Leitlinie zur sicheren Nutzung des Idana Cloud-Dienstes für Kunden

Datum: 03. November 2025

Einleitung und Ziele

Diese Leitlinie zur sicheren Nutzung des Idana Cloud-Dienstes richtet sich an Cloud-Kunden (Arztpraxen und medizinische Einrichtungen) und beschreibt Best Practices für die sichere Konfiguration, Installation und Nutzung des Cloud-Dienstes “Idana”. Sie dient als detaillierte Ausarbeitung der in der Richtlinie zur Kommunikation und Bereitstellung von Informationen festgelegten Anforderungen und basiert auf den Standards ISO 27001:2022 und BSI C5:2020.

Ziele dieser Leitlinie:

- Unterstützung der Cloud-Kunden bei der sicheren Konfiguration und Nutzung des Idana Cloud-Dienstes
- Befähigung sachverständigen Personals der Cloud-Kunden zur Umsetzung von Informationssicherheitsvorgaben
- Transparente Kommunikation über Sicherheitsmechanismen und Verantwortlichkeiten
- Minimierung von Sicherheitsrisiken durch angemessene Nutzung des Cloud-Dienstes

Geltungs- und Anwendungsbereich

Diese Leitlinie gilt für alle Cloud-Kunden der Idana AG, die den Cloud-Dienst “Idana” zur digitalen Patientenaufnahme in ihren Einrichtungen nutzen. Sie richtet sich insbesondere an:

- IT-Verantwortliche in Arztpraxen und medizinischen Einrichtungen
- Compliance-Beauftragte
- Datenschutzbeauftragte
- Praxisinhaber und -manager
- Mitarbeiter mit administrativen Berechtigungen im Idana-System

Compliance Matrix

Die Compliance Matrix stellt die Konformität dieser Leitlinie mit den relevanten Sicherheitsstandards sicher.

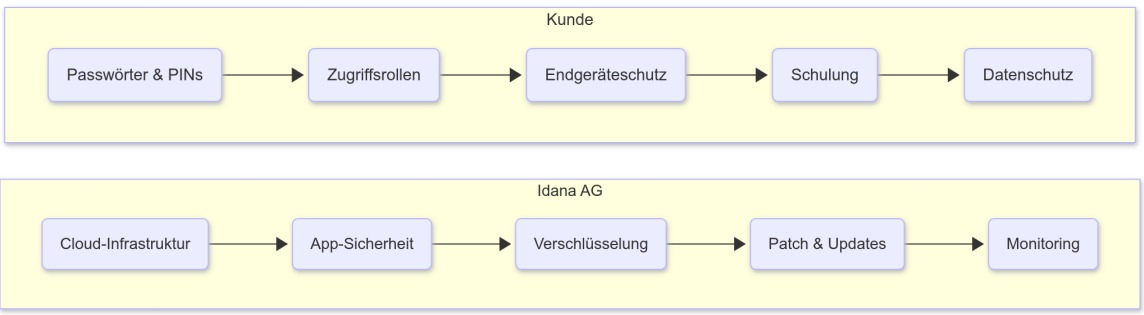
Konzept-Komponente	ISO 27001:2022 / 27002:2022	BSI C5:2020
Gesamte Leitlinie (alle Abschnitte)	**A.5.1, A.6.3**	**PSS-01**
Sichere Konfiguration und Installation	A.8.9, A.8.19	INQ-01, PSS-01
Schwachstellenmanagement und Updates	A.8.8	OPS-18, PSS-01
Fehlerbehandlung und Protokollierung	A.8.15, A.8.16	OPS-10, PSS-01
Authentisierungsmechanismen	A.5.17, A.5.18	IDM-08, IDM-09, PSS-01
Rollen- und Rechtekonzept	A.5.15, A.5.18	IDM-01, IDM-04, PSS-01
Administration durch privilegierte Benutzer	A.5.15, A.8.2	IDM-03, PSS-01
Information und Schulung	A.6.3	HR-03, PSS-01

Leitfaden zur sicheren Nutzung

1. Grundsätze und strategische Ausrichtung

Der Idana Cloud-Dienst ist als **Software-as-a-Service (SaaS)** konzipiert und bietet eine sichere, DSGVO-konforme Lösung für die digitale Patientenaufnahme im Gesundheitswesen. Die Sicherheitsarchitektur basiert auf dem **Shared Responsibility Model**, bei dem Idana AG und Cloud-Kunden gemeinsam für die Sicherheit verantwortlich sind.

