

Company Security Policy (CSP)

Diese Vorlage dient lediglich als Beispiel und beinhaltet nicht den kompletten Inhalt.

Für eine umfassende Beratung [kontaktieren](#) Sie uns gerne.

| | |
|----------------|--------------------------------|
| Verantwortlich | <name> |
| Freigabe | <name> |
| Status | Entwurf Review Freigegeben |
| Version | x.x |
| Gültig ab | <datum> |
| Klassifikation | -KLASSIFIZIERUNG- |

Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 1 | Allgemeines | 4 |
| 1.1 | Zielsetzung | 4 |
| 1.2 | Zielgruppe | 4 |
| 1.3 | Verstöße | 4 |
| 1.4 | Abweichungen..... | 4 |
| 2 | Rollen und Verantwortlichkeiten | 4 |
| 3 | Allgemeine Vorgaben..... | 5 |
| 3.1 | Meldung von Informationssicherheitsvorfällen..... | 5 |
| 3.2 | Security-Awareness..... | 5 |
| 3.3 | Änderungen im Beschäftigungsverhältnis | 5 |
| 3.4 | Beschaffung von IT-Systemen | 5 |
| 3.5 | Sicherheit bei der Beauftragung von Dritten | 6 |
| 3.6 | Sicherheit in Projekten | 6 |
| 4 | Vorgaben zur Handhabung von Informationen..... | 7 |
| 4.1 | Rollen im Umgang mit Informationen..... | 7 |
| 4.2 | Vertraulichkeit..... | 7 |
| 4.3 | Verfügbarkeit | 10 |
| 4.4 | Integrität | 10 |
| 4.5 | Ablage von Informationen | 11 |
| 5 | Vorgaben zur Nutzung von IT-Systemen | 12 |
| 5.1 | Allgemeine Vorgaben zur Nutzung von IT-Systemen..... | 12 |
| 5.2 | Nutzung von KUNDE IT-Systemen zu privaten Zwecken..... | 12 |
| 5.3 | Verbinden von Fremdgeräten mit der KUNDE IT-Infrastruktur | 13 |
| 5.4 | Verlassen des Arbeitsplatzes..... | 13 |
| 5.5 | Arbeiten außerhalb der KUNDE Büroräumlichkeiten..... | 13 |
| 5.6 | Nutzung von Software..... | 14 |
| 5.7 | Nutzung von Cloud Services | 14 |
| 5.8 | Nutzung von Smartphones und Tablets..... | 15 |
| 5.9 | Nutzung von mobilen Datenträgern | 15 |
| 5.10 | Umgang mit Passwörtern..... | 15 |
| 5.11 | Schutz vor Schadcode | 16 |
| 5.12 | Nutzung des E-Mail-Systems..... | 16 |
| 5.13 | Internetnutzung | 17 |
| 5.14 | Nutzung von Telefonie- und Videokonferenzsystemen | 17 |
| 5.15 | Protokollierung..... | 17 |
| 6 | Vorgaben an die physische Sicherheit | 18 |
| 6.1 | Betriebsgelände, Gebäude und Zonen..... | 18 |
| 6.2 | Zutrittskarten / Schlüssel | 19 |
| 6.3 | Umgang mit Sicherheitseinrichtungen..... | 19 |
| 6.4 | Mitnahme von IT-Equipment | 19 |

| | |
|---|----|
| 6.5 Umgang mit Fundsachen | 19 |
| 6.6 Mitbringen von firmenfremdem Material | 20 |
| 6.7 Besucherregelungen | 20 |
| 6.8 Notfälle..... | 20 |

Farblegende Mustervorlage:

Anpassen an unternehmensspezifische Begrifflichkeiten

Anpassen anhand der Unternehmensvorgaben (z.B. private Nutzung erlaubt/verboten)

MUSTERBEISPIEL

1 Allgemeines

1.1 Zielsetzung

Ziel dieser Richtlinie ist es verbindliche Vorgaben an die Nutzung von IT-Systemen und an den Umgang mit geschäftlichen Informationen der **Beispiel Kunde GmbH (KUNDE)** zu definieren, und die Risiken einer unsachgemäßen Nutzung zu reduzieren.

