hôpital fribourgeois
freiburger spital

Direktion Informationssysteme

Reglement des HFR zur Nutzung der IT-Ressourcen

1 Zweck

Zweck dieses Reglements ist es, zur Wahrung der Sicherheit des Informationssystems (IS) des HFR beizutragen. Es legt die Regeln für die Nutzung der IT- und Telekommunikationsressourcen fest, die den Mitarbeitenden, Lieferanten und Gästen (im Folgenden «Nutzerinnen und Nutzer» genannt) zur Verfügung gestellt werden. Es verdeutlicht und ergänzt die bestehende Gesetzgebung im Bereich Datenschutz.

Das Reglement definiert die Rechte, Pflichten und Verantwortlichkeiten der Nutzerinnen und Nutzer des HFR-IS.

2 Geltungsbereich

Das Reglement gilt für alle HFR-internen und -externen Nutzerinnen und Nutzer, die Zugriff auf das HFR-IS haben. Es umfasst die Nutzung aller IT-Ressourcen wie Computer (PC), Laptops, Drucker, Server, Anwendungen, File Sharing, VPN, E-Mail, IP-Telefonie, Internet, Smartphones sowie alle im IS verarbeiteten Daten. Die Verwendung von privaten Geräten, die ausdrücklich von der Direktion Informationssysteme (DIS) genehmigt wurde, fällt ebenfalls in den Geltungsbereich des vorliegenden Reglements.

3 Nutzungsregeln

3.1 Internet (einschliesslich sozialer Netzwerke)

Die Grundsätze der Nutzung des Internets (einschliesslich sozialer Netzwerke und Cloud) werden durch die Verordnung über die Überwachung der Nutzung des Internets durch das Staatspersonal (SGF 122.70.17) festgelegt. Der in Artikel 4 Absatz 1 festgehaltene Grundsatz lautet:

Die Internetnutzung ist beruflichen Zwecken vorbehalten.

Die gelegentliche Internetnutzung einschliesslich der Nutzung von E-Mail und Social Media zu privaten Zwecken wird innerhalb der Grenzen, die sich aus der Dienstpflicht ergeben, die ganze Arbeitszeit der amtlichen Tätigkeit zu widmen, geduldet (vgl. Art. 4 Abs. 2 SGF mit Verweis auf Art. 58 Abs. 1 StPG).

Die private Nutzung muss ausserdem die folgenden Bedingungen erfüllen:

- Sie darf den reibungslosen Abteilungsbetrieb nicht beeinträchtigen.
- Sie darf das Netzwerk nicht beeinträchtigen.
- Sie darf keinen Erwerbszwecken dienen.
- Sie darf nicht unerlaubt sein.

- Die Nutzung von sozialen Netzwerken oder die Ausübung anderer Aktivitäten im Internet darf in keiner Weise den Ruf des HFR oder seiner Partner schädigen.
- Es ist strengstens untersagt, jegliche multimediale Inhalte, die das HFR betreffen oder in denen Mitarbeitende vorkommen, ohne die Zustimmung der Abteilung Kommunikation zu veröffentlichen.

3.2 Verarbeitung in der Cloud

Grundsätzlich ist es untersagt, geschäftliche Dokumente ausserhalb des HFR in einer öffentlichen Cloud (z. B. Dropbox, Google Drive usw.) oder in einer privaten Cloud (z. B. privates NAS) zu speichern, sofern keine Zustimmung des Datenschutzkomitees des HFR vorliegt.

Als autonome öffentlich-rechtliche Einrichtung unterliegt das HFR dem Freiburger Gesetz über den Datenschutz (SGF 17.1 – Gesetz über den Datenschutz – Kanton Freiburg – Gesetzessammlung). Dieses Gesetz regelt die Voraussetzungen für die ausgelagerte Verarbeitung von Personendaten und besonders schützenswerten Daten.

Um die gesetzlichen Vorschriften einzuhalten, sind folgende Regeln zwingend zu beachten:

Grundsätzlich dürfen Cloud-Dienste (einschliesslich KI-Dienste) nicht für die Verarbeitung (Speicherung, Abruf oder Änderung) personenbezogener oder besonders schützenswerter Daten genutzt werden, sofern diese Daten zuvor nicht anonymisiert wurden. Dieses Vorgehen hat sicherzustellen, dass kein Rückschluss auf die betroffenen Personen möglich ist.

