KSA

Digitalisierung & IT

ICT-Nutzungsreglement

Reglement zur Nutzung und Überwachung der Informations- und Kommunikationsmittel (ICT-Mittel) in der Kantonsspital Aarau AG und den zugehörigen Tochterunternehmen (KSA-Gruppe)

Dokumententyp	Reglement	**Geltungsbereich**	KSA Gruppe
Gültig ab	01.07.2021	**Verantwortlich**	Informationssicherheit (ISB) Legal & Compliance
Gültig bis	30.06.2024	**Freigabe**	Geschäftsleitung

1. Zweck

Dieses Reglement regelt insbesondere:

- die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der ICT-Infrastruktur,
- die bestimmungsgemässe Nutzung der ICT-Infrastruktur,
- den persönlichen Umgang mit den eingesetzten Mitteln der Informations- und Kommunikationstechnologie (ICT-Mittel),
- die Nutzung von Daten der KSA-Gruppe, einschliesslich deren Überwachung (insbesondere des Internet- und E-Mail-Verkehrs),
- die Sanktionen bei Missbrauch der ICT-Infrastruktur und –Mittel, sowie weitere Zuwiderhandlungen gegen dieses Reglement.

2. Geltungsbereich im Detail

Das Reglement gilt für sämtliche Mitarbeitenden sowie für sämtliche Personen, welche aufgrund anderer Vertragsverhältnisse (bspw. Projektmitarbeiter, Temporär Angestellte, IT-Dienstleister, etc.), in der Folge "Nutzende" genannt, ICT-Infrastruktur, -Mittel und -Systeme der KSA-Gruppe nutzen.
Mit dem Begriff „KSA-Gruppe“ sind auch automatisch die Spital Zofingen AG sowie die weiteren Tochterunternehmen der KSA AG miteingeschlossen.
Dieses Reglement löst das „ICT-Benutzerreglement (Ausgabe April 2010)“ und im Spital Zofingen die „Weisung Informatik (Ausgabe Januar 2010)“, sowie das Merkblatt "Nutzung IT- und Telecom-Inf. & Mobiltelefone" (Ausgabe 2.0_2018_09_04) ab.

3. Definitionen

Daten
Sämtliche Informationen und Inhalte, die von der KSA-Gruppe bearbeitet werden.

ICT-Infrastruktur
Die Gesamtheit aller Anlagen, Geräte, Einrichtungen und Dienste der KSA-Gruppe, die zur elektronischen Bearbeitung von Daten eingesetzt werden, wie Hardware, Software, Netzwerke und Netzwerkgeräte, die für die KSA-Gruppe verwendeten Adressierungselemente (z.B. IP-Adressen) sowie die gespeicherten Daten selbst.

ICT-Mittel
Geräte wie Computer, Notebooks, Mobiltelefone oder Tablets.

Nutzende
Mitarbeiter und weitere Personen gemäss Ziffer 2 dieses Reglements.

Supportorganisationen
Organisationseinheiten und Mitarbeitende der KSA-Gruppe, die mit dem Betrieb der ICT-Infrastruktur beauftragt sind.

4. Nutzungsregelung

4.1. Allgemein

Die Rechte an geschäftlichen/dienstlichen Daten stehen jederzeit vollumfänglich der KSA-Gruppe zu.

Die Nutzenden sind ausschliesslich zum Gebrauch derjenigen ICT-Mittel der KSA-Gruppe befugt, welche ihnen zur Erfüllung ihrer dienstlichen oder vertraglich festgelegten Aufgaben zur Verfügung gestellt werden.

Die Nutzenden sind verpflichtet, die ihnen zur Verfügung gestellten ICT-Mittel recht- und zweckgemäss einzusetzen und Daten, insbesondere schützenswerte Personendaten wie Mitarbeiter- oder Patientendaten, nicht an unberechtigte Dritte weiterzuleiten oder diesen zugänglich zu machen.
Sie sind für die sichere Aufbewahrung von schützenswerten und vertraulichen Daten verantwortlich, von denen sie im Dienste der KSA-Gruppe Kenntnis erlangen. Zu diesen gehören neben Patientendaten/-akten und Datenerfassungsgeräten auch Zugangsdaten wie Benutzernamen und Passwörter, sowie Authentisierungshilfsmittel wie Badge, SMS- oder Secure-Token und andere Zugangsinformationen und -mittel.

