Informationssicherheitsrichtlinie
für die Nutzung mobiler Endgeräte

Dokumenteneigenschaften:

Allgemeine Angaben	
Titel	Informationssicherheitsrichtlinie für die Nutzung mobiler Endgeräte
Dokumentebene	Taktisch
Management Kategorie	IT-Sicherheit
Sicherheitsklassifizierung	SK-1 (Intern)
Referenz Dokumente	ISO 27001, BSI-Grundschutz (insb. SYS.3.2.2)
Verantwortlichkeiten	
Hauptverantwortlicher	Max Mustermann / IT-Leiter
Ansprechpartner	Peter Peters / ISB
E-Mail, Telefon	Peter Peters, +49 152 xxx xxxx
Autor	Peter Peters
Gültigkeiten	
In Kraft seit	28.08.2025
In Kraft gesetzt durch	Max Mustermann / CEO
Überarbeitungsintervall	12 Monate
Nächste Überarbeitung	28.08.2025
Erstellt am	17.07.2025

Dokumentenhistorie

Version	**Änderung**	**Datum**	**Autor**
v.1.0	Initialerstellung	17.07.2025	Peter Peters

Inhalt

1. Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer und sonstige Dritte, die mobile Endgeräte (Smartphones, Tablets) – sowohl firmeneigene als auch private (BYOD) – nutzen, um auf Daten, Systeme oder Dienste der RecodeHealth AG zuzugreifen.

2. Zweck

Zweck dieser Richtlinie ist der Schutz von sensiblen Informationen der RecodeHealth AG, insbesondere geschützte Gesundheitsinformationen (PHI) und geistiges Eigentum (IP), auf mobilen Endgeräten. Sie definiert verbindliche technische und organisatorische Maßnahmen für den gesamten Lebenszyklus der Geräte, welche sowohl die Pflichten der Nutzer im täglichen Gebrauch als auch die administrativen Prozesse der IT-Abteilung umfassen. Ziel ist es, die Risiken von Datenverlust, unbefugtem Zugriff und Kompromittierung zu minimieren und die Einhaltung der DSGVO zu gewährleisten.

3. Verantwortlichkeiten

Informationssicherheitsbeauftragter (ISB): Entwickelt und pflegt diese Richtlinie, überwacht deren Einhaltung, bewertet Risiken und genehmigt Ausnahmen.

IT-Leitung: Stellt die notwendigen Ressourcen für die Umsetzung bereit, insbesondere für die Beschaffung und den Betrieb der Mobile-Device-Management-System (MDM).

Systemadministration / IT-Helpdesk: Administriert das MDM-System, setzt die in dieser Richtlinie definierten Konfigurationen um, verwaltet den Lebenszyklus der Geräte und führt im Notfall Fernlöschungen (Remote Wipes) durch.

Mitarbeiter: Sind verpflichtet, diese Richtlinie einzuhalten, ihr zugewiesenes Gerät physisch zu sichern und Vorfälle wie Verlust oder Diebstahl unverzüglich zu melden.

4. Regelungen

4.1. Geräteregistrierung und -verwaltung (MDM)

Jedes mobile Endgerät, das auf Unternehmensdaten zugreift, muss ohne Ausnahme in der zentralen Mobile-Device-Management-System (MDM) der RecodeHealth AG registriert sein. Die Systemadministration hat sicherzustellen, dass ein Zugriff auf Unternehmensressourcen ohne ein aktives und konformes MDM-Profil technisch unterbunden wird.

4.2. Grundlegende Sicherheitskonfiguration

Die folgenden Einstellungen werden per MDM erzwungen und dürfen von Benutzern nicht deaktiviert werden:

