CISO Sprechstunde

01.07.2026

Aktuelles aus der FAU

ISMS-taugliche Dokumentenvorlagen

FAU
Friedrich-Alexander-Universität
Erlangen-Nürnberg

Titel

Dokumenteigenschaften

Titel	Titel
Klassifikation	öffentlich / intern / vertraulich / streng vertraulich
Herausgeber	FAU Erlangen-Nürnberg; Muster-Organisationseinheit
Versionsnummer	Version 0.3 – Entwurf
Stand vom	08.06.2026
Ablageort	Muster-Verzeichnis
Dokumentenverantwortliche	Mia Musterfrau
Freigabedatum	–
Freigabe durch	z.B. Präsident/in
Zielgruppe	z.B. Universitätsangehörige der FAU Erlangen-Nürnberg
Revisionsintervall	1 Jahr
Letzte Revision	–

Mitgeltende Dokumente und Inhalte

Nr.	Dokument	Speicherort / Verweis
1	Muster-Richtlinie	z.B. www.intern.fau.de/informationstechnik-it/regelungen/
2	Anhang	Anhang xx

Änderungshistorie

Version	Datum	Beschreibung	Name
0.1	09.05.2023	Ersterstellung	Mia Musterfrau
0.2	01.03.2026	Layout-Anpassung	John Doe

Inhaltsverzeichnis

Dokumenteigenschaften 1
Mitgeltende Dokumente und Inhalte 2
Änderungshistorie 3
Abkürzungsverzeichnis 5
§ 1 Einführung 6
(1) Zielsetzung 6
(2) Gesetzliche Vorgaben 6
(3) Geltungsbereich 6
§ 1 Methodik 6
§ 2 Rollen und Aufgaben 7
Anhang 8

Sicherheitsvorfall bei Overleaf

https://www.rrze.fau.de/2026/06/overleaf-4/

26. Juni 2026

Sicherheitsvorfall bei Overleaf (Digital Science) [FAU, UKER]

Der Hersteller von Overleaf, Digital Science & Research Solutions Limited, hat am 25.06.2026 einen Sicherheitsvorfall gemeldet, bei dem geschäftliche Kontaktdaten entwendet wurden. Davon betroffen sind potenziell auch Namen, E-Mail-Adressen und Telefonnummern von Mitgliedern der FAU und des Universitätsklinikums Erlangen.

Betroffene Bereiche: Overleaf Online-Dienste und Accounts

Zielgruppe: Beschäftigte und Studierende an der FAU und des Universitätsklinikums Erlangen, die Overleaf nutzen bzw. ein aktives Benutzerkonto haben; unabhängig vom Nutzungsmodell (kostenlos, kostenpflichtige Subscription)

Nach den Angaben des Herstellers sind die Kernprodukte selbst sowie die darin gespeicherten wissenschaftlichen Dokumente und Projektdaten **nicht** betroffen. Passwörter, Zugangsdaten oder Kreditkarteninformationen wurden nach aktuellem Erkenntnisstand nicht kompromittiert.

Erforderliche Verhaltensmaßnahmen für Nutzende

- **Vorsicht bei Phishing:** Es ist mit erhöhter Wachsamkeit auf verdächtige E-Mails oder Zahlungsaufforderungen zu achten, die scheinbar im Namen von Digital Science oder Overleaf versendet werden.
- **Keine Datenweitergabe:** Aufforderungen zur Änderung von Geschäftsdaten oder Kontoverbindungen sind vorab zwingend über offizielle Kanäle zu verifizieren.
- **Kontaktaufnahme im Zweifelsfall:** Unerwartete Nachrichten können vom RRZE geprüft werden (per E-Mail mit der verdächtigen Nachricht im Anhang an abuse@fau.de senden).
- **Aktuelle Informationen:** Der Hersteller aktualisiert den Status fortlaufend unter www.digital-science.com/security-update/.

Lösungen

Umstieg auf Software-Alternativen

Es gibt eine Vielzahl an Apps zur Textverarbeitung, Erstellung von pdf-Dokumenten und Publikation. Das Besondere an der kommerziellen Software Overleaf ist die weit verbreitete Nutzung zur Zusammenarbeit in den Natur- und Technischen Wissenschaften.