Schützenswerte Daten (wie etwa Mitarbeiter- oder Patientendaten) dürfen auf keinen Fall mittels webbasierten persönlichen/privaten Diensten oder Komponenten bearbeitet, übermittelt oder gespeichert werden (z.B. WhatsApp, Facebook, Instagram, Onedrive, Dropbox, Google Drive, etc.), sondern müssen zwingend mit den freigegebenen und durch die KSA-Gruppe zur Verfügung gestellten Services, Applikationen und Plattformen bearbeitet werden.

Der Zugriff auf Internet-Seiten mit rechtswidrigem, pornografischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt ist untersagt.

Bei der Verwendung und Bearbeitung von Daten aus dem Internet sind die Schutzrechte Dritter, insbesondere die Bestimmungen über das Urheberrecht und verwandte Schutzrechte zwingend zu beachten.

4.2. ICT-Infrastruktur und -Mittel

Grundsätzlich dürfen nur ICT-Mittel verwendet werden, die durch die ICT-Verantwortlichen der KSA-Gruppe offiziell beschafft oder zur Installation freigegeben wurden. Ausnahmen müssen durch die zuständigen ICT-Verantwortlichen bewilligt und gegebenenfalls durch den Informationssicherheitsbeauftragten (ISB) freigegeben werden. Bewilligungen können Auflagen enthalten und werden restriktiv gewährt.

Die ICT-Mittel der KSA-Gruppe sind für geschäftliche Zwecke ausgelegt und eingerichtet worden. Eine private Nutzung der ICT-Mittel ist grundsätzlich nicht gestattet. Soweit dadurch interne Ressourcen nicht geschäftlich beeinträchtigt werden, ist die Nutzung ausnahmsweise und auf Zusehen hin geduldet.

Es dürfen von den Nutzenden keine Änderungen an der Konfiguration der ICT-Mittel (insbesondere der Hard- und Software) vorgenommen werden, sowie keine privaten Geräte an die KSA-Hardware und Infrastruktur angeschlossen werden. Ausgenommen von dieser Regelung sind Mitarbeitende, welche durch die KSA-Gruppe mit der Installation, dem Betrieb und der Wartung dieser ICT-Mittel offiziell beauftragt wurden.

4.3. Software

Das Downloaden von Software aus dem Internet und/oder deren Installation sind grundsätzlich untersagt. Dies gilt insbesondere für frei zugängliche Software (Free- und Shareware) sowie für andere Programme wie Treiber, Plug- und Add-Ins, etc. Ausgenommen von dieser Regelung sind Mitarbeitende, welche von der KSA-Gruppe mit der Installation, dem Betrieb und der Wartung der ICT-Infrastruktur beauftragt wurden und für den betrieblichen Zweck vorgängig überprüfte/freigegebene Software im Internet beziehen müssen.

Das Öffnen von selbstausführenden Dateien unbekannter Herkunft (beispielsweise ".exe"-, ".vbs"-, ".pif"-Dateien, etc.) sowie das Ausführen von Scripts oder Makros aus unbekannten Quellen ist ausdrücklich untersagt.

Die für die KSA-Gruppe lizenzierte Software steht den berechtigten Nutzenden für die geschäftliche Anwendung zur Verfügung. Sie darf weder kopiert noch auf privaten ICT-Mitteln installiert oder freigeschaltet werden. Weiter sind sowohl die internen Lizenzbestimmungen als auch diejenigen der Softwarehersteller zu beachten.

4.4. E-Mail

Für die Kommunikation per E-Mail gelten grundsätzlich die gleichen rechtlichen Einschränkungen wie für die Benutzung des Internets.

Es dürfen keine privaten E-Mail-Konten für den elektronischen Geschäftsverkehr verwendet werden. Dieser hat ausschliesslich über das geschäftliche E-Mail-Konto zu erfolgen. E-Mails mit schützenswerten Personendaten dürfen nur verschlüsselt an einen externen Empfänger versandt werden.