Verantwortlichkeitsverteilung:



2. Sichere Konfiguration und Installation

2.1. Systemanforderungen und Zugangswege

Der Idana Cloud-Dienst ist über folgende Zugangswege nutzbar:

- **Idana Desktop-App:** Windows und macOS
- **Idana Bridge:** Verbindungssoftware für die Integration mit Praxisverwaltungssystemen (Windows und macOS)
- **Web-Browser:** Chrome, Firefox, Safari, Edge (aktuelle Versionen)

Wichtiger Hinweis: Es gibt keine mobile App von Idana. Alle offiziellen Idana-Anwendungen sind ausschließlich unter den Domains **idana.com** und **idana.app** sowie deren Subdomains zu finden. Trauen Sie keinen anderen Domains oder Apps – diese könnten betrügerisch sein.

Minimale Sicherheitsanforderungen für Ihre Endgeräte:

Als Cloud-Kunde liegt die Sicherheit Ihrer lokalen Computer und Geräte in Ihrer eigenen Verantwortung. Stellen Sie bitte sicher:

- **Aktuelles Betriebssystem:** Installieren Sie regelmäßig Sicherheitsupdates für Windows, macOS oder Linux
- **Antivirus-Software:** Halten Sie eine aktive Virenschutz-Software auf dem neuesten Stand
- **Firewall:** Aktivieren Sie die eingebaute Firewall Ihres Betriebssystems
- **Festplattenverschlüsselung:** Nutzen Sie BitLocker (Windows) oder FileVault (macOS)
- **Bildschirmsperre:** Richten Sie eine automatische Bildschirmsperre ein (maximal 5 Minuten Inaktivität)
- **Starke Benutzerkonten:** Verwenden Sie sichere Passwörter für Ihre Computer-Benutzerkonten

2.2. Initiale Konfiguration und sichere Installation

Installation der Client-Anwendungen:

WICHTIG: Installieren Sie die Idana Desktop-App und Idana Bridge ausschließlich aus offiziellen Quellen:

- **Offizielle Download-Seite:** https://assets.idana.app/downloads
- **Überprüfung der Authentizität:** Stellen Sie sicher, dass die heruntergeladenen Installationsdateien mit einem **EV-Softwarezertifikat der Firma Idana AG** signiert sind
  - Windows: Rechtsklick auf die .exe-Datei → Eigenschaften → Digitale Signaturen → Zertifikat prüfen
  - macOS: Das System überprüft die Signatur automatisch beim ersten Start

Bei der ersten Einrichtung des Idana-Systems sollten folgende Schritte beachtet werden:

1. **Praxiskonto einrichten:**
   - Verwendung einer institutionellen E-Mail-Adresse (z.B. praxis@ihre-praxis.de, keine persönlichen E-Mail-Adressen wie max.mustermann@gmail.com)
   - Sichere Passwortwahl gemäß Passwort-Policy (siehe Abschnitt 4.1)
   - Aktivierung der Zwei-Faktor-Authentifizierung (2FA) dringend empfohlen
2. **Zugangsbeschränkungen festlegen:**

   Hinweis: Aktuell unterstützt Idana noch kein Mehrbenutzer- und Rollensystem. Dies befindet sich in Entwicklung.

   Bis zur Einführung des Rollensystems empfehlen wir:
   - Beschränken Sie den Zugang zum Idana-Account auf ausgewählte, vertrauenswürdige Mitarbeiter
   - Geben Sie Zugangsdaten (Passwort und PIN) nur an Personen weiter, die diese wirklich benötigen
   - Dokumentieren Sie intern, wer Zugriff auf den Idana-Account hat
   - Ändern Sie Passwort und PIN, wenn Mitarbeiter ausscheiden oder die Praxis verlassen
   - Schulen Sie alle Personen mit Zugang zur sicheren Nutzung (siehe Abschnitt 9)
3. **Idana-PIN festlegen:**
   - Die Idana-PIN schützt den Zugriff auf verschlüsselte Patientendaten
   - **Anforderungen:** Gleiche Passwort-Anforderungen wie für den Account-Login (siehe Abschnitt 4.2)
   - PIN niemals aufschreiben oder unverschlüsselt speichern
   - Bei Verwendung von 2FA: Kein regelmäßiger Wechsel erforderlich, nur bei Verdacht auf Kompromittierung

