



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	Restricted

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 ISF IT-Systemen zu privaten Zwecken.....	12
5.3	Verbinden von Fremdgeräten mit der ISF IT-Infrastruktur	13
5.4	Verlassen des Arbeitsplatzes.....	13
5.5	Arbeiten außerhalb der ISF 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 **IS-Fox GmbH (ISF)** zu definieren, und die Risiken einer unsachgemäßen Nutzung zu reduzieren.

1.2 Zielgruppe

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

Die Einhaltung der Vorgaben dieser Richtlinie gilt gleichermaßen für Mitarbeiter der **ISF** 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 **ISF** erbringen bzw. bei der Leistungserbringung der **ISF** 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 ISF (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

Als Informationssicherheitsvorfall (InfoSec-Vorfall) wird die Gefährdung der Schutzziele Vertraulichkeit, Verfügbarkeit und/oder Integrität bezeichnet.

Jeder Mitarbeiter muss, festgestellte oder vermutete InfoSec-Vorfälle unmittelbar an den IT-Servicedesk melden:

- Als Ticket: **<mail>**
- Per Telefon: **<tel>**

Beispiele für meldepflichtige InfoSec-Vorfälle sind in Anhang A zu finden.

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 benötigte 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

- Sämtliche IT-Systeme (Hardware, Software, Applikationen, Smartphones, Drucker, Multifunktionsgeräte, ...) müssen durch **die IT** beschaffen werden.
- **Weiterführende Informationen sind in der Policy Sichere Beschaffung von IT-Systemen zu finden.**



Bereit, Ihr ISMS aufzubauen?
Lassen Sie uns gemeinsam starten!
[Kontaktieren Sie uns jetzt](#) für eine individuelle Beratung
und Unterstützung.

MUSTERBEISPIEL