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

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 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.