Werden E-Mails mit passwortgeschütztem Anhang versendet, so ist das Passwort zur Entschlüsselung über einen anderen Kommunikationskanal (z.B. per Telefon, SMS, Brief) dem Empfänger mitzuteilen, jedoch niemals per E-Mail.

Zum Schutz der ICT-Infrastruktur und allen Nutzenden ist bezüglich Malware (Spam, Phishing, Ransomware, etc.) besondere Vorsicht geboten. Die Nutzenden haben sich an die im Intranet jeweils aktuell gehaltenen spezifischen Informationen, Anleitungen und Prozesse zu halten. Im Zweifelsfall ist immer und sofort der ServiceDesk zu kontaktieren.

4.5. Internet und Social-Media

Das Veröffentlichen von Internet-Auftritten und Social-Media-Inhalten mit Bezug zur KSA-Gruppe ist ohne die vorherige Absprache mit der Marketingabteilung untersagt. Gegebenenfalls werden bereits erstellte Webseiten und Profile einzelner Kliniken oder Mitarbeitenden mit technischen und rechtlichen Mitteln unterbunden. Eine offizielle Information/Kommunikation nach aussen hat immer durch die Unternehmenskommunikation zu erfolgen oder ist mit dieser abzustimmen. Journalistische Anfragen sind an die Unternehmenskommunikation weiterzuleiten.

Daten von Patienten, Mitarbeitenden oder Partnern gehören ohne deren Einwilligung nicht ins Internet oder an die Öffentlichkeit. Es ist insbesondere untersagt Patienten zu fotografieren oder zu filmen und diese Daten öffentlich zugänglich zu machen. Ausnahmen sind durch die Abteilung Legal & Compliance zu bewilligen.

4.6. Zugriffsrechte und Stellvertretungen

Der Zugriff auf geschäftliche/dienstliche Daten steht grundsätzlich vollumfänglich der KSA-Gruppe zu.

Auf die geschäftlichen/dienstlichen Daten der Nutzenden, haben Zugriff:

- *die Nutzenden selbst,*
- *der zuständige Vorgesetzte und Linienverantwortliche,*
- *soweit vorhanden, eine Stellvertretung des Nutzenden,*
- *weitere durch den/die Datenschutzbeauftragte/r (DSB) oder durch die Vorgesetzten legitimierte Personen.*

Gruppenlaufwerke:
Daten, die nur für einen eingeschränkten Benutzerkreis zugänglich gemacht werden sollen (z.B. spezifische vertrauliche Personaldaten), sind auf einem Gruppenlaufwerk mit entsprechend eingeschränkten Zugriffsberechtigungen abzuspeichern. Die Verantwortung für den Zugriff auf die benötigten geschäftlichen/dienstlichen Daten der Mitarbeitenden liegt in der Verantwortung der jeweiligen Vorgesetzten.

Zugang zu EPD (elektronisches Patientendossier):
Die technischen und organisatorischen Zertifizierungsvorgaben (TOZ) regeln die Voraussetzungen für die Stammgemeinschaften. In diesem Zusammenhang sind das Kantonsspital Aarau und das Spital Zofingen verpflichtet, Gesundheitsfachpersonen (GFP) und Hilfspersonen (HIP) welche Zugang zum elektronischen Patientendossier erhalten, zu prüfen, zu berechtigen und aufzuklären. Das Aufklärungsdokument wird in der EPD

Schulung besprochen, vom Mitarbeitenden unterschrieben und zum Personaldossier im HR in elektronischer Form abgelegt.
Berechtigt werden Personen, welche nach eidgenössischem oder kantonalen Recht anerkannte Fachpersonen sind, die im Gesundheitsbereich Behandlungen durchführen, oder im Zusammenhang mit einer Behandlung Heilmittel oder andere Produkte abgeben oder administrative Arbeiten ausführen. Mit Auflösung des Arbeitsvertrages wird die Zugangsberechtigung gelöscht.

