Cyber­sicherheits-richtli­nie (BAsic)

Vorlage

# Autorität und Überprüfung

## Dokumentenkontrolle und -prüfung

|  |  |
| --- | --- |
| **Dokumentenprüfung**  |  |
| Autor  |  |
| Eigentümer |  |
| Datum der Erstellung |  |
| Zuletzt überarbeitet von  |  |
| Datum der letzten Überarbeitung |  |

## Versionsverwaltung

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Datum der Genehmigung** | **Genehmigt durch**  | **Beschreibung der Änderung** |
| 1.0 |  |  |  |

# Intro

**[Organisation]** ist sich der entscheidenden Rolle bewusst, die Informationen für die heutigen Geschäftsziele spielen. In einer modernen Welt müssen Informationssysteme in hohem Maße miteinander vernetzt und von überall her zugänglich sein. Dies bietet zwar große Chancen, aber das Risiko feindlicher Angriffe oder von Datenverlusten nimmt rapide zu.

Diese Cybersicherheitspolitik legt die Mindestanforderungen fest, die für alle Abteilungen von **[Organisation]** gelten, damit wir unser geistiges Eigentum, unsere geschäftlichen Vorteile und unsere Mitarbeiter vor den Folgen unzureichender Informationssicherheit und etwaiger Cyberangriffe schützen.

Natürlich wird auch auf die Einhaltung von Gesetzen und Vorschriften geachtet.

Gegebenenfalls können die Dienststellen zusätzliche Leitlinien festlegen und zusätzliche Maßnahmen ergreifen, um das erforderliche Sicherheitsniveau zu gewährleisten.

# Politische Grundsätze

**Wir haben wirksame Strategien und Verfahren eingeführt**

Wir sind uns der Risiken für die Informationssicherheit bewusst. Wir erstellen gemeinsam Sicherheitsrichtlinien und -verfahren. Wir wissen, wer verantwortlich ist und wie wir Regeln und Verfahren anwenden.

**Wir kennen unser Umfeld und managen Risiken**

Wir wissen, welche Informationssysteme für **[Organisation]** wichtig sind. Wir kennen die Risiken dieser Systeme und halten sie auf einem akzeptablen Niveau. Ein kontinuierlicher Verbesserungszyklus stellt sicher, dass unsere Sicherheitsniveaus weiterhin an die Veränderungen in unserer Organisation und unserem Umfeld angepasst werden.

**Wir entwickeln sichere Produkte und/oder Dienstleistungen**

Die Produkte und Dienstleistungen von **[Organisation]** werden unter Berücksichtigung der Cybersicherheit und des Datenschutzes entwickelt, getestet und gewartet.

**Wir verfügen über eine solide Infrastruktur**

Die Infrastruktur, von der wichtige Systeme abhängen, ist auf hohe Verfügbarkeit ausgelegt.

**Wir handeln proaktiv**

Wir patchen regelmäßig. Wir kennen die Schwachstellen in unserer Infrastruktur und halten uns über neu entdeckte Schwachstellen auf dem Laufenden. Wir lernen aus Sicherheitsvorfällen und Zwischenfällen.

**Wir gehen ordnungsgemäß mit personenbezogenen Daten um.**

Wir erheben, nutzen und speichern personenbezogene Daten im Einklang mit der DSGVO (Verordnung (EU) 2016/679). Das bedeutet, dass wir die notwendigen technischen und organisatorischen Maßnahmen vorsehen.

# Umfang

Im Allgemeinen gilt diese Cybersicherheitsrichtlinie für alle Informationen und Systeme von **[Organisation],** zusammen mit...

... die von ihnen bereitgestellten Informationssysteme,

... die Menschen (intern und extern), die sie verarbeiten,

... die Geräte, mit denen sie verarbeitet werden,

... die Verfahren, von denen sie abhängt,

... die Standorte, an denen wir arbeiten

... die anderen Aspekte, die ein Risiko darstellen können.

Kritische und vertrauliche Informationen oder Systeme sind Informationen oder Systeme, die der Organisation schaden, wenn ihre Vertraulichkeit, Integrität oder Verfügbarkeit gefährdet ist.

# Mindestanforderungen

Unsere Umgebung wird in einer Weise verwaltet, die zur Cybersicherheit beiträgt.

Dazu gehört, dass:

* Rollen und Zuständigkeiten im Zusammenhang mit der Cybersicherheit definiert sind und sowohl internen als auch externen Beteiligten mitgeteilt werden.
* Ein Inventar aller in der Organisation verwendeten physischen Geräte, Systeme und Software erstellt und gepflegt wird.
* Die für kritische Systeme wichtige Ausrüstung ordnungsgemäß gewartet werden muss, um ihre ständige Verfügbarkeit und Unversehrtheit zu gewährleisten. Wartungsverträge oder Ersatzteile sollten in Betracht gezogen werden.
* Von der Organisation genehmigte Antiviren-, Spyware- oder andere Malware-Programme auf den von der Organisation identifizierten Systemen und Endpunkten installiert und aktualisiert werden sollten.
* Das Unternehmensnetz gemäß den in der Netzsicherheitspolitik festgelegten Anforderungen gesichert wird.
* Die Betriebssysteme für Clients und Server sowie die Anwendungen mit den erforderlichen Patches und Sicherheitsupdates versorgt werden, sowie in der Richtlinie über die Verwaltung von Sicherheitslücken und Patches beschrieben.
* Unsere Mitarbeiter und Subunternehmer regelmäßig über die Cyber-Risiken und -Bedrohungen aufgeklärt werden, denen sie ausgesetzt sein könnten, und darüber, wie sie sich verhalten sollen, wenn sie auf verdächtige Aktivitäten stoßen. **Die 10 goldenen Regeln für Cybersicherheit** werden kommuniziert und jeder Mitarbeiter oder Subunternehmer muss sich verpflichten, diese Regeln einzuhalten.
* Es ein solides Zugangsmanagement gibt, das die folgenden Punkte berücksichtigt:
	+ Mehrstufige Authentifizierung.
	+ Mindestzugang. Detaillierte Richtlinien sind in der Zugangsrichtlinie beschrieben.
	+ Ausreichend sichere Passwörter. Detaillierte Richtlinien sind in der Passwortrichtlinie beschrieben
	+ Kritische und vertrauliche Systeme sollten sich zumindest erfolgreich an- und abmelden.
* Ein Verfahren zur Wiederherstellung kritischer Systeme im Falle einer Katastrophe vorhanden sein sollte. Es sollte ein Verfahren zur Wiederherstellung wichtiger Dokumente oder Aufzeichnungen geben, wenn diese versehentlich gelöscht werden. Detaillierte Richtlinien sind in dem Dokument "Backup and Recovery Policy" beschrieben.

Im Zusammenhang mit Cybersicherheitsvorfällen sollte ein Reaktionsplan vorhanden sein.

Dieses Strategiedokument ist Teil einer Reihe von Strategiedokumenten, die **[Organisation]** bei der Entwicklung einer soliden Cybersicherheitsstrategie unterstützen.