2.3. Netzwerksicherheit in der Praxis

Empfohlene Netzwerkkonfiguration:

- **WLAN-Sicherheit:** WPA3 oder mindestens WPA2 mit starkem Passwort

- **Netzwerktrennung:** Separates WLAN für Patienten (Gast-Netzwerk) und Praxis-Systeme
- **Firewall-Einstellungen:** Nur notwendige Ports freigeben (HTTPS/443)
- **VPN-Nutzung:** Bei Fernzugriff auf Idana über VPN-Verbindung

3. Informationsquellen zu Schwachstellen und Aktualisierungsmechanismen

3.1. Automatische Updates

Der Idana Cloud-Dienst wird kontinuierlich aktualisiert und gewartet:

- **Backend-Updates:** Automatisch durch Idana AG ohne Ausfallzeiten
- **Idana Desktop-App:** Automatische Update-Benachrichtigung beim Start
- **Idana Bridge:** Automatische Update-Benachrichtigung beim Start

Ihre Verantwortung als Cloud-Kunde:

Automatische Updates aktiviert lassen (empfohlen):

- Die Idana Desktop-App und Idana Bridge aktualisieren sich in der Regel vollautomatisch
- Sie erhalten eine Benachrichtigung, wenn ein Update verfügbar ist
- Starten Sie die Anwendungen nach einem Update neu

Falls Sie automatische Updates deaktiviert haben:

- Sie müssen selbst dafür Sorge tragen, dass immer die neuesten Versionen installiert sind
- Prüfen Sie regelmäßig (mindestens wöchentlich) auf verfügbare Updates
- Installieren Sie sicherheitsrelevante Updates innerhalb von 7 Tagen

Zusätzliche Verantwortung:

- Halten Sie Ihren Browser auf dem aktuellsten Stand
- Installieren Sie Betriebssystem-Updates regelmäßig (mindestens monatlich)

3.2. Schwachstellenkommunikation und -management

Wie Idana AG Sie über Sicherheitsupdates informiert:

- **E-Mail-Benachrichtigungen:** Sie erhalten E-Mails bei kritischen Sicherheitsupdates.
- **Status-Seite:** Aktuelle Systemstatus und Wartungsarbeiten unter https://status.idana.com

Online-Register bekannter Schwachstellen:

Die Idana AG veröffentlicht Informationen zu bekannten Schwachstellen in einem öffentlichen Online-Register:

- **URL:** https://portal.idana.app/vulnerabilities
- **Nutzung:** Prüfen Sie regelmäßig (z.B. monatlich), ob Ihre installierten Versionen der Idana Desktop-App und der Idana Bridge betroffen ist
- **Handlungsempfehlung:** Aktualisieren Sie bei Betroffenheit sofort auf die neueste Version, sofern Sie den automatischen Update-Mechanismus nicht nutzen

So prüfen Sie Ihre installierte Version:

- **Idana Desktop-App:** Programmeigenschaften → Versionsnummer
- **Idana Bridge:** Programmeigenschaften → Versionsnummer

Wie Idana Schwachstellen behebt:

- Automatisierte Schwachstellen-Scans in der Entwicklungspipeline
- Kritische Schwachstellen werden innerhalb von 7 Tagen behoben
- Sicherheitsupdates werden automatisch ausgerollt (bei aktivierten Auto-Updates)

4. Authentisierungsmechanismen

4.1. Passwort-Anforderungen für den Idana-Account

Was ist ein sicheres Passwort?

Ihr Idana-Account-Passwort schützt den Zugang zu sensiblen Patientendaten. Folgende Anforderungen gelten:

Mindestanforderungen (eine der beiden Varianten erfüllen):

Option 1: Kurzes, komplexes Passwort

- **Mindestlänge:** 8 Zeichen
- **Komplexität:** Alle 4 Zeichenarten verwenden:

  - Großbuchstaben (A-Z)
  - Kleinbuchstaben (a-z)
  - Zahlen (0-9)
  - Sonderzeichen (z.B. !@#$%^&*)
- **Beispiel:** “Pr4x!s2025” (8 Zeichen mit allen 4 Zeichenarten)

