hvs consulting

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

Farblegende Mustervorlage:

Anzupassen an unternehmensspezifische Begrifflichkeiten

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

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 Meldung von Informationssicherheitsvorfällen

[illegible]

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.

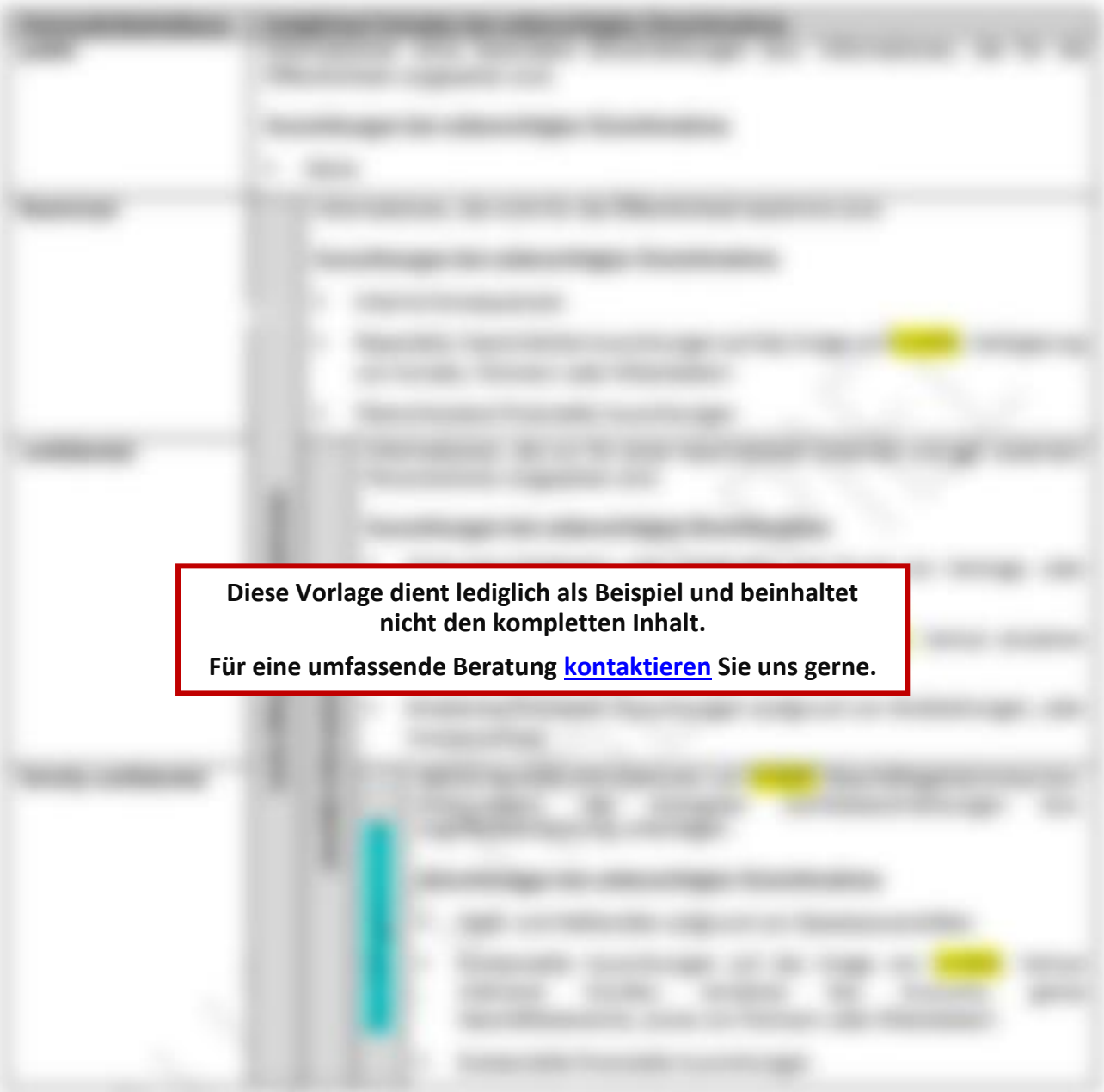
3.3 Änderungen im Beschäftigungsverhältnis

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

[illegible]



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

Für eine umfassende Beratung kontaktieren Sie uns gerne.

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 weitergegebenen werden – auch nicht an Vorgesetze, IT-Mitarbeitern oder anderen Kollegen. Auch im Fall einer Stellvertretung (Urlaub, Abwesenheit) dürfen Passwörter nicht weitergegebenen 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 **d**iesem **S**ommer **h**at **e**s **vier Mal g**eregnet **i**m **W**inter **acht Mal** ==> **IdShe4*giW8***
  - Das Passwort besteht aus einem Wort, indem Buchstaben und Zahlen und Sonderzeichen ersetzt wird: Weißwurst ==> **W3!55wur5t**

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.
Hochsicherheits-bereich	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

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

Für eine umfassende Beratung kontaktieren Sie uns gerne.

Bereit, Ihr ISMS aufzubauen?

Lassen Sie uns gemeinsam starten!

Kontaktieren Sie uns jetzt für eine individuelle Beratung und Unterstützung.