4.7. Beendigung des Arbeitsverhältnisses

Vor dem letzten Arbeitstag muss der austretende Mitarbeitende alle ICT-Mittel sowie alle geschäftlichen/dienstlichen Daten und Dokumente den zuständigen Vorgesetzten oder an eine von diesen bezeichnete Person zurückgeben. Gegebenenfalls müssen dafür vorgängig entsprechenden Zugriffsrechte eingerichtet werden.

Bei Austritt aus einem Unternehmen der KSA-Gruppe werden alle den Nutzenden betreffenden Zugriffsrechte auf Daten entsprechend den vorgesehenen Prozessen deaktiviert und nach der Deaktivierung des Accounts gelöscht oder archiviert. Ausnahmen werden von der Abteilung Legal & Compliance vorgegeben. In der Regel wird dazu die Einwilligung des Mitarbeitenden eingeholt.

Sofort nach dem letzten Arbeitstag werden die geschäftlichen/dienstlichen Zugänge des Nutzenden gesperrt. Ausnahmen hiervon müssen von den Bereichsverantwortlichen im Voraus beim ServiceDesk der Informatik beantragt werden. Der Antrag muss eine Begründung der Notwendigkeit enthalten. Die Bewilligungen werden restriktiv gewährt und können Auflagen des DSB oder des Departments Human Resources enthalten. Daten auf privaten ICT-Mitteln (z.B. Mobiltelefon) sind mit Beendigung des Arbeitsverhältnisses unwiderruflich zu löschen.

5. Sorgfaltspflicht

5.1. Gerätehandhabung

Die Nutzenden sind dafür besorgt, die ihnen zur Verfügung gestellten ICT-Mittel vor Diebstahl, Beschädigung und übermässiger Verschmutzung zu schützen. Bei der Reinigung der ICT-Mittel ist Sorgfalt geboten und es sind die spezifischen Pflegehinweise zu beachten.

Nutzende dürfen keine Manipulationen an ICT-Mitteln der KSA-Gruppe vornehmen. Davon ausgenommen sind interne und externe Personen, welche von der KSA-Gruppe mit dem Unterhalt der ICT-Mittel beauftragt wurden. Weitergehende Regelungen sind in der Betriebsnorm "ICT Hardware“ festgehalten.

5.2. Passwörter

Passwörter sind streng vertraulich und dürfen nirgends festgehalten oder notiert werden. Persönliche Passwörter dürfen anderen Nutzenden nicht offengelegt oder zur Verwendung weitergegeben werden. Gleiches gilt für unpersönliche Accounts und Passwörter, welche im Kreise einer bekannten Gruppe von Mitarbeitenden eingesetzt werden.

Beim Zugriff auf Systeme und Daten über private oder öffentliche Computer ist Vorsicht geboten und eine erhöhte Vertraulichkeit gefordert. Durch die KSA-Gruppe werden für diese Nutzung gesicherte Plattformen und stärkere Authentisierungsmethoden angewendet. Es liegt in der Kompetenz des ISB jederzeit entsprechende zusätzliche Sicherheitsmassnahmen festzulegen.

6. Datensicherheit

Jeder Nutzende ist grundsätzlich selbst für die von ihm bearbeiteten Daten verantwortlich und unterliegt dafür einer entsprechenden Sorgfaltspflicht.

Alle Daten, welche sich auf Servern und Netzlaufwerken (beispielsweise home- und Gruppenlaufwerke) befinden, werden gesichert.

Eine dauerhafte lokale (C:) oder externe Speicherung ist untersagt. Daten sind ausschliesslich auf den über das Benutzerkonto zur Verfügung gestellten Netz-Laufwerken zu speichern.
Bei einem allfällig nötigen Geräteaustausch findet keine Wiederherstellung von Daten statt. Dies gilt auch für unrechtmässig/inoffiziell installierte Programme und Lizenzschlüssel etc.

