Verfahrensanweisung (VA)
(Dokumentierte Information)

Unternehmensinterne Informationssicherheitsrichtlinie 07533

Version 0.1

Stand: 15.08.2025

Änderungsübersicht

Datum	Version	Beschreibung/Grund der Änderung	Autor
15.08.2025	0.1	Ersterstellung	TA

Freigabe des Dokuments der aktuellen Version

Datum	Verantwortlich	Name	NZ
15.08.2025	Managementbeauftragter	G. Ultes	G U

Inhaltsverzeichnis

Abkürzungen

IMS	Integriertes Managementsystem
■	Qualitätsrelevanter Inhalt
■	Umweltrelevanter Inhalt
■	Arbeitsschutzrelevanter Inhalt

Organisatorisches

1.1 Art der Anweisung

Bei dieser dokumentierten Information handelt es sich um eine:

☐ Prozessbeschreibung ☒ Verfahrensanweisung ☐ Arbeitsanweisung

1.2 Zuordnung

Diese dokumentierte Information stellt als Anweisung im Rahmen unserer Managementdokumentation ergänzende Informationen zur nachfolgenden Prozesseben zur Verfügung:

☒ Kernprozess/e ☐ Unterstützungsprozess/e ☐ Managementprozess/e

1.3 Zweck

1.4 Geltungsbereich

Unternehmensinterne Informationssicherheitsrichtlinie

1.4.1 Eingabequellen (Woher)

.....Normelemente

<Nr>	<Norm>	<Bezeichnung>
[1]	9001:2015-11	[8.4] Steuerung von extern bereitgestellten Prozessen, Produkten und Dienstleistungen
		[8.4.2] Art und Umfang der Steuerung

1.5 Mitgeltende Unterlagen

Jeweils in der aktuellen Fassung:

<Nr>	<Art>	<Bezeichnung>
[1]	VA 07531	Datenschutz
[2]	VA 07532	Notfallplan Notfallkontaktliste Cyberangriff

1.6 Verteiler

<Nr>	<Bezeichnung>
[1]	Alle Mitarbeiter der Firmengruppe mit entsprechenden Endgeräten

2 Verfahren

2.1 Zweck und Zielsetzung

Diese Richtlinie legt die unternehmensweit verbindlichen Grundsätze und Maßnahmen zur Informationssicherheit fest. Ziel ist der Schutz aller Informationen – unabhängig von ihrer Form vor Verlust, Manipulation, unbefugtem Zugriff und sonstigem Missbrauch.

Sie dient dem Erhalt der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und unterstützt die Einhaltung gesetzlicher, vertraglicher und regulatorischer Anforderungen.

Bei Fragen oder Vorfällen:

Umgehend direkten Vorgesetzten informieren oder IT/Notfallkontakt:

E-Mail: support@mevalon.de

Tel.: 0621/8455880

2.2 Geltungsbereich

Diese Richtlinie gilt für:

- Alle Mitarbeitenden der Unternehmensgruppe Heidenreich (Heidenreich Dienstleistungen GmbH, Rudolf Lorenz Gebäudereinigung GmbH, Labitzke Gebäudereinigung GmbH)
- Externe Dienstleister und Partner mit Zugriff auf Informationen oder Systeme
- Alle eingesetzten Systeme, Anwendungen, Geräte und Informationsarten (digital und analog)

2.3 Grundsätze der Informationssicherheit

2.3.1 Vertraulichkeit

Informationen dürfen nur autorisierten Personen zugänglich gemacht werden.

2.3.2 Integrität

Daten und Systeme müssen vor unbefugter oder unbeabsichtigter Veränderung geschützt sein.

2.3.3 Verfügbarkeit

Informationen und Systeme müssen für berechtigte Nutzer zuverlässig und zeitgerecht nutzbar sein.

2.3.4 Rechtmäßigkeit und Nachvollziehbarkeit

Alle sicherheitsrelevanten Handlungen müssen im Rahmen geltender Gesetze, Verträge und Richtlinien erfolgen und nachvollziehbar sein.

3 Verhalten und Pflichten der Nutzer

Alle Nutzenden sind verpflichtet:

- Vertrauliche Informationen geschützt zu behandeln

- Zugangsdaten und Authentifizierungsmerkmale (z. B. Passwörter) nicht an Unbefugte weiterzugeben
- Sicherheitsvorgaben einzuhalten und Systeme nur gemäß Berechtigungen zu nutzen
- Sicherheitsvorfälle unverzüglich zu melden
- Keine technischen oder organisatorischen Sicherheitsmaßnahmen zu umgehen oder absichtlich zu deaktivieren (z. B. Deaktivierung von Firewalls, Umgehung von Passwortschutz, Nutzung privater Speicherlösungen ohne Freigabe)

4 Sicherer Umgang mit Passwörtern

Der sichere Umgang mit Passwörtern ist für den Schutz sensibler Daten und Systeme von zentraler Bedeutung. Alle Mitarbeitenden sind verpflichtet, die Vorgaben zur Passwortsicherheit gemäß Kapitel 4.1 einzuhalten.

4.1 Passwortrichtline

Diese Richtlinie erläutert die verbindlichen Vorgaben zur Erstellung, Nutzung und Verwaltung von Passwörtern in unserem Unternehmen – basierend auf den aktuellen Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI, Stand 2025).