1.2 Zielgruppe

Die Vorgaben in dieser Richtlinie sind für alle Mitarbeiter der **KUNDE** verbindlich.

Die Einhaltung der Vorgaben dieser Richtlinie gilt gleichermaßen für Mitarbeiter der **KUNDE** als auch für externe bzw. temporäre Mitarbeiter (Berater, Freelancer, Mitarbeiter von Fremdfirmen, Mitarbeiter von Dienstleistern, Zeit- bzw. Leiharbeitskräfte, Mitarbeiter aus Arbeitnehmerüberlassung, Werkstudenten, Praktikanten, ...) die Aufgaben im Namen der **KUNDE** erbringen bzw. bei der Leistungserbringung der **KUNDE** mitwirken.

1.3 Verstöße

Verletzungen bzw. die Missachtung von den Vorgaben dieser Richtlinie können sanktioniert werden. Einzelheiten sind in der Information Security Policy (ISP) der **KUNDE** (Kap. 1.4) beschrieben.

1.4 Abweichungen

Option 1 Ausnahmeprozess nachfolgend:

Abweichungen von den Vorgaben dieser Richtlinie müssen an den **Informationssicherheits-beauftragten (ISB)** gemeldet werden. Der ISB muss die Abweichung bewerten und – je nach Risiko – ablehnen, oder genehmigen.

Abhängig vom Risiko der Regelabweichung kann eine Genehmigung pauschal, oder unter Auflagen gewährt werden, d.h. die Regelabweichung ist nur zulässig, sofern die definierten risikominimierenden Maßnahmen umgesetzt werden.

Eine Ausnahme kann dabei sowohl dauerhaft als auch temporär genehmigt werden. Die Entscheidung der Ablehnung bzw. Genehmigung (inkl. Dauer der genehmigten Ausnahme) muss vom ISB dokumentiert und nach Ablauf der Frist erneut überprüft werden.

Option 2 Verweis auf Ausnahmeprozess:

Abweichungen von den Vorgaben dieser Richtlinie müssen gemäß des ISMS-Ausnahmebehandlungsprozesses gehandhabt werden.

2 Rollen und Verantwortlichkeiten

Rollen und Verantwortlichkeiten im Rahmen dieser Richtlinie sind in der ISP (Kap. 2) beschrieben.

3 Allgemeine Vorgaben

3.1 Stellung von Informationssicherheitsbeauftragten

Die Informationssicherheitsbeauftragten (ISB) werden von der Abteilung für Informationssicherheit (AIS) ernannt und sind für die Umsetzung der ISMS-Maßnahmen verantwortlich.

Die ISB sind für die Umsetzung der ISMS-Maßnahmen in den verschiedenen Abteilungen zuständig.

1. ISB

2. ISB

3.2 Security-Awareness

Die Sensibilisierung aller Mitarbeiter über alle wesentlichen Gefährdungen und Risiken ist ein wesentlicher Bestandteil eines funktionierenden ISMS.

- Alle Mitarbeiter müssen regelmäßig (= mind. jährlich) an den angebotenen Security Awareness **Maßnahmen** (insb. Security eLearning) teilnehmen.
- Der **verantwortliche Abteilungsleiter | die Personalabteilung | der direkte Vorgesetzte** muss sicherstellen, dass die angebotenen Security-Awareness-Maßnahmen von allen Mitarbeitern im eigenen Verantwortungsbereich wahrgenommen werden und dass die erforderliche Zeit für die Teilnahme zur Verfügung steht.
- Die **Personalabteilung** muss die Teilnahme regelmäßig auswerten, kontrollieren und bei Bedarf intervenieren.

Neue Mitarbeiter müssen zeitnah (im Rahmen der Einarbeitungsphase) **das Security eLearning** absolvieren.

