

	Informationssicherheit Allgemeine Nutzungsbedingungen (ANB) für IT- und Datennutzer	Stufe 2 TLP-Green „intern“
Universitätsklinikum Heidelberg	Informationssicherheit / IT-Sicherheit	

Die Gewährleistung von IT-Sicherheit und Informationssicherheit sind wichtige und gesetzlich geforderte Aufgaben des Universitätsklinikums Heidelberg ($\triangleq$ „UK“).

Um IT-Sicherheit und Informationssicherheit erreichen zu können, verfügt das UK über eine Sammlung von Regelungen und Vorgaben ($\triangleq$ „Regelwerk“) der Informationssicherheit. IT- und Informationssicherheit können nur erreicht werden, wenn alle Personen, welche die IT und die Daten des UK nutzen, diese Regelungen und Vorgaben einhalten.

Nicht alle Dokumente aus dem Regelwerk sind für alle Personen relevant. Daher stehen für sie je nach Aufgaben, Rollen oder Nutzung von Arbeitsmitteln jeweils eigene Dokumente mit Regelungen und Vorgaben zur Verfügung.

Die vorliegenden „Allgemeinen Nutzungsbedingungen (ANB) für UK IT- und Datennutzer“ enthält die wichtigsten Regelungen und Vorgaben für diese Personen. Sie bieten einen zusammenfassenden Überblick. Der umfassende Inhalt bzw. alle Details können in den entsprechenden Vorgaben / Verfahrensanweisungen / Richtlinien des Regelwerks (siehe [roXtra](#)) nachgelesen werden.

Für einen gesamten Überblick über wichtige Regelungen und Vorgaben sei auf die Informationssicherheits-Richtlinie verwiesen.

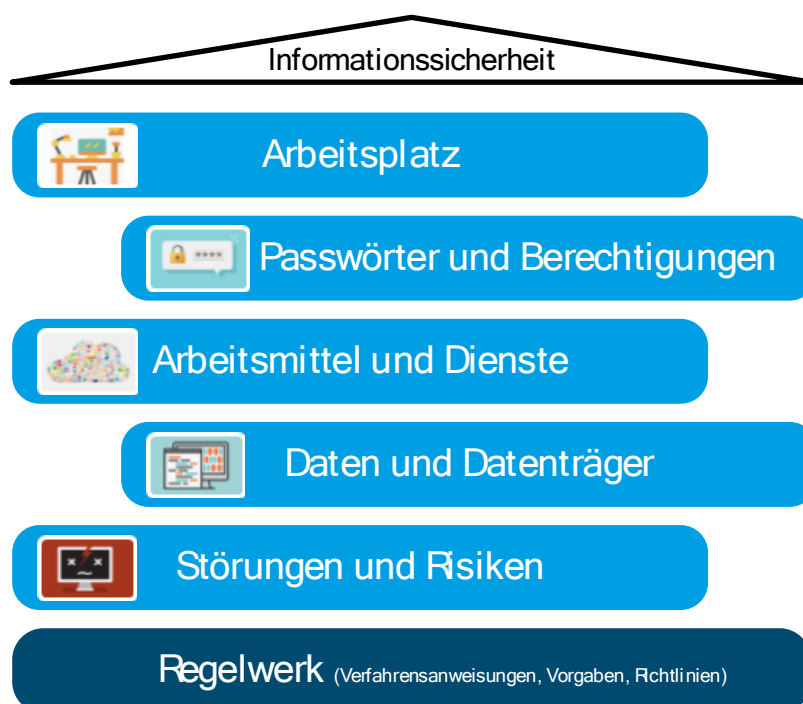
Einleitung

Das sogenannte „Regelwerk“ der Informationssicherheit am Universitätsklinikum Heidelberg umfasst eine Vielzahl von Themen, die in separaten Dokumenten mit vielen detaillierten Regelungen und Vorgaben beschrieben sind.

Die vorliegenden ANB fassen daraus die wichtigsten Regelungen und Vorgaben für alle Personen zusammen, welche die IT und Daten des UK nutzen.

Die Regelungen und Vorgaben sind hierbei nach praxisnahen Themengebieten zusammengestellt. Teilweise sind die Formulierungen kürzer und prägnanter als im Originaldokument des Regelwerks, um die Einprägsamkeit und Verständlichkeit zu erhöhen.

