der Hochschule einfache und fortgeschrittene elektronische Signaturen verwendet werden.

Um die Sicherheit und den Schutz von E-Mails innerhalb der RWTH zu verbessern, werden Nutzerzertifikate angeboten und der Einsatz dieser Zertifikate hochschulweit empfohlen. Mit den Zertifikaten lassen sich fortgeschrittene elektronische Signaturen erzeugen. Die Zertifikate bieten zum Beispiel die Möglichkeit, E-Mails zu signieren und zu verschlüsseln. Sie können sowohl für persönliche E-Mailadressen als auch für funktionale E-Mailadressen beantragt werden. Bei der Beantragung und Einbindung eines Nutzerzertifikats unterstützt das Helpdesk. Nach der erfolgreichen Einbindung eines Nutzerzertifikats besteht die Möglichkeit, E-Mails standardmäßig digital signiert zu versenden. Dies ist im Mail-Client an dem entsprechenden Signatur-Kennzeichen zu erkennen. Eine digitale Signatur stellt die Integrität von Inhalten und die Authentizität der absendenden Person sicher. Das bedeutet, dass die E-Mail auf dem Weg von der absendenden zur empfangenden Person nicht verändert wurde und dass der Empfänger darauf vertrauen kann, dass die E-Mail auch tatsächlich von der absendenden Person stammt.

Darüber hinaus besteht die Möglichkeit, E-Mails mit besonders schützenswertem Inhalt, bspw. Personalinformationen oder sensiblen Informationen, zu verschlüsseln. Damit kann sichergestellt werden, dass nur die empfangende Person den Inhalt der E-Mail lesen kann. Zu erkennen ist eine verschlüsselte E-Mail an dem entsprechenden Hinweis im Mail-Kopf. Für eine Verschlüsselung mittels Nutzerzertifikat ist es notwendig, dass auch die adressierte E-Mailadresse über ein solches Zertifikat verfügt. Empfehlenswert ist die Einbindung eines entsprechenden Adressbuchs im Mail-Client. Das IT Center gibt Hinweise zur Einbindung und Nutzung eines Adressbuchs für die fortgeschrittenen Signaturen des DFN /Géant.

Für die **WZL-User** wird ein flächendeckender Einsatz der Zertifikate sowohl für Beschäftigte als auch für funktionale E-Mailadressen angestrebt. Bei der Übermittlung personenbezogener oder sensibler Daten ist eine Verschlüsselung zwingend erforderlich. Das WZL-Helpdesk unterstützt Mitarbeitende des WZL bei der Beantragung und Einbindung von Nutzerzertifikaten und steht auch für weitere Fragen rund um das Thema Zertifikate zur Verfügung.

Weitere Informationen unter: <https://mss.zhv.rwth-aachen.de/SPS/Portal/E-Mail-Zertifikate>
(Achtung: Änderungen im Herbst 2023, ggfs. andere Doku & Links)

10 Umgang mit dienstlichen Daten / Datenschutz

Es gelten die gesetzlichen Regelungen des Datenschutzes. Dienstliche Daten dürfen den mit der Verarbeitung betrauten Personenkreis nicht verlassen. Insbesondere sind sie vor unberechtigter Einsicht zu schützen.

Es ist zu beachten, dass personenbezogene Daten nur erfasst und verarbeitet werden dürfen, wenn es eine entsprechende Rechtsgrundlage für die Erfassung und Verarbeitung gibt. Sollten in einem anzuwendenden Fachverfahren Zweifel an der Rechtmäßigkeit der Erfassung / Verarbeitung von Daten bestehen, so ist zunächst die jeweilige Einrichtungsleitung zu kontaktieren. Sollte sich der Sachverhalt einrichtungsintern nicht sicher klären lassen, so ist die Stabsstelle Datenschutz der RWTH zu kontaktieren.

Entfällt die Rechtsgrundlage für die Verarbeitung / Speicherung von Daten, so sind diese zu löschen. Dauerhaft nicht mehr benötigte Daten sollten unabhängig von ihrer Sensibilität gelöscht werden, um

Speicherressourcen freizugeben. Die Aufbewahrungsfristen sind dabei zu beachten. Auch hierbei empfiehlt sich eine Abstimmung mit der jeweiligen Einrichtungsleitung, um unterschiedliche Einschätzungen zur Notwendigkeit der Daten zu vermeiden.

11 Verbindungen mit dem RWTH-Netzwerk

Sofern mobile Endgeräte der WZL-IT außerhalb des lokalen Hochschul-Netzes (d.h. in den Dienstgebäuden der RWTH mit entsprechenden Netzwerk-Wandanschlüssen) genutzt werden, ist **nach Möglichkeit das RWTH-VPN zu nutzen**, um den Datenverkehr abzusichern.

Dies gilt insbesondere für Datenverbindungen, die aus dem Ausland hergestellt werden, z.B. bei Auslandsdienstreisen.

Das Verbinden nicht durch das WZL verwalteter Endgeräte, insbesondere aber privater Endgeräte über festinstallierte Netzwerkdosen in den Büros mit dem WZL-Netzwerk ist nicht erwünscht. Nicht dienstliche Endgeräte dürfen nicht – auch nicht zum Laden – an die USB-Anschlüsse von Laptop-Docking-Stationen oder WZL-Rechnern angeschlossen werden.