LaTeX ist freie Software gemäß den Nutzungsbedingungen von LaTeX Project Public License (LPPL)

LaTeX – die kostenlose Wahl für die professionelle Gestaltung von Texten, Präsentationen und anderen Dokumenten. Als freie und komplett kostenlose Software bietet LaTeX eine Vielzahl an Funktionen und Möglichkeiten, um Dokumente datenschutzkonform lokal zu bearbeiten. Für die kollaborative Bearbeitung im Team können sichere universitäre oder selbst gehostete Cloud-Lösungen verwendet werden.

Exportkontrolle

Iran, Kongo, Libyen, Myanmar, u.a.

Aus aktuellem Anlass: Transfer von Forschungsdaten in ein Embargoland

➔ Kein technisches sondern ein Exportkontroll- und Sanktionsproblem.

Entscheidend ist NICHT der physische Transport, sondern die Frage, ob Technologie oder Software gezielt einem Nutzer zugänglich gemacht wird.

Was du in der Praxis oft NICHT darfst

- Verschlüsselte Cloud-Übertragung für Embargo-Nutzer (FAUBox)
- Zero-Knowledge Cloud-Services im Embargoland anbieten (verschlüsselter Content)
- VPN-/Tunnel-Software bereitstellen (eduVPN mit Wireguard)
- Sichere File-Transfer-Systeme aktiv bereitstellen
- SaaS/Accounts für Nutzer im Embargoland freischalten
- Download-Server gezielt für Embargoländer öffnen

Wenden Sie sich in jedem Fall vorher an die Exportkontrolle der FAU

Betroffener Güterkreis

(https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_embargo.pdf?__blob=publicationFile&v=2):

1. Rüstungsgüter
2. Sonstige Güter
   Embargomaßnahmen können sich aber auch auf jedwede sonstigen Güter erstrecken. Eine abschließende Auflistung der Güter existiert nicht.
   Demzufolge können auch Güter erfasst werden, welche nicht der allgemeinen Exportkontrolle unterfallen, wie z. B. Luxusgüter oder Schlüsselausrüstung für den Energiebereich.

   Darauf hinzuweisen ist, dass der Begriff Güter nicht nur physische Waren, sondern auch **Technologie und Software** umfasst.

Exportkontrolle

Praxis

Was in der Praxis eher erlaubt sein kann

1) Reine „passive Veröffentlichung“ (wichtiger Unterschied)

Wenn Software:

- weltweit öffentlich auf GitHub liegt
- **ohne gezielte Bereitstellung**
- ohne „controlled encryption“ im Sinne der EU-Listen erreichbar

Aber Vorsicht:

Wer aktiv „bereitstellt“ (und z. B. einen User freischaltet), unterliegt schnell dem Exportrecht

2) kein gezielter Export / keine Kontrolle / Beispiel:

- jemand im Embargoland lädt Open Source selbst herunter
- FAU betreibt keine spezielle Infrastruktur für die Person im Embargoland

➔ Vermutlich deutlich weniger problematisch

3) Kommunikation ohne kontrollierte Technologie

- E-Mail ohne spezielle Verschlüsselungstechnologie
- einfache Text-/Dokumentübermittlung ohne „kontrollierte Kryptografie“

Der kritische Punkt: Verschlüsselung, EU-Recht unterscheidet stark:

- problematisch

- TLS Libraries / VPN / E2E encryption / secure file transfer
- alles, was als „controlled cryptography“ gilt

- manchmal Grauzone

- Standard-Open-Source mit „normaler Verschlüsselung“
- abhängig von ECCN / EU-Dual-Use List

Beachte auch immer einen evtl. US-Bezug

SW-Erfassung

geplant

Umfrage zur (freiwilligen) Erfassung von eingesetzter und/oder benötigter SW ist geplant

Organisatorische Voraussetzungen werden aktuell geprüft

Vorabinformation erfolgt rechtzeitig über Newsletter.

Aktuelles aus der Welt

US-Urteil erschüttert das Fundament des transatlantischen Datentransfers

Drei Experten sehen das rechtlichen Kartenhaus droht der Einsturz (heise.de)

Mit der Entscheidung des Obersten Gerichtshofs der USA in der Rechtssache *Trump v Slaughter* (Az. 25–332) hat die konservative Mehrheit der Richter die Unabhängigkeit der Federal Trade Commission (FTC) für verfassungswidrig erklärt.