Der Zweck dieses Dokuments besteht darin, eine übersichtliche und anwenderfreundliche Auswahl der wichtigsten Regelungen und Vorgaben der Informationssicherheit bereitzustellen, um eine möglichst große Akzeptanz und Einhaltung zu erreichen.



 UNIVERSITÄTS KLINIKUM HEIDELBERG	Informationssicherheit Allgemeine Nutzungsbedingungen (ANB) für IT- und Datennutzer	Stufe 2 TLP-Green „intern“
Universitätsklinikum Heidelberg	Informationssicherheit / IT-Sicherheit	



Arbeitsplatz

Arbeiten am Arbeitsplatz

	Nur gerade benötigte Unterlagen und Datenträger auf dem Schreibtisch behalten
	Nicht kurzfristig/aktuell benötigte Bildschirmfenster schließen. Bildschirminhalte und Dokumente vor Einsichtnahme Unbeteiligter schützen
	Boards/Flipcharts/Pinnwände so verwenden, dass Unbeteiligte die Inhalte nicht sehen und Boards/Flipcharts/Pinnwände nach Gebrauch „aufräumen“, „leeren“.
	Beim Drucken darauf achten, dass der korrekte Drucker ausgewählt ist und nicht versehentlich an einem anderen Ort gedruckt wird
	Ausdrucke unverzüglich vom Drucker abholen

Vor dem Verlassen des Arbeitsplatzes

	Bildschirme auch beim kurzzeitigen Verlassen des Arbeitsplatzes sperren
	Notizen mit sensiblen Inhalten nicht „offen“ am Arbeitsplatz zurücklassen
	Bei längerem Verlassen des Arbeitsplatzes alle sensiblen Dokumente, Informationen und Datenträger von der Arbeitsfläche nehmen und wegschließen
	Arbeitsplatzgeräte (PCs, Laptops, Bildschirme etc.) bei Arbeitsende ausschalten

Zusätzlich bei Telearbeit

	Dienstliche Gespräche oder Telefonate so führen, dass kein Unbeteiligter mithört
	Dokumente und Datenträger bei Telearbeit ausreichend schützen (Einsicht, Manipulation, Beschädigung, Diebstahl) und das nicht nur während der aktiven Tätigkeiten
	Netzwerk- und weitere Verbindungen zum UK am jeweiligen Telearbeitsplatz nach Arbeitsende trennen / abmelden
	Wenn kein Telearbeitsplatz mehr benötigt wird, dann alle dort verwendeten Geräte/Daten/Unterlagen des UK zurückgeben, falls sie nicht für die Tätigkeiten des Nutzers im UK benötigt werden

 UNIVERSITÄTS KLINIKUM HEIDELBERG	Informationssicherheit Allgemeine Nutzungsbedingungen (ANB) für IT- und Datennutzer	Stufe 2 TLP-Green „intern“
Universitätsklinikum Heidelberg	Informationssicherheit / IT-Sicherheit	



Passwörter und Berechtigungen

Passwörter

	Passwörter sind vertraulich, persönlich und geheim; nicht „einfach weitergeben“!
	Werkseitig eingestellte Passwörter („default“ Passwort) vor Inbetriebnahme von Geräten / Diensten / Accounts / etc. in personen- oder funktionsbezogene Passwörter ändern
	Passwörter bei der Eingabe bzw. der Verwendung so benutzen, dass niemand Drittes das Passwort erhält
	Zur Speicherung von Passwörtern (auch in Anmeldemasken, Webformularen u.ä.) ausschließlich freigegebene Passwort-Management-Tools und Passwortsafes einsetzen
	Ein kompromittiertes Passwort (auch bei begründetem Verdacht) unverzüglich ändern

Berechtigungen

	Verlorene oder entwendete Zutritts-/Zugangsmittel (Schlüssel, Mitarbeiterausweis, etc.) sind umgehend zu melden und nachfolgend unbrauchbar zu machen, zu sperren oder zu deaktivieren
--	--