- **Gerätesperre**:
  - Jedes mobile Endgerät muss mit einer Gerätesperre (PIN, Passwort oder biometrisches Verfahren) geschützt werden.
  - Die Komplexität und Art der Gerätesperre hat den Vorgaben der zentralen "Passwort- und Authentisierungsrichtlinie" der RecodeHealth AG zu entsprechen. Diese Richtlinie definiert unterschiedliche Anforderungen für verschiedene Geräteklassen:
    - Für Laptops: Es gilt die Anforderung an komplexe Passwörter.
    - Für Smartphones und Tablets: Es gilt die Anforderung an eine PIN mit definierter Mindestlänge.
  - Sofern ein Gerät über biometrische Verfahren verfügt, muss deren Nutzung zur Entsperrung des Geräts aktiviert werden.
- **Automatische Sperre**: Das Gerät muss so konfiguriert sein, dass es nach maximal 3 Minuten Inaktivität automatisch gesperrt wird.
- **Verschlüsselung**: Die Ablageverschlüsselung des Geräts muss aktiviert sein.
- **Betriebssystem-Updates**: Das mobile Gerät muss so konfiguriert sein, dass kritische Sicherheitsupdates des Betriebssystems erzwungen werden. Mitarbeitern ist es untersagt, die Installation dieser Updates über einen Zeitraum von mehr als drei Werktagen nach ihrer Bereitstellung durch das MDM aufzuschieben.
- **Jailbreak/Rooting**: Modifizierte Betriebssysteme (Jailbreaks, Rooting) sind strengstens verboten. Das MDM muss so konfiguriert sein, dass es modifizierte Betriebssysteme erkennt und den Zugriff auf Unternehmensdaten für diese Geräte automatisch sperrt.

4.3. Trennung von Unternehmens- und Privatdaten (Containerisierung)

Auf allen Geräten, insbesondere bei BYOD, müssen Unternehmensdaten und -anwendungen in einem separaten, verschlüsselten Container gespeichert werden. Es ist untersagt, Daten aus dem sicheren Unternehmenscontainer in private Anwendungen oder unsichere Speicherorte zu kopieren oder zu verschieben. Das MDM-System hat sicherzustellen, dass diese Trennung technisch erzwungen wird.

4.4. Anwendungsmanagement (Apps)

- **App-Bezug:** Anwendungen, die auf Unternehmensdaten zugreifen, dürfen ausschließlich über den von der IT-Abteilung bereitgestellten "Enterprise App Store" bezogen und installiert werden.
- **Gesperrte Anwendungen**: Das MDM erzwingt eine Liste verbotener Anwendungen, deren Installation die Sicherheit oder Vertraulichkeit gefährden könnte.
- **Berechtigungen**: Die Systemadministration hat sicherzustellen, dass alle über das MDM bereitgestellten Unternehmensanwendungen nur mit den für den Betrieb minimal erforderlichen Berechtigungen konfiguriert sind.

4.5. Sichere Netzwerknutzung

- **VPN:** Der Zugriff auf interne Ressourcen der RecodeHealth AG darf mobil nur über die vom MDM konfigurierte VPN-Verbindung erfolgen.
- **WLAN:** Der Zugriff auf interne Unternehmensdaten über öffentliche oder ungesicherte WLAN-Netze ist untersagt. Für den Fernzugriff darf ausschließlich die durch das MDM bereitgestellte VPN-Verbindung genutzt werden.

4.6. Nutzung von Cloud-Diensten und externer Hardware

- Die Nutzung von privaten oder nicht durch die IT-Leitung genehmigten Cloud-Speicherdiensten zur Ablage von Unternehmensdaten ist strengstens untersagt.
- Der Anschluss von nicht autorisierter externer Hardware an mobile Endgeräte ist verboten. Das MDM muss die Datenschnittstellen der Geräte entsprechend einschränken

4.7. Datenklassifizierung und -schutz auf dem Gerät

- Alle auf mobilen Endgeräten verarbeiteten Unternehmensdaten unterliegen der Datenklassifizierungsrichtlinie der RecodeHealth AG.
- Daten mit der Klassifizierung „Sehr hoch“ (in der ISMS-Methodik Schutzbedarfsstruktur als D001 Sensible Unternehmensdaten identifiziert) dürfen auf mobilen Endgeräten grundsätzlich nicht dauerhaft gespeichert werden. Der Zugriff muss ausschließlich temporär über gesicherte Anwendungen gestattet.
- Die Erstellung von Screenshots oder Bildschirmaufnahmen von Inhalten innerhalb des sicheren Unternehmenscontainers ist untersagt. Diese Funktion muss durch das MDM technisch blockiert werden.

4.8. Physische Sicherheit und Verhalten bei Verlust

- Mobile Endgeräte dürfen zu keiner Zeit unbeaufsichtigt an öffentlichen Orten gelassen werden.
- Verlust oder Diebstahl eines Geräts muss unverzüglich dem IT-Helpdesk gemeldet werden. Diese Meldung löst den formalen Prozess zur Berichterstattung und Eskalation gemäß **Abschnitt 6** dieser Richtlinie aus, der eine sofortige Sperrung des Geräts zur Folge hat.