Option 2: Lange Passphrase (empfohlen)

- **Mindestlänge:** 20-25 Zeichen
- **Komplexität:** Mindestens 2 Zeichenarten verwenden
- **Beispiel:** “MeinePraxisIstSehrSicher2025” (28 Zeichen, Groß-/Kleinbuchstaben + Zahlen)

Weitere wichtige Anforderungen:

- **Einzigartigkeit:** Verwenden Sie das Passwort nicht für andere Dienste
- **Keine bekannten schwachen Passwörter:** Das System verhindert häufig verwendete oder bekannte unsichere Passwörter
- **Kein regelmäßiger Wechsel erforderlich:** Bei Verwendung von Zwei-Faktor-Authentifizierung (2FA)
- **Sofortiger Wechsel:** Nur bei Verdacht auf Kompromittierung notwendig

Tipps für ein gutes Passwort:

- **Empfohlen:** Nutzen Sie eine lange Passphrase (Option 2) – diese ist sicherer und leichter zu merken
- Verwenden Sie einen Passwort-Manager (z.B. 1Password, Bitwarden, KeePass)
- Aktivieren Sie unbedingt die Zwei-Faktor-Authentifizierung (siehe Abschnitt 4.3)

Das sollten Sie vermeiden:

- Passwörter auf Zetteln notieren oder in Klartext speichern
- Passwörter per E-Mail, WhatsApp oder SMS versenden
- Einfache Passwörter wie “Praxis123”, “Idana2025” oder “Passwort”
- Wiederverwendung von Passwörtern anderer Dienste
- Wörter aus dem Wörterbuch ohne Abwandlung

4.2. Idana-PIN (Verschlüsselungs-PIN)

Was ist die Idana-PIN?

Die Idana-PIN schützt den Zugriff auf die verschlüsselten Patientendaten in Ihrer Praxis. Ohne die korrekte PIN können die Daten nicht entschlüsselt werden.

PIN-Anforderungen:

Die Idana-PIN unterliegt den **gleichen Sicherheitsanforderungen wie das Account-Passwort** (siehe Abschnitt 4.1). Sie haben zwei Optionen:

Option 1: Kurze, komplexe PIN

- **Mindestlänge:** 8 Zeichen
- **Komplexität:** Alle 4 Zeichenarten verwenden:
  - Großbuchstaben (A-Z)
  - Kleinbuchstaben (a-z)
  - Zahlen (0-9)
  - Sonderzeichen (z.B. !@#$%^&*)
- **Beispiel:** “Pr4x!s25” (8 Zeichen mit allen 4 Zeichenarten)

Option 2: Lange PIN-Passphrase (empfohlen)

- **Mindestlänge:** 20-25 Zeichen
- **Komplexität:** Mindestens 2 Zeichenarten verwenden
- **Beispiel:** “MeinePatientenSindSicher2025” (30 Zeichen, Groß-/Kleinbuchstaben + Zahlen)

Wichtige Hinweise:

- **Unterschiedlich zum Account-Passwort:** Verwenden Sie eine andere PIN als Ihr Account-Passwort
- **PIN-Reset möglich**
  - Um Ihre PIN zurückzusetzen loggen Sie sich mit Ihrem Idana-Account auf https://portal.idana.app/ ein.
  - Navigieren Sie zum Bereich “Mein Konto” und folgen den Anweiseungen zu “Pin zurücksetzen”.
  - Bei Problemen kontaktieren Sie den Idana-Support: support@idana.com
- **Kein regelmäßiger Wechsel erforderlich:** Bei Verwendung starker PINs und sicherer Aufbewahrung

- **Sofortiger Wechsel:** Nur bei Verdacht auf Kompromittierung notwendig

Backup-Key sicher aufbewahren:

Der Backup-Key ermöglicht die Wiederherstellung Ihrer Daten bei PIN-Verlust:

- Bewahren Sie ihn an einem sicheren Ort auf (z.B. Tresor, versiegelter Umschlag)
- Notieren Sie den Backup-Key niemals zusammen mit der PIN
- Teilen Sie den Backup-Key nur mit autorisierten Personen (z.B. Praxisinhaber)
- Erstellen Sie eine sichere Kopie an einem zweiten, separaten Ort
- Speichern Sie den Backup-Key NICHT unverschlüsselt auf dem Computer

4.3. Zwei-Faktor-Authentifizierung (2FA)

Was ist 2FA und warum ist es wichtig?