Arbeitsmittel und Dienste

E-Mail-Nutzung

	Dienstliche E-Mail-Adressen dienstlich nutzen; die gestattete „geringfügige private Nutzung“ der UK E-Mail mit großem Bedacht anwenden
	Gegebenenfalls private E-Mails auf dienstlichen E-Mail-Konten werden nicht anders als dienstliche E-Mails behandelt; Ansprüche aus privaten E-Mails gegenüber dem UK oder Verpflichtungen des UK entstehen keine
	Keine Zugangsdaten (auch Rechte auf persönliche E-Mail-Konten und Kalender) weitergeben
	Eine Weiterleitung von Mails ist nur für dienstliche Zwecke erlaubt. Eine automatisierte Weiterleitung oder Synchronisierung von E-Mails/Kalendereinträgen an Mailadressen oder Web-Dienste außerhalb des UK ist nicht erlaubt
	Vor dem E-Mailversand prüfen, ob die Empfänger korrekt sind und ob der/die Empfänger die enthaltenen Informationen erhalten dürfen
	Bei empfangenen E-Mails hinsichtlich möglicher Bedrohungen (z.B. Schadcode, Virenbefall, Phishing-Attacken, Betrugsversuche) sensibilisiert und vorsichtig sein, da die eingesetzten automatischen Schadcodescanner nicht alle Bedrohungen erkennen können
	Geschäfts- und patientenbezogene E-Mails zusätzlich außerhalb der E-Mail-Postfächer in dafür vorgesehenen Applikationen / Strukturen speichern

 UNIVERSITÄTS KLINIKUM HEIDELBERG	Informationssicherheit Allgemeine Nutzungsbedingungen (ANB) für IT- und Datennutzer	Stufe 2 TLP-Green „intern“
Universitätsklinikum Heidelberg	Informationssicherheit / IT-Sicherheit	

Internet-Nutzung

	Das Internet nur für dienstliche, zulässige Zwecke nutzen und nur die vom UK bereitgestellten Kommunikationsmittel verwenden
	Die private Internet-Nutzung wird durch UK-interne Regelungen festgelegt
	Der Einsatz des Internetzugangs zu privaten Zwecken hat ohne negative Auswirkungen auf die dienstlichen Tätigkeiten zu erfolgen und UK-Nutzer führen keine nicht genehmigten kommerziellen, gewerblichen, freiberuflichen oder privat-geschäftlichen Tätigkeiten im Internet aus
	Bei Veröffentlichung, Bereitstellung und dem Austausch von Informationen im Internet die relevanten gesetzlichen, vertraglichen und UK-internen Regelungen beachten (u.a. Schweigepflicht, Datenschutz, Geheimhaltungserklärungen, Urheber-, Marken-, Persönlichkeitsrechte)
	Schützenswerte bzw. sensible zu übertragenden Informationen verschlüsseln, falls eine unverschlüsselte Verbindung / ein unverschlüsselter Transport verwendet wird

Geräte als Arbeitsmittel

	Am UK ausschließlich vom UK offiziell freigegebene Geräte einsetzen und gemäß den Hersteller-Vorgaben anschließen / verwenden
	Der Einsatz von <u>privaten</u> IT-Geräten (z.B. Handys, Laptops, USB-Speichersticks) zu dienstlichen Zwecken ist nur zulässig, wenn diese explizit durch das ZDI freigegeben und in das Gerätemanagement aufgenommen sind. Sie müssen hinsichtlich Verfügbarkeit, Integrität und Vertraulichkeit die gleichen Anforderungen erfüllen wie UK-Geräte.
	Geräte sowie Verkabelungen so platzieren, transportieren und schützen, dass Risiken durch umweltbedingte Bedrohungen und Gefahren weitestgehend verhindert werden, sowie Störungen, Manipulationen, Diebstahl oder Beschädigungen und unbefugter Zugriff ausreichend unterbunden sind
	Defekte, Verluste oder Beschädigungen von Geräten unverzüglich an den Geräteeigentümer, Gerätebetriebsverantwortlichen oder DV-Service melden
	Vor der Rückgabe, Reparatur und Außerbetriebnahme die auf den Geräten vorhandenen Daten, Information und Konfigurationen löschen
	Beim Wechsel der Arbeitstätigkeit oder beim Beenden des Arbeitsverhältnisses alle nicht mehr notwendigen Arbeitsmittel zurückgeben und alle erforderlichen Daten und Informationen an das UK übergeben

Achtung! Ausdruck könnte veraltet sein. Aktuelle Version immer in roXtra. Druckdatum: 29.07.2025