3.3 Änderungen im Beschäftigungsverhältnis

Im Falle von personellen Änderungen (interner Wechsel, Beendigung des Beschäftigungsverhältnisses) muss Folgendes berücksichtigt werden:

- Der zuständige **Abteilungsleiter** muss frühzeitig (bei Bekanntwerden der personellen Veränderung) die Personalabteilung informieren.
- Die **Personalabteilung** muss sicherstellen, dass das Offboarding des Mitarbeiters initiiert wird und ordnungsgemäß / vollständig durchgeführt wird.
- Im Rahmen des Offboardings muss die **Personalabteilung (gemeinsam mit dem Abteilungsleiter)** sicherstellen, dass
 - nicht mehr benötigte Berechtigungen entfernt bzw. angepasst werden.
 - nicht mehr benötigt e Accounts deaktiviert bzw. gelöscht werden.
 - nicht mehr benötigtes IT-Equipment (u.a. Notebook, Smartphone, Datenträger, Authentifizierungstokens, Zutrittskarten und -Schlüssel, ...) zurückgegeben werden.
- **Weiterführende Informationen sind in der Policy Personnel Security zu finden.**

3.4 Beschaffung von IT Systemen

Die Beschaffung von IT Systemen erfolgt über die Personalabteilung (AIS) und ist an die ISMS-Maßnahmen gebunden.

| | |
|-------------------|-------------------|
| [Blurred content] | [Blurred content] |

Diese Vorlage dient lediglich als Beispiel und beinhaltet nicht den kompletten Inhalt.
Für eine umfassende Beratung [kontaktieren](#) Sie uns gerne.

[Blurred footer text and additional content]

5.10 Umgang mit Passwörtern

Jeder Mitarbeiter erhält zur Nutzung der IT-Systeme einen eigenen, personalisierte Benutzeraccount.

- Jeder Mitarbeiter trägt die Verantwortung für sämtliche Aktionen, die mit dem Account durchgeführt werden.
- Passwörter dürfen nicht weitergegeben werden – auch nicht an Vorgesetzte, IT-Mitarbeitern oder anderen Kollegen. Auch im Fall einer Stellvertretung (Urlaub, Abwesenheit) dürfen Passwörter nicht weitergegeben werden. In solchen Fällen müssen die vorgesehenen Stellvertretungsfunktionen genutzt werden.
- Passwörter dürfen nicht aufgeschrieben werden. Stattdessen sollen Passwortsafes genutzt werden. **Diese können durch die IT bereitgestellt werden.**
- Passwörter dürfen nicht in automatischen Anmeldeprozeduren (z.B. Makros, Skripten, ...) oder im Webbrowser gespeichert werden.
- Nutzer mit mehreren Accounts müssen für jeden Account ein separates Kennwort verwenden. Auch die Wiederverwendung desselben Passworts zwischen privaten und geschäftlichen Accounts soll vermieden werden.
- Bei vermutetem oder festgestelltem Missbrauch des Benutzeraccounts muss dies als InfoSec-Vorfall (siehe Kap. 3.1) gemeldet werden.
- Bei der Eingabe des Passworts muss darauf geachtet werden, dass die Eingabe nicht beobachtet wird.

Als sicheres Passwort (betrifft Benutzer-Passwörter) wird bei **KUNDE** Folgendes verstanden:

- **Länge:** 12 Zeichen
- **Komplexität:** 3 aus 4 (d.h. Passwörter müssen Zeichen aus mindestens 3 der nachfolgenden 4 Zeichengruppen enthalten):
 - Großbuchstaben: A B C D E F ...
 - Kleinbuchstaben: a b c d e f ...
 - Ziffern: 0 1 2 3 4 5 ...
 - Sonderzeichen: * ! & % \$ § ... (sofern diese vom jeweiligen IT-System unterstützt werden).
- **Historie:** die letzten 5 Passwörter dürfen nicht wiederverwendet werden.
- **Änderungsintervall:** alle 180 Tage (muss das Passwort geändert werden).
- Verwendete Passwörter dürfen ...
 - keine ganzen Wörter (Passwort, Weißwurst, Rosenheimerherbstfest, ...),
 - keine Kombinationen von Buchstaben / Zahlen mit Gesetzmäßigkeiten (z.B. abc123, test1234, ...) und
 - sollen keine „leicht zu erratende Teile“ oder persönliche Informationen (z.B. Geburtsdatum, Name des Partners, Name der Kinder oder des Haustiers, ...) enthalten.
- Für Accounts mit erhöhten- bzw. administrativen Berechtigungen gelten höhere Passwortanforderungen (definiert in der **Richtlinie zum sichern IT-Betrieb**).
- Eselsbrücken helfen dabei sich auch sichere und komplexe Passwörter zu merken. z.B.
 - Das Passwort besteht aus den Anfangsbuchstaben eines Satzes. Zusätzlich werden bestimmte Zeichen durch Zahlen oder andere Zeichen ersetzt:
In diesem Sommer hat es vier Mal geregnet im Winter acht Mal ==> IdShe4*giW8*
 - Das Passwort besteht aus einem Wort, indem Buchstaben und Zahlen und Sonderzeichen ersetzt wird:
Weißwurst ==> **W3!55wur5t**