Die Zwei-Faktor-Authentifizierung (2FA) bietet eine zusätzliche Sicherheitsebene beim Login. Selbst wenn jemand Ihr Passwort kennt, kann er sich ohne den zweiten Faktor (z.B. ein Code aus einer App) nicht anmelden.

Wir empfehlen dringend die Aktivierung von 2FA für alle Idana-Accounts!

Unterstützte 2FA-Methode:

- **Authenticator-App:** Google Authenticator, Microsoft Authenticator, Authy oder vergleichbare TOTP-Apps

So richten Sie 2FA ein:

1. Öffnen Sie in Idana den Bereich “Mein Konto”.
2. Navigieren Sie zu “Zwei-Faktor-Authentifizierung (2FA)”
3. Klicken Sie auf “Zwei-Faktor-Authentifizierung hinzufügen”.
4. Wählen Sie eine der angebotenen Authentifizierungsmöglichkeiten und folgen Sie den Anweisungen auf dem Bildschirm.
5. **Wichtig im Falle einer Authenticator-App:** Laden Sie die Backup-Codes der Authenticator-App herunter und bewahren Sie diese sicher auf:
    - Drucken Sie die Codes aus und legen Sie sie in einen Tresor
    - Oder speichern Sie sie verschlüsselt in einem Passwort-Manager
    - Diese Codes ermöglichen den Zugang, falls Sie Ihr Smartphone verlieren
6. Bestätigen Sie die Einrichtung mit einem Test-Code aus der App

WICHTIG: Ohne Backup-Codes können Sie bei Verlust Ihres Smartphones nicht mehr auf Ihren Account zugreifen!

5. Zugangsmanagement und Berechtigungen

5.1. Aktueller Status: Noch kein Mehrbenutzersystem

Wichtiger Hinweis: Der Idana Cloud-Dienst unterstützt derzeit noch kein vollständiges Mehrbenutzersystem mit unterschiedlichen Rollen und Rechten. Diese Funktionalität befindet sich in Entwicklung und wird in zukünftigen Versionen verfügbar sein.

5.2. Empfohlene Zugangsbeschränkungen (aktuelle Situation)

Da aktuell alle Personen mit Zugang zum Idana-Account die gleichen Berechtigungen haben, ist es besonders wichtig, den Zugang streng zu kontrollieren:

Empfohlene Maßnahmen:

Zugang auf notwendige Personen beschränken:

- Gewähren Sie Zugang nur an Mitarbeiter, die Idana für ihre tägliche Arbeit benötigen
- Dokumentieren Sie intern, welche Personen Zugriff haben (Name, Datum der Berechtigung)
- Beispiel: Ärzte, medizinische Fachangestellte am Empfang, ggf. Praxismanager

Sichere Weitergabe der Zugangsdaten:

- Teilen Sie Passwort und PIN niemals per E-Mail, SMS oder WhatsApp
- Übergeben Sie Zugangsdaten persönlich (z.B. auf einem Zettel, der anschließend vernichtet wird)
- Oder nutzen Sie verschlüsselte Passwort-Manager für die sichere Weitergabe

Zugang entziehen bei Personalwechsel:

- Ändern Sie sofort Passwort und PIN, wenn ein Mitarbeiter die Praxis verlässt
- Aktualisieren Sie Ihre interne Dokumentation der zugriffsberechtigten Personen
- Informieren Sie alle verbleibenden berechtigten Personen über die neuen Zugangsdaten

Schulung aller Personen mit Zugang:

- Stellen Sie sicher, dass alle Personen mit Zugang diese Leitlinie gelesen haben
- Schulen Sie neue Mitarbeiter zur sicheren Nutzung (siehe Abschnitt 9)
- Sensibilisieren Sie regelmäßig für Datenschutz und Informationssicherheit

5.3. Zukünftiges Rollen- und Rechtekonzept (in Entwicklung)

Das geplante Mehrbenutzersystem wird voraussichtlich folgende Rollen unterstützen:

- **Praxisadministrator:** Vollzugriff mit Benutzerverwaltung und Konfiguration
- **Arzt/Ärztin:** Zugriff auf medizinische Daten
- **Medizinische Fachangestellte (MFA):** Eingeschränkter Zugriff (z.B. Patientenaufnahme, Check-In)
- **Abrechnungspersonal:** Zugriff nur auf abrechnungsrelevante Daten
- **Lesezugriff (Viewer):** Nur lesender Zugriff für temporäre Nutzer

Sobald diese Funktionalität verfügbar ist, wird diese Leitlinie entsprechend aktualisiert.