 UNIVERSITÄTS KLINIKUM HEIDELBERG	Informationssicherheit Allgemeine Nutzungsbedingungen (ANB) für IT- und Datennutzer	Stufe 2 TLP-Green „intern“
Universitätsklinikum Heidelberg	Informationssicherheit / IT-Sicherheit	

Social Media-Dienste

	Nur vom UK ausgewählte und freigegebene Social Media-Plattformen oder Dienste für dienstliche Tätigkeiten verwenden
	Keine UK Kontakte (z.B. aus dem Outlook-Adressbuch) und weitere Daten, weder händisch noch automatisiert, in Social Media Dienste kopieren oder synchronisieren
	Die dienstliche Nutzung von Social Media klar von der privaten Nutzung von Social Media trennen. Bei der privaten Nutzung von Social Media darauf achten, dass andere „Leser“ private Aussagen nicht als offizielle / geschäftliche Aussage des UK missverstehen können (bedeutet auch: Dienstliche und private Social Media Konten / Accounts müssen sich unterscheiden)
	Nur dann Social Media verwenden, wenn alternative Kommunikationsmittel (z.B. E-Mail) für den beabsichtigten Zweck weniger geeignet sind
	Immer daran denken, dass in Social Media-Plattformen und Diensten das Löschen von einmal veröffentlichten Informationen nahezu unmöglich ist
	Bei der Veröffentlichung oder dem Austausch von Informationen über Social-Media-Dienste die relevanten gesetzlichen und vertraglichen Anforderungen und Pflichten beachten (z.B. Schweigepflicht, Datengeheimnis, Geheimhaltungserklärungen, Urheber-, Marken- oder weitere Persönlichkeitsrechte wie z.B. Recht am gesprochenen Wort, Recht am eigenen Bild, etc.)

Cloud-Dienste

	Nur vom UK freigegebene Clouddienste für einzeln festgelegte Zwecke verwenden
	Nutzer befolgen die Vorgaben / Weisungen des Clouddienst-Verantwortlichen
	Auch bei Verwendung von Clouddiensten bleibt die Verantwortung für die dort verarbeiteten Daten / Informationen beim UK und den Nutzern und ist nicht auf den Clouddienst-Anbieter übertragbar
	Das Regelwerk der Informationssicherheit sowie die Punkte der vorliegenden ANB gelten auch für Clouddienste (soweit anwendbar)

Video- und Webkonferenzen

	Video- und Webkonferenzen sollen immer aktiv gestartet und auch beendet werden, damit die Teilnehmer wissen, wann und dass sie sich in einer laufenden Video- oder Webkonferenz befinden
	Bei allen Video- und Webkonferenzen müssen sich die Teilnehmer identifizieren (z.B. mit ihrem Namen), damit sie für alle anderen Teilnehmer erkennbar sind
	Als Teilnehmer oder Veranstalter von Video- und Webkonferenzen immer auf die anwesenden Teilnehmer achten, damit kein „Fremder“ anwesend ist oder hinzukommt
	Aufzeichnungen von Video- und Webkonferenzen sind standardmäßig nicht erlaubt. Falls dennoch Aufzeichnungen notwendig sind, müssen alle Teilnehmer zustimmen
	Sorgfältig über Kamera und Mikrofon wachen, damit keine ungewollten Informationen oder Bilder (z.B. auch Hintergründe mit Whiteboards) aus dem Raum übermittelt werden
	Immer darauf achten, welche Informationen des UK herausgegeben werden, damit keine zu schützenden Informationen das UK ungewollt verlassen

Achtung! Ausdruck kann nicht veraltet sein. Aktuelle Version immer in roXtra. Druckdatum: 29.07.2025

 UNIVERSITÄTS KLINIKUM HEIDELBERG	Informationssicherheit Allgemeine Nutzungsbedingungen (ANB) für IT- und Datennutzer	Stufe 2 TLP-Green „intern“
Universitätsklinikum Heidelberg	Informationssicherheit / IT-Sicherheit	