5. Pflichten von Systemadministration

Die Systemadministration ist verpflichtet, den sicheren und regelkonformen Betrieb der gesamten MDM-Infrastruktur gemäß den Vorgaben des BSI IT-Grundschutz zu gewährleisten. Dazu gehören insbesondere die folgenden Pflichten:

- **Härtung und Absicherung der MDM-Systeme:**
  - Das zugrundeliegende Betriebssystem des MDM-Servers **muss** gemäß den aktuellen Härtungsempfehlungen des Herstellers und des BSI konfiguriert werden.
  - Der Zugriff auf die Administrationskonsole des MDM darf ausschließlich von dedizierten und gesicherten Administrator-Workstations erfolgen.
  - Es muss ein Rollen- und Berechtigungskonzept für die Verwaltung des MDM umgesetzt werden, das dem Minimalprinzip folgt.
- **Regelmäßige Überprüfung und Protokollierung:**
  - Die Systemadministration hat sicherzustellen, dass die Konfigurations-einstellungen aller verwalteten Geräte mindestens quartalsweise auf Konformität mit dieser Richtlinie überprüft werden. Abweichungen müssen protokolliert und korrigiert werden.
  - Sicherheitsrelevante Ereignisse, wie fehlgeschlagene Anmeldeversuche am Gerät, die Erkennung von Jailbreaks/Rooting oder Verstöße gegen Compliance-Regeln, müssen zentral protokolliert und täglich ausgewertet werden.
- **Management des Gerätelebenszyklus:**
  - **Außerbetriebnahme (Unenrollment):** Wenn ein Gerät außer Betrieb genommen wird, hat die Systemadministration sicherzustellen, dass alle Unternehmensdaten und zugehörige Konfigurationen (gemäß der zentralen "Passwort- und Authentisierungsrichtlinie" der RecodeHealth AG) sicher und nachweislich vom Gerät entfernt werden.
  - **Geofencing:** Für Geräte von Mitarbeitern, die mit besonders schutzbedürftigen Informationen arbeiten (in der ISMS-Methodik Schutzbedarfsstruktur als D001 Sensible Unternehmensdaten identifiziert), müssen Geofencing-Richtlinien definiert werden. Bei Verlassen eines vordefinierten geografischen Bereichs des Europäischen Wirtschaftsraums (EWR) muss eine automatische Sperrung des Zugriffs auf kritische Daten erfolgen, nachdem der ISB informiert wurde.
- **Compliance-Durchsetzung:**
  - Das MDM muss so konfiguriert werden, dass bei erkannten Compliance-Verstößen (Installation einer verbotenen App, deaktivierte Verschlüsselung) automatisch gestufte Maßnahmen ergriffen werden. Dies hat die folgenden Aktionen zu umfassen:
    - Versenden einer automatischen Warnung an den Benutzer und den IT-Helpdesk.
    - Sperren des Zugriffs auf Unternehmensanwendungen.
    - Automatisches Löschen des Unternehmenscontainers nach wieder-holten oder schwerwiegenden Verstößen in Absprache mit dem ISB.

6. Berichterstattung und Eskalation

Jeder Mitarbeiter ist verpflichtet, alle sicherheitsrelevanten Vorfälle und Schwachstellen, die mobile Endgeräte betreffen, unverzüglich zu melden. Dies umfasst nicht nur Verlust oder Diebstahl, sondern auch den Verdacht auf Kompromittierung, Schadsoftware, erfolgreiche Phishing-Angriffe oder ungewöhnliches Geräteverhalten.

