Richtlinie „Aufgeräumter Arbeitsplatz“

(security policy for clear desk and clear screen)

Ziel

Das Karlsruher Institut für Technologie (KIT) muss bei der Informationsverarbeitung und -versorgung (IV) eine Vielzahl von gesetzlichen Anforderungen erfüllen. In den Querschnittsthemen Datenschutz und Informationssicherheit sind insbesondere die europäische Datenschutz-Grundverordnung (DS-GVO) und die Verwaltungsvorschrift Informationssicherheit des Landes Baden-Württemberg zu beachten.

Darüber hinaus besteht am KIT selbst ein hoher Anspruch in Forschung und Innovation, Studium und Lehre sowie Administration an die Qualität der IV, um Spitzenforschung, exzellente wissenschaftliche Ausbildung und gute Administration gewährleisten zu können.

Zur Organisation der Informationssicherheit und der Erreichung ihrer Ziele Vertraulichkeit, Integrität und Verfügbarkeit hat das KIT als grundlegende Dokumente die Ordnung für die digitale Informationsverarbeitung und Kommunikation (IuK-Ordnung)[1], das IV-Governance-Framework[2], die IT-Sicherheitsleitlinie[3] und ein IT-Sicherheitskonzept[4] in Kraft gesetzt.

Diese Richtlinie unterstützt die Beschäftigten, indem sie Maßnahmen beschreibt, wie personenbezogene, vertrauliche oder persönliche Informationen auf Papier oder IT-Geräten im persönlichen oder öffentlichen Arbeitsraum zu schützen sind, wenn diese nicht in Verwendung oder unbeaufsichtigt sind.

Für alle anderen am KIT tätigen Personen gilt die Richtlinie sinngemäß.

Version

Version	Datum	Bearbeitet
0-15	08.02.2021	Burgdorf

[1] https://www.kit.edu/downloads/AmtlicheBekanntmachungen/2013_AB_036.pdf
[2] https://www.stab.kit.edu/downloads/de_IV-Gov-Framework.pdf
[3] https://www.stab.kit.edu/downloads/KIT_IT-Sicherheitsleitlinie_2009.pdf
[4] https://www.stab.kit.edu/downloads/KIT_IT-Sicherheitskonzept_2018.pdf

Inhaltsverzeichnis

1 Grundsatz des aufgeräumten Arbeitsplatzes und Begriff „Informationen“

1.1 Grundsatz des aufgeräumten Arbeitsplatzes

Die Beschäftigten des Karlsruher Instituts für Technologie (KIT) schützen bei Ausführung ihrer Aufgaben personenbezogene, vertrauliche oder persönliche Informationen vor unbefugter Kenntnisnahme, Diebstahl oder Gebrauch.

1.2 Informationen

Informationen können auf Papier gedruckt oder in elektronischer Form, oftmals auch Daten genannt, oder in sonstiger Form oder im „Kopf“ vorliegen.

1.3 Personenbezogene Informationen

Personenbezogene Informationen oder sog. personenbezogene Daten beziehen sich auf eine identifizierte oder identifizierbare natürliche Person[5]. Sie sind ein Spezialfall der vertraulichen Informationen.

1.4 Vertrauliche Informationen

Vertrauliche Informationen sind dienstliche Informationen des KIT, die nur für einen eingeschränkten Personenkreis und insbesondere nicht für die Öffentlichkeit bestimmt sind[6]. Die Vertraulichkeit kann sich aufgrund einer ausdrücklichen Kennzeichnung als „vertraulich“ oder aus der Natur der Sache heraus ergeben; insbesondere bei mündlichen oder visuellen Informationen sollte die Vertraulichkeit schriftlich bestätigt werden.

1.5 Persönliche Informationen

Persönliche Informationen sind Informationen der Beschäftigten, die im Kontext des Arbeitsverhältnisses entstehen[7].

[5] Beispiele für personenbezogene Informationen: Stammdaten von Beschäftigten oder Studierenden, Bewerber-/Studienverlaufs-/Prüfungsdaten, Forschungsdaten mit Bezug zu Probanden, Benutzername, IP-Adresse.
[6] Beispiele für vertrauliche Informationen: geistiges Eigentum wie unveröffentlichte Forschungsergebnisse, urheberrechtlich geschützte Inhalte oder Patente; geschäftskritische Informationen wie strategische Konzepte, Finanzdaten oder Vertragsdaten, die nur wenigen bekannt sind; sonstige interne Daten sowie Daten, die das KIT von Dritten erhalten hat.
[7] Beispiele für persönliche Informationen: Aufzeichnungen über das Mitarbeitergespräch oder Zielvereinbarungen, Schriftverkehr mit der Personalabteilung, dem Betriebsarzt oder dem Personalrat.