Daten und Datenträger

Informationsklassifizierung von Daten

	Informationen, Daten und Dateien im UK nach der TLP-Einstufung (TLP-white = öffentlich, TLP-green = intern, TLP-amber = vertraulich, TLP-red = streng vertraulich) klassifizieren
	Informationen, die nicht ausdrücklich klassifiziert sind, besitzen die Vertraulichkeitsklasse „intern“
	Der Verfasser/Ersteller von Informationen klassifiziert sie auf Basis der Angaben des Informationsverantwortlichen
	Informationen müssen nicht unbedingt einzeln bzw. direkt klassifiziert werden. Man kann auch Informationskategorien bilden (z.B. die Kategorie „Röntgenbilder“) und dieser Kategorie eine Vertraulichkeitsklasse zuordnen (die Zuordnung muss dokumentiert werden)
	Den Regelungen für den Lebenszyklus einzelner Informationen, Daten und Dateien (Erstellung, Aufbewahrung, Speicherung, Verarbeitung, Weitergabe, Verteilung, Löschung, Entsorgung) anhängig von ihrer Klassifizierung folgen

Datenablage und -Speicherung

	Patientendaten, Daten für das Tagesgeschäft sowie Informationen von Geschäftsabläufen werden auf Infrastrukturen des UK (bevorzugt in den Rechenzentren) und auf vom UK kontrollierten Systemen strukturiert abgelegt
	Bei mobilen Datenträgern darauf achten, dass diese verschlüsselt sind, wenn sensible Informationen darauf gespeichert werden
	Die Vorgaben vom Dateneigentümer beachten, wo welche Daten/Informationen abgelegt werden und wie mit ggf. notwendigen Kopien/Replikas umgegangen wird. Nur dienstlich notwendige Kopien von Daten anlegen
	Dokumente, Papierunterlagen, Daten und Datenträger so aufbewahren, dass sie vor Zugriff, Entwendung, Manipulation oder Zerstörung geschützt sind
	Das UK unterliegt hinsichtlich von Mitarbeitern auf UK-Infrastrukturen abgelegten privaten Daten keinerlei Verpflichtungen. Nach dem Ausscheiden von Mitarbeitern sind Zugriffe auf ihre Daten nicht mehr möglich

Übertragung und Verwendung von Daten

	Für die digitale Informationsübertragung nur durch das UK freigegebene, zugelassene und dokumentierte Informations- & Kommunikations-Infrastrukturen einsetzen
	Für Test- und Entwicklungssysteme keine „Echt“-Daten verwenden

Achtung! Ausdruck könnte veraltet sein. Aktuelle Version immer in roXtra. Druckdatum: 29.07.2025

 UNIVERSITÄTS KLINIKUM HEIDELBERG	Informationssicherheit Allgemeine Nutzungsbedingungen (ANB) für IT- und Datennutzer	Stufe 2 TLP-Green „intern“
Universitätsklinikum Heidelberg	Informationssicherheit / IT-Sicherheit	

Vernichtung und Löschung von Daten

	Dokumente/Datenträger ausschließlich über die dafür vorgesehenen Wege bzw. Sammelbehälter entsorgen
	Datenträger erst dann weiter- oder weggeben, wenn mit dem Dateneigentümer geklärt ist, ob/welche/wie Daten gesichert und gelöscht werden müssen
	Für die Löschung von Daten ist immer der Dateneigentümer verantwortlich. Die Vorgaben des Dateneigentümers sind bei der Löschung / Vernichtung zu beachten
	Datenlöschung ist nicht nötig, wenn Datenträger angemessen physisch vernichtet werden
	Gesetzliche Aufbewahrungsfristen für Dokumente/Daten vor dem Löschen prüfen und einhalten
	Daten so löschen, dass sie nicht oder nur mit außergewöhnlich hohem Aufwand wiederhergestellt werden können



Störungen und Risiken

IT-Störungen und Informationssicherheits-Risiken

	Alle IT-Störungen (IT-Incidents) in der med. Versorgung melden, damit diese 7/24 in einem Ticketsystem erfasst, dokumentiert, bearbeitet und nachverfolgt werden
	Erkannte Risiken in der Informationssicherheit mit spürbaren Auswirkungen (reaktiv oder proaktiv) melden. Durch Risikomeldungen dürfen die Mitarbeiter keine Nachteile oder sonstige negativen Auswirkungen erfahren.

Achtung! Ausdruck könnte veraltet sein. Aktuelle Version immer in roXtra. Druckdatum: 29.07.2025