Der folgende Eskalationsprozess muss eingehalten werden:

- Meldung an den IT-Helpdesk: Alle Vorfälle sind als Erstes dem IT-Helpdesk zu melden. Der IT-Helpdesk dient als zentrale Anlaufstelle (Single Point of Contact) und hat sicherzustellen, dass für jeden gemeldeten Vorfall ein Ticket im zentralen System mit allen verfügbaren Informationen erstellt wird.
- Ersteinschätzung und Sofortmaßnahmen: Der IT-Helpdesk führt eine Ersteinschätzung durch und leitet basierend auf der Art der Meldung Sofortmaßnahmen ein. Bei Meldung von Verlust oder Diebstahl muss unverzüglich eine Fernsperrung (Remote Lock) des Geräts veranlasst werden, um einen unmittelbaren Zugriff durch Dritte zu verhindern.
- Eskalation an den ISB: Nach der Ersteinleitung von Maßnahmen hat der IT-Helpdesk den Vorfall unverzüglich an den Informationssicherheitsbeauftragten (ISB) zu eskalieren.
- Vorfallmanagement durch den ISB: Der ISB übernimmt die weitere Koordination, bewertet die Schwere des Vorfalls und entscheidet über das weitere Vorgehen. Dies beinhaltet die Autorisierung weitergehender Maßnahmen, wie die vollständige Fernlöschung (Remote Wipe) der Unternehmensdaten vom Gerät.
- Dokumentation: Alle Schritte des Melde- und Eskalationsprozesses, von der initialen Meldung bis zur endgültigen Schließung des Vorfalls, müssen lückenlos im Ticketsystem dokumentiert werden, um die Nachvollziehbarkeit für Audits zu gewährleisten.

7. Schulung der Mitarbeiter

Alle Mitarbeiter sind verpflichtet, an einer jährlichen Sicherheitsschulung teilzunehmen, die die Inhalte dieser Richtlinie sowie die korrekte Reaktion auf Sicherheitsvorfälle behandelt. Neue Mitarbeiter erhalten diese Schulung im Rahmen ihres Onboardings.

8. Genehmigung von Ausnahmen

Ausnahmen von dieser Richtlinie sind nur in begründeten Einzelfällen und nach einer dokumentierten Risikobewertung zulässig. Sie erfordern die schriftliche Genehmigung durch den ISB und die IT-Leitung.

9. Audits und Auswertung der Wirksamkeit und Angemessenheit

Der Informationssicherheitsbeauftragte (ISB) ist verpflichtet, die Einhaltung, Wirksamkeit und Angemessenheit dieser Richtlinie durch regelmäßige Audits zu überprüfen.

- **Prüfungsintervall**: Es muss mindestens einmal jährlich ein planmäßiges Audit stattfinden. Darüber hinaus können anlassbezogene Prüfungen nach schwerwiegenden Sicherheitsvorfällen oder bei wesentlichen Änderungen der IT-Infrastruktur erforderlich sein.
- **Prüfungsumfang**: Die Audits haben sowohl technische als auch organisatorische Aspekte zu umfassen. Dazu gehören insbesondere:
  - Eine stichprobenartige technische Überprüfung der MDM-Konfigurationsprofile auf Konformität mit dieser Richtlinie.
  - Die Kontrolle der Prozessdokumentation, für die Geräteregistrierung, die Genehmigung von Ausnahmen und die Reaktion auf gemeldete Vorfälle.
  - Die Auswertung der Protokolldaten aus dem MDM auf sicherheitsrelevante Ereignisse und Compliance-Verstöße.
  - Die Überprüfung der Schulungsnachweise für alle Mitarbeiter.
- **Auswertung und Bericht**: Die Ergebnisse jeder Prüfung müssen in einem Auditbericht vollständig dokumentiert und analysiert werden. Der Bericht hat eine Bewertung der Effektivität der umgesetzten Maßnahmen zu enthalten und eventuelle Schwachstellen oder Verbesserungspotenziale klar aufzuzeigen.

10. Aktualisierung der Richtlinie

Auf Grundlage der Auditergebnisse sowie bei wesentlichen Änderungen der technologischen oder rechtlichen Rahmenbedingungen hat der ISB diese Richtlinie zu aktualisieren, um deren fortdauernde Angemessenheit sicherzustellen. Die jeweils aktuelle und freigegebene Fassung muss versioniert und allen Mitarbeitern nachweislich zur Kenntnis gebracht werden. Die Richtlinie muss einmal jährlich überprüft und freigegeben werden.

11. Konsequenzen bei Nichteinhaltung

Ein Verstoß gegen diese Richtlinie kann arbeitsrechtliche Konsequenzen, einschließlich einer Abmahnung oder Kündigung, nach sich ziehen. Zudem kann der Zugriff auf die IT-Systeme der RecodeHealth AG eingeschränkt oder entzogen werden.

Peter Peters

Peter Peters

CEO

17.07.2025

Ort, Datum