2 Umsetzung und Sensibilisierung

Die jeweilige Leitung einer Organisationseinheit des KIT unterstützt die Umsetzung dieser Richtlinie, indem sie ihre Beschäftigten auf diese aufmerksam macht, regelmäßig zum aufgeräumten Arbeitsplatz und den Umgang mit Informationen sensibilisiert sowie erforderlichenfalls ergänzende Maßnahmen für die Organisationseinheit trifft.

Sofern der jeweiligen Leitung wiederholte Verstöße gegen die Richtlinie bekannt werden, beispielsweise wenn diese aus Unachtsamkeit oder aufgrund hoher Arbeitsbelastung geschehen, kontrolliert sie die Einhaltung in der Organisationseinheit und leitet Maßnahmen nach Nummer 2 Satz 1 ein.

Bei wiederholten, grob fahrlässigen oder vorsätzlichen Verstößen gegen die Richtlinie setzt sich die jeweilige Leitung mit der Organisationseinheit Personalservice (PSE) in Verbindung, um die Möglichkeit arbeitsrechtlicher bzw. disziplinarischer Maßnahmen zu besprechen.

3 Den Arbeitsplatz aufgeräumt hinterlassen

3.1 Türen und Fenster verschließen

Bei Arbeitsunterbrechungen, bei denen der Arbeitsplatz unbeaufsichtigt gelassen wird, verschließen die Beschäftigten Türen zu ihrem Arbeitsraum und zusätzlich Fenster, wenn diese von außen einfach zugänglich sind.

Nach der Arbeit verschließen die Beschäftigten Türen und Fenster.

Sofern sich mehrere Beschäftigte einen Arbeitsraum teilen, gilt das in Nummer 3.1 Satz 1 und Nummer 3.1 Satz 2 genannte, wenn die oder der letzte Beschäftigte diesen verlässt.

3.2 Einsicht in Informationen begrenzen

Die Beschäftigten achten darauf, dass bei der Bearbeitung von Aufgaben ausschließlich sie oder ebenfalls an der Bearbeitung beteiligte Beschäftigte Einsicht oder Zugriff auf personenbezogene, vertrauliche oder persönliche Informationen haben, mit denen sie arbeiten und die in Dokumenten vermerkt oder auf Datenträgern gespeichert sind[8].

Teilen sich Beschäftigte einen Arbeitsraum, so berücksichtigen sie das in Nummer 3.2 Satz 1 genannte auch gegenüber Beschäftigten, die andere Aufgaben bearbeiten.

Das in Nummer 3.2 Satz 1 genannte beachten die Beschäftigten in besonderem Maße gegenüber nicht zur Arbeitsgruppe bzw. zum Zuständigkeitsbereich gehörenden Personen.

3.3 Öffentliche Räume aufgeräumt hinterlassen

In öffentlichen Räumen, beispielsweise in Hörsälen, Seminarräumen, Poolräumen, Zeichensälen oder Konferenz- und Besprechungsräumen, achten die Beschäftigten darauf, dass keine Dokumente, IT-Geräte oder Datenträger mit personenbezogenen, vertraulichen oder persönlichen Informationen zurückgelassen werden und die Türen und Fenster wieder geschlossen werden.

3.4 Dokumente entsorgen

Die Beschäftigten entsorgen Dokumente oder Datenträger, die personenbezogene, vertrauliche oder persönliche Informationen enthalten, nicht im normalen Müll- / Papierkorb, sondern in dafür bereitgestellten Dokumenten- oder Datenträgermüllbehältern oder –zerkleinern[9].

[8] Z. B. richtiges Positionieren des PC-Bildschirms oder Verwenden von Mappen oder Aktendeckeln, leises Telefonieren, Benutzung von oder Verschluss in Rollcontainern und Schränken.
[9] Siehe Abfallratgeber unter https://www.fm.kit.edu/952.php

3.5 Schlüssel, KIT-Card, Token

Die Beschäftigten verwahren die ihnen überlassenen Dienstschlüssel, KIT-Card oder Zwei-Faktor-Token sorgfältig. Ein Verlust ist unverzüglich der ausgebenden Stelle sowie der oder dem jeweiligen Vorgesetzten mitzuteilen.