7. Geheimhaltung

Externe Mitarbeitende wie Projektmitarbeitende, Auditoren etc. haben vor dem ersten Zugriff auf Daten die KSA-Geheimhaltungsverpflichtung zu unterschreiben. Die für diese Person intern zuständige Stelle ist verantwortlich für die Beschaffung des unterschriebenen Dokuments, inkl. der Weiterleitung an den ISB.
Der Datenschutz ist für die gesamte KSA-Gruppe im Datenschutzreglement geregelt.

8. Melden von Vorfällen

Bei Verlust, Diebstahl oder Beschädigung von ICT-Mitteln und Daten hat unverzüglich eine Meldung an das ServiceDesk zu erfolgen.

Datenschutzrechtliche- und sicherheitsrelevante Ereignisse sind sofort an die zuständigen Stellen (ISB/DSB) zu melden.

Weiter haben die Nutzenden von ICT-Mitteln die Pflicht, bei sicherheitsrelevanten Vorfällen bezüglich Daten oder bei Verdacht auf Störungen und Sicherheitsrisiken, diese unverzüglich an den ServiceDesk zu melden. Der ServiceDesk leitet die Meldung, sofern erforderlich, an die intern zuständigen Stellen weiter. Diese sind gegebenenfalls für die Weiterleitung an die beauftragten ICT-Leistungserbringer oder Meldestellen verantwortlich.

9. "Clear Screen" und "Clear Desk"

Jeder Nutzende muss beim Verlassen des Arbeitsplatzes den verwendeten Computer sperren (Windows-Taste + L oder Ctrl+Alt+Del und Enter) oder den Computer herunterfahren. Die automatische Windows-Bildschirmsperrzeit nach 15 Minuten wird nur in begründeten Ausnahmefällen erhöht oder deaktiviert.

Um schützenswerte und vertrauliche Daten vor unkontrollierter Einsicht oder unbefugtem Zugriff in offen zugänglichen Bereichen zu schützen, müssen Dokumente und ungeschützte Datenträger (wie CD/DVDs, Festplatten oder USB-Sticks) bei Abwesenheit weggeschlossen oder mitgenommen werden.

10. Technische Schutzmassnahmen an ICT-Mitteln

Zwecks Verhinderung von Störungen, zum Schutze von Personendaten und zur Verhinderung von Missbräuchen der ICT-Mittel werden technisch adäquate Massnahmen getroffen. Hierbei handelt es sich etwa um die Verwendung von Virenscannern, den Einsatz von Firewalls, die Vergabe von Zugriffsberechtigungen sowie die Anwendung von Security-Services.

Die zuständigen Stellen können jederzeit die technischen Schutzmassnahmen oder dieses Reglement an den technischen Fortschritt anpassen, z.B. durch die Beschaffung eines neuen Antivirusprogramms oder durch Erweiterung des Sicherheitskonzeptes, den Einsatz neuer Firewalls mit anderen Authentisierungs-, Überwachungs-, Prüf- und Blockierungsmechanismen, usw. Diesbezügliche Anpassungen werden durch die Informatik vorgeschlagen und durch den ISB freigegeben.

11. Support

Für alle ICT-Mittel der KSA-Gruppe stehen interne Supportorganisationen zur Verfügung, welche bei technischen Problemen und bei Fragen als Erstanlaufstelle zu kontaktieren sind. Die Supportorganisationen stehen nicht für persönliche/private Angelegenheiten zur Verfügung und es ist ihnen untersagt, Konfigurationen und andere Veränderungen an privaten Geräten, Betriebssystemen und Software vorzunehmen.

12. Überwachung

12.1. Überwachung von Netzwerken; Speichersystemen und Applikationen

Die von der KSA-Gruppe beauftragten ICT-Leistungserbringer überwachen automatisiert den Datenverkehr und überprüfen periodisch oder in gezieltem Auftrag des ISB sämtliche Netzwerkverbindungen und -Laufwerke. Ebenfalls werden Netzlaufwerke auf Malware und periodisch auf sicherheitsrelevante und personenbezogene Daten überprüft.

Eine Überwachung/Überprüfung innerhalb von Applikationen findet in der Regel über sogenannte Logfiles statt. Weitergehende Massnahmen werden durch den DSB oder ISB bei der Informatik beauftragt.