Dieser Grundsatz gilt beispielsweise für ChatGPT, Copilot, Claude, Gemini, DeepL, Azure Translate, Microsoft OneDrive, Microsoft SharePoint Online.

Ist die Nutzung eines Cloud-Dienstes (einschliesslich KI-Diensten) erforderlich und eine Anonymisierung nicht möglich, muss eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden. Zudem ist eine Genehmigung durch das Datenschutzkomitee des HFR zwingend erforderlich.

Jede Verarbeitung nicht anonymisierter personenbezogener oder besonders schützenswerter Daten in der Cloud (einschliesslich KI-Diensten) ohne vorherige Genehmigung durch das Datenschutzkomitee des HFR führt zur Haftung der Nutzerin oder des Nutzers.

3.3 Künstliche Intelligenz (KI)

KI-gestützte Tools sind leistungsstark und müssen verantwortungsvoll sowie unter Einhaltung der ethischen Grundsätze eingesetzt werden. Die finale Verantwortung für die Nutzung von KI und die daraus resultierenden Ergebnisse liegt immer bei der Nutzerin oder beim Nutzer.

Der Einsatz von KI muss den geltenden gesetzlichen Bestimmungen und Vorschriften zum Datenschutz und zur Vertraulichkeit entsprechen (insbesondere Kap. 3.2 «Verarbeitung in der Cloud»).

Die Bedingungen für den Einsatz von KI am HFR sowie die damit verbundenen Verantwortlichkeiten sind in der internen Richtlinie «Institutionelle Weisung zur Nutzung von künstlicher Intelligenz (KI)» festgelegt.

3.4 E-Mail

Die Nutzung von E-Mail-Diensten unterliegt den folgenden Regeln:

- Der Austausch von beruflichen Informationen darf nur über geschäftliche E-Mail-Adressen erfolgen. Darüber hinaus ist es strengstens untersagt, besonders schützenswerte Daten (z. B. Patientendaten) ungesichert an private, persönliche E-Mail-Adressen von Mitarbeitenden zu senden. Bei Bedarf ist einzig ein sicherer Versand zulässig («Verschlüsselter E-Mail-Versand – HIN Secure Mail»).
- Der Austausch besonders schützenswerter Daten mit externen Partnern darf ausschliesslich über ein gesichertes Mail-Netzwerk erfolgen (HIN-Netzwerk oder «Verschlüsselter E-Mail-Versand – HIN Secure Mail»).
- Die Nutzerinnen und Nutzer sind dafür verantwortlich, die Quelle der ihnen zugesandten E-Mails zu überprüfen. Beim Öffnen von Anhängen oder Links ist höchste Vorsicht geboten. Im Zweifelsfall ist der IT-Support des HFR zu kontaktieren.
- Um Spamming zu vermeiden, ist es den Nutzerinnen und Nutzern nicht gestattet, sich mit ihrer HFR-Adresse auf privaten Websites zu registrieren, die keinen Zusammenhang mit der beruflichen Tätigkeit haben.
- Beleidigende, verleumderische, diskriminierende, gewalttätige und anstössige Äusserungen sind verboten und dürfen daher nicht per E-Mail verbreitet werden.

3.5 Austausch grosser Dateien mit besonders schützenswerten Daten

Wenn eine grosse Datei mit besonders schützenswerten Daten an einen externen Partner übermittelt werden muss und kein Versand bzw. Empfang über eine gesicherte E-Mail-Verbindung möglich ist, muss ein Antrag beim IT-Support gestellt werden. Dieser stellt anschliessend einen Zugang zur offiziellen HFR-Austauschplattform sowie eine entsprechende Anleitung bereit. Der Austausch grosser Dateien mit besonders schützenswerten Daten über öffentliche Plattformen ist untersagt.

3.6 IT-Support und Fernzugriff

Nur die DIS-Mitarbeitenden sind im Rahmen einer von den Nutzerinnen und Nutzern übermittelten Support-Anfrage berechtigt, mit deren Zustimmung auf deren Computer zuzugreifen.