1. Zielsetzung des Projekts

Das Projekt hat zum Ziel, die Effizienz der Produktion zu steigern und die Kosten zu senken. Dies wird durch die Implementierung neuer Technologien und die Optimierung der Arbeitsabläufe erreicht.

2. Projektorganisation

Das Projekt wird von einem Projektmanager geleitet, der die Verantwortung für die Umsetzung des Projekts trägt. Ein Projektteam besteht aus Experten für die verschiedenen Bereiche des Unternehmens.

3. Projektbudget

Das Projektbudget beträgt 1.000.000 Euro. Dies umfasst die Kosten für die Anschaffung von Hardware, Software, Schulung und Personal.

4. Projektzeitplan

Das Projekt wird über einen Zeitraum von 12 Monaten durchgeführt. Die wichtigsten Meilensteine sind die Planung, die Implementierung und die Evaluation des Projekts.

5. Projektkommunikation

Die Kommunikation ist ein zentraler Bestandteil des Projekts. Regelmäßige Meetings und Berichterstattungen sind erforderlich, um den Fortschritt zu verfolgen und Probleme zu lösen.

6. Projektabschluss

Das Projekt wird erfolgreich abgeschlossen, wenn die Ziele erreicht sind und die Kosten im Rahmen des Budgets liegen. Ein abschließendes Projektbericht wird erstellt.

Diese Vorlage dient lediglich als Beispiel und beinhaltet nicht den kompletten Inhalt.
Für eine umfassende Beratung [kontaktieren](#) Sie uns gerne.

7. Projektabschluss

Das Projekt wird erfolgreich abgeschlossen, wenn die Ziele erreicht sind und die Kosten im Rahmen des Budgets liegen. Ein abschließendes Projektbericht wird erstellt.

8. Projektabschluss

Das Projekt wird erfolgreich abgeschlossen, wenn die Ziele erreicht sind und die Kosten im Rahmen des Budgets liegen. Ein abschließendes Projektbericht wird erstellt.

9. Projektabschluss

Das Projekt wird erfolgreich abgeschlossen, wenn die Ziele erreicht sind und die Kosten im Rahmen des Budgets liegen. Ein abschließendes Projektbericht wird erstellt.

10. Projektabschluss

Das Projekt wird erfolgreich abgeschlossen, wenn die Ziele erreicht sind und die Kosten im Rahmen des Budgets liegen. Ein abschließendes Projektbericht wird erstellt.

6 Vorgaben an die physische Sicherheit

6.1 Betriebsgelände, Gebäude und Zonen

Die **KUNDE** untergliedert Grundstück(-steile), Gebäude(-teile) bzw. Räumlichkeiten in folgende Sicherheitszonen:

| Sicherheitszone | Beschreibung |
|------------------------|---|
| öffentlicher Bereich | Bereiche und Räume, die keine schutzbedürftigen Informationen oder Einrichtungen beinhalten. Beispiele: Park- und Außenbereiche, Eingangs- und Wartebereiche. |
| Mitarbeiterbereich | Bereiche und Räume, die nicht öffentliche Informationen sowie informationsverarbeitende Einrichtungen mit Zugriffsmöglichkeit auf nicht öffentliche Informationen beinhalten. Beispiele: Großraumbüros, Standardbüros, Besprechungsräume, Gänge innerhalb der Gebäude. |
| Sicherheitsbereich | Bereiche und Räume, in denen zentrale informationsverarbeitenden Einrichtungen vorhanden sind (z.B. Serverraum, Archiv etc.), der Zugriff zu besonders sensiblen Daten ermöglicht wird oder in denen sich Sammeleinrichtungen von zu vernichtenden Unterlagen/Gegenständen befinden. Beispiele: HR-Büro, Archiv, Management-Büros, IT-Arbeitsplätze, Technikräume, Serverräume. |
| Hochsicherheitsbereich | Hochsicherheits-Rechenzentrum von KUNDE . Beispiele: Rechenzentrum. |

Sicherheitsvorgaben für den öffentlichen Bereich

Der Zutritt zu öffentlichen Bereichen ist für Dritte während der Dienst- / Servicezeiten grundsätzlich vorgesehen bzw. gestattet.

- Außerhalb der Dienst- / Servicezeiten muss der Zutritt zu den Gebäuden von **KUNDE** vor dem Zutritt durch Unbefugte geschützt werden.
- Im öffentlichen Bereich dürfen nur Informationen oder informationsverarbeitende Einrichtungen gelagert, betrieben oder bereitgestellt werden, die für die öffentliche Nutzung bestimmt sind.

Sicherheitsvorgaben für den Mitarbeiterbereich

Der Zutritt zum Mitarbeiterbereich ist nur autorisierten Mitarbeitern gestattet. Alle anderen Mitarbeiter (Mitarbeiter ohne Autorisierung) haben ausschließlich Zutritt zu Bereichen, die ihr Arbeitsumfeld bzw. Aufgabengebiet direkt betreffen.

- Der Verantwortliche der Schlüssel- / Kartenverwaltung muss ein Verzeichnis über die zutrittsberechtigten Personen führen.
- Alle nicht autorisierten Personen dürfen sich nur in Begleitung eines autorisierten Mitarbeiters in Mitarbeiterbereichen aufhalten.
- Sofern eine autorisierte Person einen Mitarbeiterbereich verlässt und sich dort kein weiterer autorisierter Mitarbeiter aufhält, muss der Mitarbeiterbereich abgeschlossen bzw. sichergestellt werden, dass keine unbefugten Personen Zutritt zu diesem Bereich erhalten.
- Das Vorhandensein unbekannter Personen im Mitarbeiterbereich, muss freundlich, aber konsequent hinterfragt werden (Grund ihres Aufenthaltes, Ansprechpartner bei **KUNDE**). Falls kein valider Grund für den Aufenthalt vorliegt, muss die Person aufgefordert werden den Mitarbeiterbereich zu verlassen

Wichtig: Dieses Dokument ist ein Entwurf!

Zielsetzung:

1. Zielsetzung des Projekts
2. Zielsetzung der einzelnen Aufgaben
3. Zielsetzung der einzelnen Mitarbeiter
4. Zielsetzung der einzelnen Teams
5. Zielsetzung der einzelnen Abteilungen
6. Zielsetzung der einzelnen Bereiche
7. Zielsetzung der einzelnen Funktionen
8. Zielsetzung der einzelnen Stellen
9. Zielsetzung der einzelnen Mitarbeiter
10. Zielsetzung der einzelnen Teams
11. Zielsetzung der einzelnen Abteilungen
12. Zielsetzung der einzelnen Bereiche
13. Zielsetzung der einzelnen Funktionen
14. Zielsetzung der einzelnen Stellen
15. Zielsetzung der einzelnen Mitarbeiter

Maßnahmen:

Diese Vorlage dient lediglich als Beispiel und beinhaltet nicht den kompletten Inhalt.
Für eine umfassende Beratung [kontaktieren](#) Sie uns gerne.

| Maßnahmen | Ziele |
|------------|--------|
| Maßnahme 1 | Ziel 1 |
| Maßnahme 2 | Ziel 2 |

Bereit, Ihr ISMS aufzubauen?

Lassen Sie uns gemeinsam starten!

[Kontaktieren Sie uns jetzt](#) für eine individuelle Beratung
und Unterstützung.

MUSTERBEISPIEL