IT-RICHTLINIE
der House of Healthcare-Unternehmensgruppe

Einleitung

IT-Sicherheit betrifft jeden einzelnen Mitarbeiter. Im Arbeitsalltag werden regelmäßig personenbezogene, geschäftskritische und besonders schützenswerte Daten verarbeitet. Ein Verlust, Missbrauch oder die Einsicht durch Unbefugte kann schwerwiegende Konsequenzen nach sich ziehen – sowohl für die betroffene Person als auch für unser Unternehmen.

Ziel dieser Richtlinie ist es, einen verantwortungsvollen und sicheren Umgang mit Daten sowie eine zuverlässige IT-Infrastruktur zu gewährleisten.

1. Teilnahme an Schulungen

Alle Mitarbeiter sind verpflichtet, an den von **House of Healthcare / House of HR** angebotenen Schulungen zur IT-Sicherheit und Security Awareness teilzunehmen.

2. Nutzung betrieblicher Geräte

- **Private Nutzung betrieblicher Geräte** (z. B. Computer, Internetzugang) ist untersagt.
- **Privates Streaming** während der Arbeitszeit ist verboten, um Betriebsabläufe nicht zu stören.

3. Dienstliche Nutzung privater Geräte

- Die Nutzung privater Geräte für dienstliche Zwecke ist **grundsätzlich untersagt**.
- Dies gilt insbesondere für:
  - Zugriff auf dienstliche E-Mails (z. B. über Office 365).
  - Nutzung von Firmensoftware (zvoove o. Ä.) auf privaten Geräten.
  - Speicherung dienstlicher Daten auf privaten Speichermedien (USB, SD-Karten etc.).
  - Die Nutzung privater Geräte für den Zugriff auf die konzernweite MS365 Cloud, incl. aller MS Office Produkte, wird durch globale Richtlinien von HoHR unterbunden.
- **Ausnahme:** Die Verwendung der MS Authenticator App auf privaten Smartphones, sofern kein dienstliches Gerät zur Verfügung steht.

4. E-Mail-Nutzung

- Dienstliche E-Mail-Adressen dürfen ausschließlich zu dienstlichen Zwecken genutzt werden.
- **Verdächtige E-Mails** (z. B. Phishing) dürfen nicht geöffnet und müssen gelöscht werden.
- **Links** sind zunächst durch Rechtsklick → „Hyperlink kopieren“ zu prüfen, bevor sie aufgerufen werden.
- **Spam-Nachrichten** nicht beantworten oder abbestellen.
- **BCC-Funktion** bei externem Massenversand ist verpflichtend.
- Nach Austritt behält sich **House of Healthcare** das Recht vor, die dienstliche E-Mail-Adresse vorübergehend weiterzuleiten.

5. Zugangsdaten und Verschlüsselung

- Kommunikation über das Internet muss verschlüsselt erfolgen (erkennbar am Schloss-Symbol im Browser).
- Zugangsdaten sind **nicht in E-Mails oder Dateien zu speichern**. Es wird die Nutzung eines Passwort-Safes empfohlen.
- Nach dem Ausscheiden aus dem Unternehmen ist die Nutzung oder Speicherung von Zugangsdaten untersagt.

6. Verbotene Handlungen aus IT-Sicherheitsgründen

Untersagt sind insbesondere:

- Weitergabe oder Änderung dienstlicher PINs.
- Speicherung auf nicht genehmigten Medien.
- Kennwortschutz von Dateien.
- Veränderung von Unternehmensvorlagen.
- Installation nicht genehmigter Software (nur gemäß „genehmigte Software“-Leitfaden erlaubt).
- Löschen betriebsrelevanter Daten oder E-Mails.
- Websites mit pornografischen, gewaltverherrlichenden oder strafrechtlich bedenklichen Inhalten aufzurufen.