6. Verantwortungsvolle Nutzung und administrative Aufgaben

6.1. Besondere Verantwortung für Personen mit Zugang

Da aktuell noch kein Rollensystem existiert, haben alle Personen mit Idana-Zugang die gleichen Berechtigungen. Daher gelten für alle Nutzer erhöhte Sicherheitsanforderungen:

Pflicht-Maßnahmen für alle Nutzer mit Zugang:

Starke Authentifizierung:

- Nutzen Sie ein starkes Passwort (mindestens 8 Zeichen, siehe Abschnitt 4.1)
- Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA) - siehe Abschnitt 4.3

Sichere Arbeitsweise:

- Greifen Sie nur von sicheren, vertrauenswürdigen Geräten auf Idana zu
- Nutzen Sie Idana nicht von öffentlichen Computern (z.B. Internet-Cafés)
- Seien Sie vorsichtig bei der Nutzung öffentlicher WLANs (besser: Mobile Daten oder VPN)
- Aktivieren Sie die Bildschirmsperre ihres Geräts jedes Mal, wenn Sie Ihren Arbeitsplatz verlassen

Vertraulichkeit:

- Geben Sie Ihre Zugangsdaten niemals an Unbefugte weiter
- Lassen Sie niemanden über Ihre Schulter schauen, wenn Sie mit Patientendaten arbeiten
- Schützen Sie Ihren Computer mit einer automatischen Bildschirmsperre

6.2. Besondere Hinweise zur Idana Bridge

Was ist die Idana Bridge?

Die Idana Bridge ist eine Software, die auf Ihrem Praxis-Computer läuft und die Verbindung zwischen Idana und Ihrem Praxisverwaltungssystem (PVS) herstellt.

Sicherheitshinweise zur Idana Bridge:

Schutz der Konfigurationsdatei:

Die Konfigurationsdatei der Idana Bridge `config.yaml` enthält hochsensible Sicherheitsschlüssel:

- **Private- und Public-Key:** Zur Ver- und Entschlüsselung Ihrer Praxisdaten
- **Refresh-Key:** Zur automatischen Anmeldung bei Idana

Wichtige Sicherheitsmaßnahmen:

Zugriffsschutz:

- Der Zugriff auf die Konfigurationsdatei sollte nur IT-Administratoren der Praxis vorbehalten sein
- Schützen Sie die Datei vor Lesezugriffen durch normale Benutzer
- Windows: Setzen Sie entsprechende NTFS-Berechtigungen
- macOS/Linux: Nutzen Sie `chmod` um Berechtigungen einzuschränken (z.B. `chmod 600`)

Bei Verdacht auf Kompromittierung:

- Kontaktieren Sie sofort den Idana-Support (security@idana.com)
- Ändern Sie alle Zugangsdaten (Passwort, PIN)

- Lassen Sie neue Schlüssel generieren

6.3. Notfall-Zugriff und Vertretungsregelung

Vorbereitung auf Notfälle:

Dokumentation der Zugänge:

- Erstellen Sie eine Liste aller Personen mit Idana-Zugang
- Definieren Sie mindestens 2 Personen, die im Notfall Zugriff wiederherstellen können
- Dokumentieren Sie den Standort von Backup-Key und 2FA-Backup-Codes

Sichere Aufbewahrung wichtiger Informationen:

- Backup-Key für die Idana-PIN: Versiegelter Umschlag im Tresor
- 2FA-Backup-Codes: Ausgedruckt und sicher verwahrt
- Notfall-Kontakt zum Idana-Support: support@idana.com

Regelmäßige Tests:

- Prüfen Sie, ob die Vertretungspersonen wissen, wie sie im Notfall vorgehen müssen
- Aktualisieren Sie die Notfall-Dokumentation bei Änderungen

7. Fehlerbehandlung und Protokollierung

7.1. Fehlerbehandlungsmechanismen

Der Idana Cloud-Dienst verfügt über robuste Fehlerbehandlung:

