IT-Sicherheitspolitik (Stand 04 | 2024)

Einfluss auf die Sicherheitspolitik auf Basis der ISO 27001 (International Organization for Standardization) und des BSI-Standards (Bundesamt für Sicherheit in der Informationstechnik) hat vor allem die sorgfältige Berücksichtigung von, und Anpassung an, die spezifischen Anforderungen der Stakeholder bei Klüh. Die Sicherheitspolitik wird daher mit den Anforderungen der Chancen- und Risikomatrix von Klüh regelmäßig abgeglichen. Zudem werden regelmäßige Überprüfungen und Aktualisierungen im Rahmen des PDCA-Zyklus (Plan-Do-Check-Act) durchgeführt, um sicherzustellen, dass die Sicherheitspolitik weiterhin effektiv bleibt. Hierzu wird ab sofort die gesamte IT jährlich durch das zentrale QM auditiert und nicht wie bisher im Stichprobenverfahren.

Die Säulen der IT-Sicherheitspolitik bei Klüh stellen sich wie folgt dar:

1. Einleitung:
Die IT-Sicherheit dient dazu alle IT-Assets wie z.B. Computersysteme, Netzwerke, digitale Geräte und Daten von Institutionen oder Unternehmen vor unbefugtem Zugriff, Datenverletzungen, Cyberangriffen und anderen bösartigen Aktivitäten zu schützen. Informationen werden als wertvoller und wichtiger Bestandteil des Klüh Unternehmensvermögens geschützt.

Die IT-Sicherheitspolitik ist eine Anforderung aus der ISO 27001. Alle Anforderungen, wie der Schutz von Daten und Dokumenten, sind grundsätzlich auf einem Basisniveau sicherzustellen. Im Umfeld von kritischer Infrastruktur wird dieses Niveau angehoben, damit betroffene Komponenten, Schnittstellen und Prozesse auf das höchste Schutzniveau ausgerichtet sind. Besonders hohe Ansprüche werden dabei an die klare und eindeutige Beschreibung der Übergänge und Abgrenzungen zwischen den Anspruchsniveaus gestellt.

2. Anwendungsbereich:
Die Sicherheitspolitik gilt für die IT-Infrastruktur aller deutschen Gesellschaften und betrifft alle damit verbundenen Bereiche, Systeme und Prozesse. Die Abstimmung mit den internationalen Einheiten ist fortlaufend.

3. Sicherheitsziele:
Integrität, Vertraulichkeit, Verfügbarkeit und Authentizität sind die Grundlagen unserer IT-Sicherheitspolitik. Sie dienen dabei dem Schutz aller Stakeholder. Es gilt die Ausrichtung an den Prinzipien der ISO 27001 und des BSI-Standards in den zuvor gemachten Einschränkungen.

4. Risikomanagement:
Prozessrisiken werden systematisch ermittelt und in der von QM zur Verfügung gestellten Chancen- und Risikomatrix dokumentiert (Identifizierung, Bewertung und Behandlung von Risiken). Diese wird im Rahmen der Festlegung von Prozessen zur Anwendung eines risikobasierten Ansatzes im Einklang mit den ISO Normen regelmäßig überprüft.

5. Organisation der Informationssicherheit:
Der Informationssicherheitsbeauftragte (ISB) leitet ein Gremium, das Risiken und Chancen bewertet und Angriffe analysiert und bewertet. Der ISB stellt dabei sicher, dass das Gremium 24/7 für die Klüh Organisation und Stakeholdern (Behörden, Kunden) erreichbar ist.

Die Besetzung des Gremiums wird von der Holding Geschäftsführung freigegeben. Neben den Berichten an die Holding Geschäftsführung werden Protokolle an den Compliance- und die Datenschutzbeauftragten verteilt. Die Datenschutzbeauftragten wiederum teilen ihre Informationen mit dem ISB.

6. Asset-Management:
Der ISB und sein Gremium sorgen für die Identifikation und Klassifizierung von Informationen und IT-Ressourcen. Gleichzeitig erfolgt dort die Festlegung von Maßnahmen zur angemessenen Sicherung von Assets.

7. Zugangskontrolle:
Der ISB und sein Gremium legen gemeinsam mit den Datenschutzbeauftragen die Zugriffsberechtigungen und -kontrollen für Systeme und Daten nach Vorgaben der Holding Geschäftsführung fest.

8. Verschlüsselung und Datensicherheit:
Der ISB und sein Gremium sorgen für die Definition von Verschlüsselungsstandards und –verfahren und für die Sicherstellung der Integrität und Vertraulichkeit von Daten.

9. Incident-Management:
Der ISB und sein Gremium sind für die Klärung von Verfahren zur Meldung und Bearbeitung von Sicherheitsvorfällen (sog. Incidents) verantwortlich. Gleiches gilt für die Integration von Incident-Response-Plänen entsprechend den Standards ISO 27001 und BSI in den unterschiedlichen Anwendungsfeldern.

10. Kommunikation und Schulung:
Die Festlegung von Schulungsprogrammen für Mitarbeitende im Bereich Informationssicherheit erfolgt, sofern es notwendig ist, in Abstimmung mit dem Teilnehmenden des Datenschutzmeetings. Gleiches gilt für die Etablierung von Kommunikationsmechanismen für sicherheitsrelevante Informationen.

11. Überwachung und Bewertung:
Klüh hat seit der Einführung der ISO 9001-Systematik die Implementierung von Kontrollmechanismen zur Überwachung der Informationssicherheit vorangetrieben. Diese Instrumente werden durch den ISB und sein Gremium übernommen, regelmäßig bewertet und auf den aktuellen Stand der Sicherheitspolitik gebracht.
Der ISB wird dabei vom Leiter QM und den Datenschutzbeauftragten unterstützt.

12. Dokumentation und Aufzeichnungen:
Die Festlegung von Anforderungen an die Dokumentation von Sicherheitsmaßnahmen erfolgt im Rahmen des Managementsystems. Dabei stellt der Leiter QM die Verfügbarkeit von Aufzeichnungen für Audits und Überprüfungen sicher.