3.6 Multifunktions- oder Kopiergeräte

Bei der Verwendung von Multifunktions- oder Kopiergeräten entnehmen die Beschäftigten die ausgedruckten Dokumente oder die Scan-Vorlagen mit personenbezogenen, vertraulichen oder persönlichen Informationen unmittelbar nach dem Drucken bzw. Einscannen aus dem Gerät oder verwenden eine Funktion wie „Vertrauliches Drucken“ oder „Sicheres Drucken“.[10]

3.7 Datenträger in IT-Geräten sicher löschen vor Weiter- oder Rückgabe

Vor einer Aus-, Weiter- oder Rückgabe von IT-Geräten wie PC-Arbeitsplatz, Laptop, Smartphone, Festplatte oder sonstigen mobilen Datenträgern werden diese durch die Beschäftigten oder die IT-Beauftragten sicher gelöscht[11], so dass der Nachnutzende keine personenbezogenen, vertraulichen oder persönlichen Informationen des Vornutzenden mehr lesen kann.

Nicht löschbare Datenträger sind insbesondere vor der Abgabe von Altgeräten an Personen oder Einrichtungen außerhalb des KIT aus diesen auszubauen und ebenso wie defekte Datenträger als sogenanntes Datenschutzmaterial über die Abfallwirtschaftszentrale zu entsorgen.

4 Den IT-Arbeitsplatz „aufgeräumt“ hinterlassen

4.1 Verwendung persönlicher Benutzerumgebungen

Die Beschäftigten verwenden auf IT-Geräten persönliche Benutzerprofile und teilen diese nicht mit anderen Beschäftigten. Vor der Verwendung des IT-Geräts durch eine/n anderen Beschäftigte/n sind geöffnete Programme zu schließen und das Benutzerprofil zu wechseln.[12] Zu Ausnahmen bei Industriesteuerungen vgl. unter Nummer 4.3.

4.2 Persönliches Benutzerkonto und Schutz des persönlichen Passworts

Die Beschäftigten erhalten ein persönliches Benutzerkonto, sogenanntes KIT-Benutzerkonto oder KIT-Account, dem insbesondere ein Benutzername und ein Passwort zugeordnet sind, um sich an IT-Geräten oder Diensten des KIT anzumelden.

Das persönliche Passwort darf nicht weitergegeben werden, siehe § 5 Abs. 2 IuK-Ordnung sowie Passwortrichtlinie[13].

Gleiches gilt für weitere persönliche Benutzerkonten, die geräte- oder dienstlokal eingerichtet werden, oder für Konten, die mit besonderen Rechten, sogenannte Administrator-Konten, versehen sind.

4.3 Industriesteuerungen und Servicekonten

Bei Industriesteuerungen oder ähnlichen Systemen, auf denen keine persönlichen Benutzer-umgebungen oder -konten eingerichtet werden können, bearbeiten die Beschäftigten keine

[10] Bei diesen Funktionen wird ein Druckjob z. B. mit einer zusätzlichen PIN versehen.
[11] Vgl. Altgeräte-Richtlinie unter https://www.evm.kit.edu/downloads/Altgeraete-Richtlinie_Fassung_vom_01.01.2020.pdf; zu Daten auf Festplatten richtig löschen unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node.html bzw. zu Smartphone-Daten löschen unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/Smartphone/Smartphone_Daten_loeschen_node.html bzw. IT-Grundlagenschulung Kap. 3 unter https://www.cert.kit.edu/p/talks/grundlagenschulung.zip
[12] Erläuterung Benutzerprofilwechsel: Die/der bisherige Benutzer/in meldet sich von ihrem/seinem Benutzerprofil ab und die/der neue Benutzer/in meldet sich mit ihrem/seinem Benutzerprofil an.
[13] Abrufbar unter https://www.scc.kit.edu/dienste/4319.php

personenbezogenen, vertraulichen oder persönlichen Informationen und verwenden nicht ihr persönliches Passwort nach Nummer 4.2.

Ein geteiltes Passwort für sogenannte Servicekonten darf nur einem eingeschränkten Personenkreis zugänglich gemacht werden und ist bei Änderung dieses Kreises neu zu setzen.

4.4 Verwendung der Bildschirmsperre

Bei Arbeitsunterbrechungen, bei denen der Arbeitsplatz unbeaufsichtigt ist, oder zum Arbeitsende sperren die Beschäftigten ihre IT-Geräte oder Benutzerkonten[14].