- **Automatische Fehlerberichterstattung:** Technische Fehler werden automatisch an Idana gemeldet
- **Benutzerfreundliche Fehlermeldungen:** Klare Handlungsanweisungen bei Fehlern
- **Fallback-Mechanismen:** Automatische Wiederholung bei temporären Netzwerkproblemen

Kunden-Verantwortung bei Fehlern:

- Fehlermeldungen dokumentieren (Screenshot + Fehlerbeschreibung)
- Sofortige Meldung an Idana-Support bei sicherheitsrelevanten Fehlern
- Keine Umgehung von Sicherheitsmechanismen versuchen

7.2. Protokollierung und Audit-Logs

Aus Compliance-Gründen protokolliert Idana folgende Ereignisse:

- Benutzeranmeldungen und -abmeldungen
- Zugriffe auf Patientendaten (wer, wann, welche Daten)
- Änderungen an Benutzern und Berechtigungen
- Konfigurationsänderungen durch Administratoren
- Fehlgeschlagene Anmeldeversuche

Zugriff auf Audit-Logs:

- Über das Kundenportal https://portal.idana.app/account/logs haben Sie Zugriff auf Überwachungs-Protokolle für Ihren Account.
- Diese werden nach Erstellung für 30 Tage gespeichert und dann automatisch gelöscht.

7.3. Incident Reporting und Reaktion auf Sicherheitsvorfälle

Was ist ein Sicherheitsvorfall?

Ein Sicherheitsvorfall liegt vor, wenn der Verdacht besteht, dass:

- Unbefugte Zugriff auf Ihren Idana-Account erhalten haben
- Ein Gerät mit Idana-Zugang verloren gegangen oder gestohlen wurde
- Zugangsdaten (Passwort, PIN) kompromittiert wurden (z.B. durch Phishing)
- Ungewöhnliche Aktivitäten im Account festgestellt wurden
- Ihr Computer mit Schadsoftware (Virus, Trojaner) infiziert sein könnte

Sofort-Maßnahmen bei Verdacht auf einen Sicherheitsvorfall:

Schritt 1: Zugang sofort sperren

- Melden Sie sich bei Idana an und ändern Sie sofort Ihr Passwort
- Falls dies nicht möglich ist, kontaktieren Sie den Idana-Support zur Sperrung des Accounts
- Bei Verlust oder Diebstahl eines Geräts: Sofort Support kontaktieren

Schritt 2: Zugangsdaten ändern

- Ändern Sie Ihr Idana-Passwort
- Ändern Sie die Idana-PIN
- Falls Sie 2FA nutzen: Erneuern Sie die 2FA-Einrichtung

Schritt 3: Vorfall dokumentieren

- Notieren Sie Datum und Uhrzeit des Vorfalls
- Beschreiben Sie die Art des Vorfalls (z.B. “Phishing-E-Mail erhalten und angeklickt”)
- Listen Sie betroffene Systeme auf (z.B. “Arbeitsplatz-PC im Behandlungszimmer 2”)
- Bewahren Sie Screenshots und E-Mails als Beweismittel auf

Schritt 4: Idana-Support informieren

- **E-Mail:** support@idana.com
- **Betreff:** “SICHERHEITSVORFALL - [Ihre Praxis-ID oder Name]”
- **Inhalt:** Beschreibung des Vorfalls, bereits ergriffene Maßnahmen
- **WICHTIG:** Übermitteln Sie KEINE sensiblen Patientendaten per E-Mail!

Was der Idana-Support für Sie tut:

- Sicherheitsanalyse des Vorfalls durchführen
- Prüfung, ob weitere Kunden betroffen sind
- Technische Maßnahmen zur Schadensbegrenzung einleiten
- Incident-Report für Ihre Dokumentation bereitstellen
- Unterstützung bei der Wiederherstellung des sicheren Betriebs

Nach dem Vorfall:

- Überprüfen Sie Ihre Sicherheitsmaßnahmen und passen Sie diese an
- Schulen Sie Ihre Mitarbeiter zum Thema (siehe Abschnitt 9)
- Dokumentieren Sie “Lessons Learned” für zukünftige Vorfälle

8. Datenschutz und DSGVO-Compliance

8.1. Gemeinsame Verantwortlichkeit

Idana AG (Auftragsverarbeiter):