Sämtliche Anfragen von Dritten betreffend den Fernzugriff auf HFR-Geräte müssen abgelehnt werden, sofern keine Mitarbeiterin bzw. kein Mitarbeiter der DIS diesem zugestimmt hat.

3.7 Nutzung von persönlichen Konten und Authentifizierung

Den Nutzerinnen und Nutzern werden ein persönliches Windows-Konto und, je nach Funktion, verschiedene persönliche Konten in Fachanwendungen zugewiesen.

Persönliche Konten, Passwörter und andere Authentifizierungsmittel (Einmal-Code, SMS, Token usw.) dürfen unter keinen Umständen an Dritte (Kolleginnen und Kollegen oder Externe) weitergegeben werden.

Dies gilt für Windows-Konten und alle spezifischen Anwendungskonten.

3.8 Verwendung von externer Hardware / externen Hilfsmitteln

Die Verwendung von externen Medien am PC und Laptop der Nutzerinnen und Nutzer (z. B. USB-Stick, externe Festplatte usw.) ist aus Sicherheitsgründen nicht gestattet. Allfällige Ausnahmen sind in einem Antrag an den IT-Support zu begründen. Die DIS wird eine Genehmigung prüfen. Dabei behält sie sich das Recht vor, diese im Falle eines Risikos zu verweigern.

3.9 Private Geräte und Netzwerk

Ohne ausdrückliche Zustimmung der DIS darf kein privates Gerät (PC, Laptop, Smartphone, Tablet usw.) mit dem kabelgebundenen Netzwerk oder dem WLAN des HFR verbunden werden.

Die Speicherung von geschäftlichen Dokumenten und damit verbundenen besonders schützenswerten Daten auf privaten Geräten ist strengstens untersagt.

3.10 VPN-Zugang und Homeoffice

Der externe Zugriff auf das HFR-IS kann mit einem HFR-Laptop und einer institutionellen Full-VPN-Lösung erfolgen, je nach Bedarf und Verfügbarkeit der entsprechenden Hardware bei der DIS.

Der Zugriff ist ferner von einem privaten Computer über ein entsprechendes Portal möglich. Der private Computer muss in diesem Fall mit einem Virenschutzprogramm gesichert und einem aktuellen Betriebssystem ausgestattet sein. Wie unter Punkt 3.7 erwähnt, ist es verboten, geschäftliche Dokumente und besonders schützenswerte Daten auf den privaten Computer zu kopieren oder dort zu speichern. Das HFR übernimmt keine Haftung für Schäden, die durch den Befall eines privaten Computers mit Schadsoftware entstehen. Für private Computer wird kein Support angeboten.

3.11 Software und geistiges Eigentum

Die Nutzerinnen und Nutzer erhalten entsprechend ihrer Funktion und/oder ihrem beruflichen Wirkungsbereich Zugang zu bestimmter, von der DIS bereitgestellter Software. Software, die bestimmte, kostenpflichtige Lizenzen erfordert, muss von der/vom Vorgesetzten genehmigt werden.

Sämtliche Software muss von der DIS validiert und von ihr oder mit ihrer Zustimmung bereitgestellt werden. Software, die ohne Zustimmung der DIS installiert wurde, kann gelöscht werden und es wird dafür kein Support angeboten.

Die Verwendung von Software ohne entsprechende Lizenz und die Verwendung von Softwarekopien sind verboten.

3.12 Ausdrucke

Das Equitrac-System («Follow me-Printing») ermöglicht eine Kontrolle der Ausdrucke, wie in der Print Policy festgehalten.

In der Regel drucken oder kopieren Mitarbeitende nur Dokumente, die im Zusammenhang mit ihrer beruflichen Tätigkeit stehen. Die private Nutzung von Multifunktionsdruckern wird nur toleriert, wenn sie in Zeit und Häufigkeit minimal ausfällt, die Ressourcen vernachlässigbar beansprucht, die berufliche Tätigkeit nicht gefährdet oder behindert und nicht Teil einer privaten Erwerbstätigkeit ist.

Bei Missbrauch werden die Mitarbeiterin/der Mitarbeiter und die/der Vorgesetzte informiert und es wird eine Rechnung ausgestellt.