Zusätzlich aktivieren die Beschäftigten auf den von ihnen verwendeten IT-Geräten eine automatische Geräte- oder Bildschirmsperre bei Nichtnutzung. Diese Sperre ist passwort-, PIN- oder Fingerabdruck-geschützt. Die automatische Sperre wird risikobasiert zu den Arbeitsvorgängen bemessen.[15]

Bei IT-Geräten, die neu ausgegeben werden, soll zusätzlich eine Geräte- oder Bildschirmsperre vom zuständigen IT-Beauftragten voreingestellt werden. Bei IT-Geräten, die über einen Verzeichnisdienst des KIT verwaltet werden, soll die Sperre technisch vorgegeben werden. Bei vollverwalteten IT-Geräten wird die Sperre durch das Steinbuch Centre for Computing (SCC) zentral umgesetzt.

4.5 Bildschirmbenachrichtigungen

Die Beschäftigten stellen die Benachrichtigungen des Betriebssystems oder von Apps auf mobilen IT-Geräten, insbesondere auf Smartphones oder Tablets, so ein, dass bei gesperrtem Bildschirm keine personenbezogenen, vertraulichen oder persönlichen Informationen, beispielsweise aus SMS, Instant-Messaging- oder E-Mail-Nachrichten, angezeigt werden[16].

5 Verschlüsselung von IT-Geräten oder Speichermedien

Speichermedien in mobilen IT-Geräten, wie Laptops oder Notebooks, oder andere mobile Speichermedien, wie USB-Festplatten, USB-Sticks, Smartcards oder vergleichbar, auf denen die Beschäftigten personenbezogene, vertrauliche oder persönliche Informationen speichern oder verarbeiten, sind nach dem Stand der Technik vorsorglich bei Geräteausgabe oder nachträglich zu verschlüsseln[17].

Speichermedien in stationären IT-Geräten sind ebenfalls nach Nummer 5 Satz 1 zu verschlüsseln, wenn diese in öffentlichen Räumen aufgestellt sind.

Ausnahmen zu Nummer 5 Satz 1 oder Satz 2 sind im Einzelfall zulässig, allerdings ist ein vergleichbares Sicherheitsniveau herzustellen.

[14] Z. B. mittels Windows-Taste + L (Windows), CTRL + CMD + Q (MacOS) oder STRG + ALT + L (Linux) oder bei Smartphones über Ein/Aus-Taste.
[15] Für normale IT-Arbeitsplätze werden fünf Minuten, für Smartphones oder Tablets eine Minute empfohlen.
[16] Vgl. für iOS (iPhone, iPad) unter https://support.apple.com/de-de/HT201925 bzw. für Android unter https://support.google.com/android/answer/9079661?hl=de
[17] Das SCC bietet im Rahmen der Bereitstellung sicherer PC-Arbeitsplätze die Verschlüsselung von Windows-Arbeitsplätzen mittels Bitlocker-Verschlüsselung an; der Wiederherstellungsschlüssel wird dabei im Active Directory des KIT hinterlegt. Windows-Arbeitsplätze können bei der Erstinstallation oder über die Software-Verteilung oder manuell verschlüsselt werden. Der Erfolg einer Verschlüsselung ist abhängig von der verwendeten Hardware und des verwendeten Betriebssystems; eine Datensicherung vor der Initialisierung der Verschlüsselung ist empfehlenswert. Es beschreibt zusätzlich auf seinen Webseiten die Verschlüsselung für Festplatten in PC-Arbeitsplätzen unter MacOS X und Linux, die Einrichtung eines verschlüsselten mobilen Speichermediums mittels Bitlocker-Verschlüsselung (Windows), die Einrichtung und Verwendung verschlüsselter Container-Dateien, um diese auf Festplatten oder mobilen Speichermedien anzulegen (Windows, MacOS X, Linux), siehe https://www.scc.kit.edu/dienste/13019.php

6 Evaluation

Die Umsetzung und Wirksamkeit der Richtlinie wird alle drei Jahre durch den Informationssicherheitsbeauftragten überprüft.

7 Inkrafttreten und Bekanntgabe

Die Richtlinie tritt am Tag nach ihrem Beschluss durch das Präsidium des KIT in Kraft. Sie wird durch Rundschreiben bekannt gegeben.

Die Organisationseinheiten setzen die Verschlüsselung nach Nummer 5 für neue Geräte unmittelbar und für Bestandsgeräte innerhalb von vier Monaten nach Inkrafttreten um.

Die Richtlinie wurde am 22. Februar 2021 vom Präsidium des KIT beschlossen.