Ins EDUROAM darf grundsätzlich sowohl private als auch dienstliche Hardware eingebucht werden. Auch private Smartphones oder Tablets können über das EDUROAM eine Verbindung zum Hochschulnetz herstellen. Nutzende sind jedoch verpflichtet, für Aktualität von Betriebssystem und Antivirensoftware auf diesen Geräten zu sorgen. Sofern in einzelnen Bereichen Zweifel über die Zugehörigkeit zu ZHV- oder RWTH-Netz bestehen, ist zur Klärung unser WZL-Helpdesk zu kontaktieren.

12 Aktualisierungen / Updates

Hard- und Software werden stets weiterentwickelt. Es werden Funktionalitäten verändert und hinzugefügt. Regelmäßig werden aber auch Sicherheitslücken entdeckt und geschlossen. Wichtig ist, dass nach dem Entdecken einer Sicherheitslücke eine entsprechende Aktualisierung der Hard- oder Software erfolgt, damit die bekannt gewordene Sicherheitslücke nicht ausgenutzt werden kann und so ein Schaden entsteht.

Bei außereuropäischen Auslandsdienstreisen ist auch die Exportkontrolle zu beachten. Mobile Endgeräte können nicht unbedingt beliebig mitgenommen werden, wenn sich darauf Projektergebnisse aus bilateralen und/oder öffentlich geförderten Projekten befinden. Reisende haben die für Ihre Reise zutreffenden Regelungen vor Reiseantritt zu klären und ggf. Leihgeräte bei der WZL-IT für den Reisezeitraum zu entleihen.

In der WZL-IT wird ein Großteil der Hard- und Software zentral verwaltet. Über die automatische Softwareverteilung werden Updates auf die zentral verwalteten Endgeräte übertragen und installiert. Anforderungen für die Installation und / oder eventuell benötigte Neustarts sind **zu beachten** und **zeitnah** umzusetzen.

Sollte im genehmigten Ausnahmefall dienstliche Hard- oder Software eingesetzt werden, welche nicht zentral verwaltet wird, so ist durch die Nutzenden selbst für eine regelmäßige Aktualisierung zu sorgen. Hard- oder Software ohne aktuellem Updatestand können nicht sicher in der WZL-Umgebung genutzt werden und sind umgehend aus dieser zu entfernen.

13 Sicherer Zugang zu Systemen / Passwörter

Um Systeme vor unberechtigt Zugriff zu schützen, wird heutzutage standardmäßig mit persönlichen Accounts für die Nutzenden gearbeitet. Nutzende müssen sich dann mit bestimmten Informationen (meist Benutzerkennung und Passwort) anmelden / authentifizieren, um entsprechende Berechtigungen wahrnehmen zu können.

Passwörter sind stets geheim zu halten. In Ausnahmefällen (z.B. bei Passwörtern zu Gruppenzertifikaten) kann es erforderlich sein, dass eine abgegrenzte Personengruppe Kenntnis über ein Passwort hat.

Wenn Mechanismen wie Multifaktor-Authentifizierung (MFA) oder One-Time-Passwords (OTP) angeboten werden, dann macht es auf alle Fälle Sinn, diese zu nutzen!

Es ist sehr wichtig, dass Passwörter bestimmte Eigenschaften erfüllen, um ein hohes Maß an Sicherheit zu erreichen. Ein sicheres Passwort sollte möglichst viele der folgenden Eigenschaften erfüllen, wobei zu beachten ist, dass nicht jedes System alle Eigenschaften unterstützt:

- Nicht zu kurz (mit der Länge steigt bei Beachtung weiterer Eigenschaften auch die Sicherheit, , i.d.R. sollten Passwörter heutzutage mindestens 8 Zeichen haben, besser 13 und mehr)
- Enthält Großbuchstaben
- Enthält Kleinbuchstaben
- Enthält Sonderzeichen
- Enthält Zahlen
- Steht nicht vollständig im Wörterbuch
- Namen oder Jahreszahlen sind generell als Passwort nicht empfehlenswert
- Ein Passwort für ein System/Account (also Passwörter nicht mehrfach verwenden)

Grundsätzlich wird ein Passwort nicht dadurch sicherer, dass man es häufig ändert. Eher das Gegenteil ist der Fall. Da aber einzelne der o.g. Eigenschaften durch eine sehr lange Verwendung eines gleichbleibenden Passworts wiederum zu Unsicherheiten führen können, ist in der WZL-IT für den WZL-Account (Windows, HCL etc.) eine Passwortänderung in größeren Zeitabständen empfohlen.

Wichtig: Sollte der Verdacht bestehen, dass ein Passwort unberechtigt einer weiteren Person bekannt geworden sein könnte, so ist das entsprechende Passwort sofort zu ersetzen.

Je mehr der o.g. Eigenschaften Beachtung finden, desto schwieriger wird es, sich die Vielzahl der Passwörter für die tägliche Arbeit zu merken. Deshalb kann auf Wunsch durch das WZL-Helpdesk ein „Passwortsafe“ (aktuell Keepass2) auf dienstlichen Endgeräten installiert werden. Nutzende eines Passwortsafes müssen sich dann nur das Master-Passwort für diesen Safe merken und können alle weiteren Passwörter daraus ablesen oder sogar automatisch in die entsprechenden Anmeldedaten eintragen lassen. Dieses Masterpasswort sollte dann natürlich „schön sicher“ gewählt werden! Charmant ist hier außerdem die Möglichkeit, einen Passwortsafe zwischen mehreren Endgeräten synchronisieren zu können.