Wird festgestellt, dass sich Dateien auf Netzlaufwerken befinden, welche Schaden verursachen können, werden durch die Informatik umgehend, ohne Vorinformation an einen vermeintlichen Verursacher, gegebenenfalls in Abstimmung mit dem ISB, entsprechende Bereinigungs- und Schutzmassnahmen getroffen oder in Auftrag gegeben.

12.2. Nicht personenbezogene Auswertung oder Aufzeichnung

Nicht personenbezogen sind Auswertungen, bei welchen die Ermittlung der Identität der einzelnen Benutzer nicht stattfindet. Sie werden insbesondere in folgenden Fällen vorgenommen:

- *zur Sicherung der Qualität der Leistungen der Informations- und Kommunikationstechnologie (ICT) der KSA-Gruppe bzw. der ICT-Leistungserbringer,*
- *zur Erstellung von Statistiken,*
- *zur stichprobeweisen Überprüfung und Einhaltung der Vorgaben dieses Reglements sowie weiterer die ICT-Nutzung betreffenden Vorschriften und Weisungen,*
- *zur Kostenverteilung und -kontrolle,*
- *zur Lizenzmessung.*

Nicht personenbezogene Auswertungen können durch die Informatik der KSA-Gruppe in Auftrag geben werden. Die Auswertungen werden durch die Informatik selbst, oder durch den ICT-Leistungserbringer erstellt. Der ISB der KSA-Gruppe wird über das Auswertevorhaben informiert und erhält Auszüge zur Einsicht.

12.3. Personenbezogene Auswertung von Aufzeichnungen

Bei personenbezogenen Auswertungen ist der einzelne Benutzer entweder bestimmt (identifiziert) oder bestimmbar („pseudonymisiert“).

Sie werden insbesondere durchgeführt:

- aufgrund der Anordnung einer Justizbehörde,
- wenn nach einer nicht personenbezogenen Auswertung von Aufzeichnungen oder aufgrund eines konkreten Hinweises der Verdacht eines Missbrauchs besteht,
- aufgrund weiterer forensischer Untersuchungen (z.B. Userermittlung, Beweismittelsicherung).

Personenbezogene Auswertungen werden durch den DSB oder den ISB durchgeführt, oder durch diese bei der Informatik oder dem ICT-Leistungserbringer in Auftrag gegeben. Der DSB und der ISB erhalten diese Auswertungen zur weiteren Prüfung und Weitergabe. Sämtliche an der Auswertung beteiligten Personen haben diese Informationen vertraulich zu behandeln.

13. Sanktionen

Sanktionen werden getroffen, wenn eine Verletzung dieser Nutzungsregelungen bzw. missbräuchliche oder gesetzeswidrige Nutzung der Informatikmittel nachweisbar feststeht.

Eine Zuwiderhandlung gegen dieses Reglement kann personalrechtliche Konsequenzen nach sich ziehen. Bei Verstoss gegen strafrechtliche Bestimmungen und bei Verletzung von Rechten Dritter, insbesondere von Urheberrechten, muss mit straf- bzw. zivilrechtlichen Konsequenzen gerechnet werden.

14. Haftung

Nutzende haften im gesetzlichen Rahmen (insbesondere von Art. 321e OR) für jeden Schaden, der vorsätzlich oder fahrlässig der KSA-Gruppe zufügt wurde.

Die KSA-Gruppe übernimmt keine Haftung für Schäden, die aus Mängeln in der ICT-Infrastruktur bzw. bei der Benutzung von ICT-Diensten entstehen. Vorbehalten bleiben anderslautende schriftliche Abmachungen.

15. Vorgehen bei Verdacht auf eine Straftat

Bei Verdacht auf eine Straftat ist die Abteilung Legal & Compliance der KSA-Gruppe unverzüglich zu informieren.

16. Schlussbestimmungen

Die KSA AG behält sich die jederzeitige Änderung des vorliegenden Reglements vor. Eine Änderung wird den Nutzenden schriftlich oder auf eine andere von der KSA AG als geeignet erachtete Weise über das Departement Human Resources bekannt geben.