7. Vertraulichkeit und Zugriffsschutz

- **Keine Weitergabe** betrieblicher Daten an Dritte, auch nicht durch Einsichtnahme am Bildschirm.
- Verbot der **Speicherung, Kopie oder Weiterverwendung** zu privaten Zwecken.
- **Passwörter und Chipkarten** dürfen nicht zugänglich aufbewahrt oder weitergegeben werden.
- **Zutritt für betriebsfremde Personen** zur IT-Infrastruktur ist untersagt.
- **Technische Veränderungen** an bereitgestellten Geräten sind verboten.
- **Verlust personenbezogener Daten** ist sofort der Rechtsabteilung zu melden.

8. Entsorgung von Daten

Die Entsorgung von Dokumenten hat in der Betriebsstätte über den dort zur Verfügung gestellten Dokumenten-Schredder oder durch das von der Niederlassung beauftragte, auf die Entsorgung spezialisierte Dienstleistungsunternehmen zu erfolgen. Über die fachgerechte Entsorgung ist ein Zertifikat auszustellen. **Es ist untersagt, Dokumente durch den Papierkorb zu entsorgen.**
Nicht mehr benötigte Datenträger (USB Stick, Festplatte, SD Karte, CD/DVD etc.) sind an die IT-Abteilung zu übergeben.

9. Arbeiten außerhalb der Betriebsstätte

Die Tätigkeit außerhalb der ersten Tätigkeitsstätte darf ausschließlich über eine angemessen abgesicherte Verbindung, z. B. sogenanntes Virtual Private Network (VPN) über alle Kommunikationswege einschließlich des genutzten heimischen WLAN/WiFi-Netzes sowie der Internetanbindung über Festnetz erfolgen. WiFi Zugänge müssen mit einem sicheren Passwort abgesichert sein. Das Arbeiten in folgenden Ländern ist untersagt und wird per globaler Richtlinie blockiert: Blocked Countries.

10. Bildschirm- und Arbeitsplatzschutz

Der Arbeitsplatz ist so zu gestalten, dass **Dritte keine Einsicht** in personenbezogene Daten erhalten.

11. Abwesenheit vom Arbeitsplatz

Bei Verlassen des Arbeitsplatzes (auch kurzfristig) gilt:

- Computer sperren (z. B. per Tastenkombination Windows + L).
- Fenster schließen, sofern Einbruchrisiko besteht.
- Dokumente sicher einschließen oder Büro verschließen.

12. Vertrauliche Gespräche

Telefonate und Videokonferenzen mit vertraulichen Inhalten sind so zu führen, dass Unbefugte nichts mithören können (z. B. keine Gespräche auf Balkon oder in Cafés).

13. Herausgabe betrieblicher Daten

Sämtliche dienstliche Daten bleiben Eigentum von House of Healthcare. House of Healthcare kann jederzeit die vollständige Herausgabe aller Daten und Zugangsmittel verlangen. Ein Zurückbehaltungsrecht besteht nicht.

14. Meldung von Störungen

Auffälligkeiten (z. B. Fehlermeldungen, Geräteeinbußen) sind unverzüglich der IT-Abteilung zu melden. Das betrifft auch den Verlust des Arbeitsgeräts.

15. Überprüfung von Kommunikation

Sämtliche Kommunikations- und Dokumentationsabläufe werden grundsätzlich gespeichert. Im berechtigten Interesse können diese zu jeder Zeit überprüft und analysiert werden.

16. Gültigkeit und Änderungen

- Diese Richtlinie ist Bestandteil aller Arbeitsverträge und gilt auf unbestimmte Zeit.
- **House of Healthcare** kann die Richtlinie jederzeit mit Wirkung für die Zukunft ändern oder aufheben.
- Die jeweils aktuelle Version ist einzusehen unter „Richtlinien und Formulare“ oder den rechts abgebildeten QR-Code.

17. Konsequenzen bei Verstößen

Verstöße gegen diese Richtlinie können zu arbeitsrechtlichen Maßnahmen führen sowie zivilrechtliche, bußgeldbewehrte oder strafrechtliche Folgen nach sich ziehen (z. B. gemäß Art. 83 DSGVO, § 42 BDSG, § 23 GeschGehG).