4 Pflichten der Nutzerinnen und Nutzer

4.1 Amts- und Berufsgeheimnis

Je nach Funktion erhalten die Nutzerinnen und Nutzer Zugriff auf Fachanwendungen mit besonders schützenswerten Daten. Sie unterstehen damit zwei Geheimhaltungspflichten:

- Amtsgeheimnis: Es ist den Nutzerinnen und Nutzern untersagt, dienstliche Angelegenheiten zu verbreiten, von denen sie in Ausübung ihrer Funktion Kenntnis erhalten haben und die in ihrer Natur und den Umständen nach oder gemäss besonderen Vorschriften geheim zu halten sind.
- Berufsgeheimnis (oder ärztliche Schweigepflicht): spezifisch für Informationen über Patientinnen und Patienten.

Das Amts- und Berufsgeheimnis gilt über das Ende des Arbeitsverhältnisses hinaus.

Bei Verletzung des Amts- und Berufsgeheimnisses sind rechtliche oder strafrechtliche Konsequenzen vorbehalten (Art. 320 und 321 des Schweizerischen Strafgesetzbuchs).

Nutzerinnen und Nutzer sind grundsätzlich nur berechtigt, Daten von Patientinnen und Patienten einzusehen und zu verarbeiten, mit denen sie in einem therapeutischen Verhältnis stehen oder deren Daten sie aus beruflichen Gründen verarbeiten.

4.2 Einhaltung der Sicherheitsmassnahmen

Die Nutzerinnen und Nutzer dürfen unter keinen Umständen die getroffenen Sicherheitsmassnahmen umgehen (Einrichtung eines persönlichen WLAN, Deaktivieren oder Umgehen von IS-Sicherheitstools usw.).

4.3 Teilnahme an Sensibilisierungsmassnahmen zur Cybersicherheit

Die Nutzerinnen und Nutzer sind verpflichtet, an Sensibilisierungsmassnahmen zum Thema Cybersicherheit teilzunehmen, insbesondere an den zur Verfügung gestellten Online-Schulungsmodulen. Bei wiederholter Nichtteilnahme an Schulungen und Phishing-Tests kann die DIS Massnahmen zur Einschränkung der Internetnutzung und der Nutzung externer Medien beschliessen.

4.4 Meldung von Sicherheitsproblemen

Wenn Nutzerinnen und Nutzer von einem Sicherheitsproblem Kenntnis erhalten, so haben sie dieses unbedingt so schnell wie möglich dem IT-Support zu melden, um mögliche Folgen des Vorfalls zu begrenzen.

4.5 Einhaltung der Ethikregeln des HFR

Die Speicherung und absichtliche Weitergabe von Daten (Bilder, Videos usw.), die den Ethikregeln des HFR widersprechen, sind strengstens untersagt.

5 Kontrolle und Sanktionen

Alle Internetzugriffe werden protokolliert und es können Kontrollen durchgeführt werden (vgl. SGF 122.70.17). Auch der Zugriff auf interne Netzwerke und Geschäftsanwendungen sowie die Nutzung von Nutzerkonten können kontrolliert werden.

Bei Nichteinhaltung der in diesem Reglement festgelegten Bestimmungen behält sich die DIS das Recht vor, den Computerzugang zu sperren oder einzuschränken, und die betroffenen Nutzerinnen und Nutzer müssen je nach Schwere des Sachverhalts mit internen disziplinarischen und/oder strafrechtlichen Sanktionen rechnen.

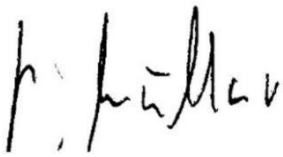
Die Nichteinhaltung des Amts- oder Berufsgeheimnisses setzt Nutzerinnen und Nutzer einer strafrechtlichen Verfolgung nach den Artikeln 320 und 321 des Schweizerischen Strafgesetzbuches aus.

6 Verabschiedung und Inkrafttreten

Der Direktionsrat hat das vorliegende Reglement in seiner Sitzung vom 26. August 2026 verabschiedet.

Es tritt am 1. Oktober 2026 in Kraft. Freiburg,

26. September 2026.





Philipp Müller

Generaldirektor

Sven Penelle

Direktor Informationssysteme