Was nach einer rein innenpolitischen Debatte über die Machtfülle des US-Präsidenten aussieht, entpuppt sich bei genauem Hinsehen als Sprengsatz für die europäische Digitalwirtschaft.

Denn die vermeintliche Unabhängigkeit der FTC war lange Zeit das rechtliche Fundament, auf dem der Datenverkehr zwischen der EU und den USA ruhte.

Das EU-Vertragsrecht und die Grundrechtecharta schreiben vor, dass die Überwachung des Datenschutzes durch unabhängige Behörden erfolgen muss. Da Drittstaaten ein „im Wesentlichen gleichwertiges" Datenschutzniveau zu garantieren haben, galt diese Pflicht zur Unabhängigkeit auch für die US-Aufsicht.

Desaster mit Ansage für den EU-Datenschutz?

Im aktuellen Angemessenheitsbeschluss der EU, dem heftig umstrittenen EU-US Data Privacy Framework von 2023, beruft sich die EU-Kommission sage und schreibe 259 Mal auf die Kontrollfunktion der FTC. Mit dem neuen Urteil untersteht diese Behörde jetzt jedoch prinzipiell direkt den politischen Weisungen des US-Präsidenten. Die mühsam konstruierte Argumentation, die USA böten unabhängige Aufsicht, dürfte damit über Nacht hinfällig geworden sein.


US-Urteil erschüttert das Fundament des transatlantischen Datentransfers

Der Supreme Court hat die Unabhängigkeit der FTC für verfassungswidrig erklärt. Das droht, dem EU-US Data Privacy Framework die rechtliche Basis zu entziehen.

heise.de bei Google folgen

81

Das Gebäude des US Supreme Court in Washington, DC (Bild: Sunira Moses CC BY-SA 3.0)

Max Schrems, Gründer der Datenschutzorganisation Noyb, sieht die Brüsseler Regierungsinstitution damit in der Pflicht. Da es in den USA schlicht keine unabhängigen Behörden mehr gebe, hat Noyb die Kommission formell aufgefordert, die Angemessenheitsentscheidung für die USA in einem geordneten Prozess aufzuheben.

Schutz von Open Source SW

Neue Allianz

Die Linux Foundation hat gemeinsam mit zahlreichen Tech-Unternehmen und Finanzinstituten die **Initiative Akrites** gestartet. **Ziel ist es, den Umgang mit Sicherheitslücken in wichtiger Open-Source-Software zentral zu koordinieren, sie vertraulich mit den jeweiligen Projektverantwortlichen zu beheben und erst anschließend offenzulegen.** Hintergrund ist die wachsende Sorge, dass moderne KI-Modelle Schwachstellen deutlich schneller finden als bisher und damit den Zeitdruck für Verteidiger erheblich erhöhen.

Zu den Gründungsmitgliedern gehören unter anderem Amazon Web Services, Anthropic, Cisco, Google, IBM, Microsoft, GitHub, Nvidia, OpenAI, Red Hat sowie JPMorganChase, Citi und Vodafone. Die beteiligten Unternehmen wollen Personal, Sicherheitswissen und finanzielle Mittel bereitstellen.

Hintergrund: … leistungsfähige KI-Modelle können große Open-Source-Projekte innerhalb weniger Minuten auf potenzielle Schwachstellen untersuchen.

Kern des Projekts sind ein gemeinsames Security Incident Response Team (SIRT) sowie ein einheitlicher Prozess zur koordinierten Offenlegung von Sicherheitslücken (Coordinated Vulnerability Disclosure, CVD). Die beteiligten Organisationen wollen bestätigte Schwachstellen gemeinsam mit den Upstream-Maintainern beheben, bevor Details veröffentlicht werden.

heise online › Open Source › **Neue Allianz für mehr Open-Source-Schutz**

Neue Allianz für mehr Open-Source-Schutz

Die Linux Foundation und Tech-Giganten starten Akrites, um Open-Source-Sicherheitslücken zentral und vertraulich zu beheben.

heise.de bei Google folgen 3

(Bild: heise medien)

29.06.2026, 12:37 Uhr Lesezeit: 3 Min. | iX Magazin

Von Moritz Förster

Was können wir für Sie tun?

Ihre Fragen?

Ihre Wünsche?