- Technische und organisatorische Maßnahmen (TOMs) gemäß Art. 32 DSGVO
- Verschlüsselung von Daten in Transit und at Rest
- Zugriffskontrolle und Protokollierung
- Regelmäßige Sicherheitsaudits und Penetrationstests

Cloud-Kunden (Verantwortliche):

- Rechtsgrundlage für Datenverarbeitung sicherstellen
- Patienteneinwilligungen einholen (wo erforderlich)
- Betroffenenrechte umsetzen (Auskunft, Löschung, etc.)
- Datenschutzfolgenabschätzung durchführen
- Mitarbeiter zu Datenschutz schulen

8.2. Patientenrechte

Unterstützung bei der Umsetzung von Betroffenenrechten:

- **Auskunftsrecht (Art. 15 DSGVO):** Export-Funktion für Patientendaten
- **Recht auf Löschung (Art. 17 DSGVO):** Löschfunktion
- **Recht auf Datenübertragbarkeit (Art. 20 DSGVO):** Strukturierter Datenexport (GDT, PDF, JSON)
- **Widerspruchsrecht (Art. 21 DSGVO):** Deaktivierung von Kommunikationskanälen

9. Schulung und Sensibilisierung

Wo finden Sie Schulungsmaterialien?

Offizielle Idana-Schulungsressourcen:

- **Idana Selbstschulung:** https://praxis.idana.com/idana-selbstschulung#
- **Implementierungs-Portal:** https://praxis.idana.com/portal-zur-implementierung

Zusätzliche Ressourcen:

- Online-Webinare zu Spezialthemen (Ankündigung per E-Mail)

10. Überwachung und kontinuierliche Verbesserung

10.1. Feedback und Verbesserungsvorschläge

Kunden können Feedback und Verbesserungsvorschläge einreichen über:

- **E-Mail:** productmanagement@idana.com
- **Support-Portal:** https://support.idana.com

10.3. Review und Aktualisierung

Diese Leitlinie wird regelmäßig überprüft und aktualisiert:

- **Jährliches Review:** Überprüfung auf Aktualität und Vollständigkeit
- **Ad-hoc Updates:** Bei wesentlichen Änderungen am Cloud-Dienst oder Sicherheitslandschaft

11. Support und Kontakt

11.1. Idana-Support kontaktieren

Bei Fragen oder Problemen zur sicheren Nutzung von Idana stehen wir Ihnen gerne zur Verfügung:

- **E-Mail:** support@idana.com
  - Antwort innerhalb von 24 Stunden (während Geschäftszeiten Mo-Fr)
  - Für allgemeine Fragen und technische Probleme
- **Sicherheitsvorfälle:** support@idana.com
  - Betreff: “SICHERHEITSVORFALL - [Ihre Praxis]”
  - Bei Verdacht auf unbefugten Zugriff, Datenverlust oder Kompromittierung
  - **WICHTIG:** Keine Patientendaten per E-Mail versenden!

11.2. Weitere Ansprechpartner bei Idana AG

- **Datenschutz-Fragen:** kontakt@idana.com
  - Fragen zu DSGVO, Patientenrechten, Auftragsverarbeitung
- **Vertrieb und Kundenbetreuung:** vertrieb@idana.com
  - Fragen zu Verträgen, Abonnements, neuen Funktionen

11.3. Nützliche Links

- **Offizielle Downloads:** https://assets.idana.app/downloads
- **Selbstschulung:** https://praxis.idana.com/idana-selbstschulung#
- **Implementierungsportal:** https://praxis.idana.com/portal-zur-implementierung
- **Status-Seite:** https://status.idana.com
- **Schwachstellen-Register:** https://portal.idana.app/vulnerabilities

---

Dokumentinformationen

Titel: Leitlinie zur sicheren Nutzung des Idana Cloud-Dienstes für Kunden
Version: 1.0
Datum: 03.11.2025
Verantwortlich: IT-Sicherheitsbeauftragter (Jerome Meinke) und Head of Customer Success (Johannes Lederich)
Genehmigt von: Lucas Spohn
Überprüfungsintervall: Jährlich oder bei wesentlichen Änderungen am Cloud-Dienst
Nächste Überprüfung: 06.11.2026
Zielgruppe: Cloud-Kunden (Arztpraxen und medizinische Einrichtungen)
Veröffentlichung: Öffentlich zugänglich über Idana-Website und Support-Portal