4.1.1 Allgemeine Grundsätze

- Passwörter sind persönlich und vertraulich. Die Weitergabe – auch intern – ist (mit Ausnahme der Systemadministratoren) verboten.
- Für jeden Dienst/Zugang ist ein individuelles Passwort zu verwenden.
- Die Nutzung von Mehr-Faktor-Authentifizierung (MFA/2FA) wird, wo technisch möglich, empfohlen.

4.1.2 Anforderungen an sichere Passwörter

- Die Empfehlungen des BSI werden in der Unternehmensgruppe Heidenreich wie folgt umgesetzt:
  - Mindestens 12 Zeichen
  - Nutzung von mindestens 3 der folgenden Zeichengruppen bestehen:

    Großbuchstaben, Kleinbuchstaben, Ziffern (0-9), Sonderzeichen (!§$%&?)
  - Keine erkennbaren Muster (z. B. „Muster123!“ ist unsicher)
  - Kennwort darf nicht den Kontonamen des Benutzers oder mehr als 2 Zechen enthalten, die nacheinander im vollständigen Namen des Benutzers vorkommen:

    z. B.: Benutzername Tatzel: ~~**Tat**zel123%, **Tat**sache123%~~
  - Kennwortchronik: Ein neu vergebenes Passwort darf nach Aktivierung der vorliegenden Passwortrichtlinie dem alten nicht zu stark ähneln (wird automatisch über die Windows-Logik geprüft).
  - Kann aus mehreren zufälligen Wörtern bestehen, z. B. Treppe+Auto+Schach2025!

Empfehlung: Die Passphrasenstrategie bietet im Alltag bessere Merkbarkeit bei höherer Sicherheit.

4.1.3 Passwortverwendung

- Nie dasselbe Passwort für mehrere Accounts verwenden
- Keine Speicherung in Klartext (auch nicht in Notizen, Word-Dateien etc.)

4.1.4 Passwortänderung

- Nur bei Anlass oder Verdacht auf Kompromittierung (unbefugter Zugriff)
- Kein erzwungener regelmäßiger Wechsel (dies ist laut BSI nicht zielführend)
- Bei Änderung: neues Passwort darf nicht ähnlich zum alten sein

4.1.5 Was ist zu vermeiden

- Namen, Geburtsdaten, Haustiere
- Tastaturmuster („qwertz“, „asdfgh“)
- „123456“, „Passwort!“, „Willkommen2023“
- Sonderzeichen nur am Anfang/Ende (vorhersehbar)
- Gleiches Passwort für mehrere Konten

4.1.6 Verdacht auf Missbrauch?

- Bei Sicherheitsvorfällen bitte sofort an support@mevalon.de (Tel.: 06218455880) oder den direkten Vorgesetzten melden
- Indikatoren: Benachrichtigung über Login versuche aus fremden Ländern, Passwort-Reset ohne eigenes Zutun, unerwartete E-Mails zu Anmeldeaktivitäten
- Bei Zutreffen der Indikatoren: Info an Vorgesetzten und/oder IT und sofortige Passwortänderung einleiten

5 Sicherheitsmaßnahmen und Schutzvorgaben

- Zugriff auf Informationen und Systeme erfolgt ausschließlich nach dem Need-to-know-Prinzip (jede Person erhält nur Zugriff auf die Informationen, die sie für die Erfüllung ihrer konkreten Aufgaben benötigt – und nicht mehr)
- Berechtigungen werden rollenbasiert vergeben und regelmäßig überprüft
- Mobile Geräte sind durch technische Schutzmaßnahmen (z. B. PIN, Verschlüsselung) abzusichern
- Sicherheitsupdates und Patches sind zeitnah einzuspielen
- Schutzmaßnahmen (z. B. Anti-Malware, Firewalls, Verschlüsselung) dürfen nicht deaktiviert werden

6 Schulung und Sensibilisierung

Alle Mitarbeitenden mit Zugang zur IT nehmen regelmäßig an verpflichtenden Schulungen zur Informationssicherheit teil. Neue Mitarbeitende werden im Rahmen des Onboardings geschult.

7 Umgang mit Sicherheitsvorfällen

Sicherheitsvorfälle, Verdachtsmomente oder Anomalien (z. B. ungewöhnliche Login versuche, Datenverlust) sind sofort an den IT-Support oder den/die Informationssicherheitsbeauftragte/n zu melden.

Ein standardisierter Vorfalls Prozess gewährleistet die Dokumentation, Bewertung und Nachverfolgung aller Meldungen.

8 Durchsetzung, Kontrolle und Sanktionen

Die Einhaltung dieser Richtlinie wird regelmäßig durch die IT-Leitung überprüft. Verstöße gegen diese Richtlinie – insbesondere das vorsätzliche Umgehen von Sicherheitsmaßnahmen – können zu arbeitsrechtlichen Konsequenzen bis hin zur Kündigung und ggf. strafrechtlichen Verfolgung führen.

9 Revision und Gültigkeit

Diese Richtlinie wird mindestens einmal jährlich überprüft und bei Bedarf angepasst. Änderungen bedürfen der Freigabe durch die Geschäftsführung und werden rechtzeitig veröffentlicht.

10 Inkrafttreten

Diese Richtlinie tritt am 22.08.2025 in Kraft und ersetzt alle vorhergehenden Regelungen zur Informationssicherheit innerhalb der Unternehmensgruppe Heidenreich.

ENDE der Verfahrensanweisung