Bundesamt
für Sicherheit in der
Informationstechnik

Richtlinie zur internen ISMS-Auditierung

Dokumenteneigenschaften

Verantwortung	Informationssicherheitsbeauftragter (ISB)
Klassifizierung	S2 intern
Gültigkeitszeit	Unbegrenzt
Überarbeitungsintervall	Jährlich
Nächste Überarbeitung	Oktober 2020
Dateiname	A.0.4_Richtlinie_zur_internen_ISMS-Auditierung

Dokumentenstatus und Freigabe

Status	**Version**	**Datum**	**Name und Abteilung/Firma**
Erstellt	1.0	tt.mm.jjjj	

Dokumentenhistorie

Version	**Änderung**	**Datum**	**Autor**
1.0		tt.mm.jjjj	

Inhaltsverzeichnis

1 Kontext

1.1 Einleitung

Die RECPLAST GmbH hat ein Managementsystems für Informationssicherheit (ISMS) etabliert, das dem Regelwerk „IT-Grundschutz“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) genügt. Zentraler Bestandteil eines ISMS ist u.a. die regelmäßige Kontrolle durch ein internes ISMS-Audit. Die vorliegende Richtlinie beschreibt die Vorgaben zur Durchführung der internen ISMS-Audits.

1.2 Geltungsbereich

Die vorliegende Richtlinie gilt für die Durchführung interner ISMS-Audits zur Kontrolle des Managementsystems für Informationssicherheit (ISMS) der RECPLAST GmbH gem. IT-Grundschutz. Der Geltungsbereich ist damit der Geltungsbereich des ISMS, wie in der Strukturanalyse beschrieben. Die Richtlinie gilt für die internen Auditoren, die diese Richtlinie anwenden, sowie alle Mitarbeiter im Geltungsbereich, um die internen ISMS-Audits zu unterstützen.

1.3 Ansprechpartner

Ihr Ansprechpartner zu allen Fragen dieser Richtlinie: Informationssicherheitsbeauftragter (ISB)

2 Prozessbeschreibung

2.1 Verantwortlich

Verantwortlich für die Durchführung der internen ISMS-Audits ist der interne ISMS-Auditor.
Selbstverständlich soll der interne ISMS-Auditor nicht seinen eigenen Bereich auditieren.
An den internen ISMS-Auditor werden folgende Anforderungen gestellt:

- Kenntnisse in Informationstechnik und -sicherheit
- Kenntnisse in der IT-Grundschutz-Methodik
- Kenntnisse in Auditierung (etwa gem. ISO 19011)

Sowohl das Management als auch alle Mitarbeiter unterstützen den Prozess zur Durchführung interner ISMS-Audits.

2.2 Prüfzyklen

Interne ISMS-Audits werden jährlich durchgeführt.

2.3 Umfang

Das interne ISMS-Audit umfasst folgende Punkte:

- A.0-Referenzdokumente
- A.1: Strukturanalyse
- A.2: Schutzbedarfsanalyse
- A.3: Modellierung
- A.4: IT-Grundschutz-Check
- A.5: Risikoanalyse

Schwerpunkt des internen ISMS-Audits ist der IT-Grundschutz-Check.
Für den IT-Grundschutz-Check wird ein Auditplan erstellt, der über drei Jahre vorgibt, welche Anforderungen wann geprüft werden.
Beim internen ISMS-Audit sind zu prüfen:

- Aktualität der Angaben
- Umsetzungsstand der Vorgaben
- Wirksamkeitsprüfung

2.4 Dokumentation

Das interne ISMS-Audit wird vollumfänglich dokumentiert:

- Auditplanung
- Dokumentation der Prüfung der A.0-A.3 und A.5-Dokumente.
- Dokumentation des IT-Grundschutz-Checks (A.4).

Die Auditdokumentation soll wiedergeben:

- wer
- wann

- wen
- zu welchem Sachverhalt (Zielobjekt, Baustein, Referenzdokument,...) befragt hat und
- welche Feststellungen getroffen wurden.

Es sind folgende Feststellungen vorgesehen:

- erfüllt: Dokument ist aktuell, Sachverhalt trifft zu oder Maßnahme ist wirksam umgesetzt
- Empfehlung: grundsätzlich gilt „erfüllt“, es gibt aber Verbesserungspotential
- Abweichung: Dokument ist nicht aktuell, Sachverhalt trifft nicht zu und/oder eine Maßnahme ist nicht oder nicht wirksam umgesetzt

Das interne ISMS-Audit wird durch einen Bericht abgeschlossen.
Etwaige Nicht-Konformitäten (Abweichungen und Empfehlungen) werden klar gekennzeichnet.
Der Bericht zum internen ISMS-Audit geht in die Managementbewertung ein.

2.5 Umgang mit Abweichungen und Empfehlungen

Nicht-Konformitäten (Abweichungen und Empfehlungen) gehen in den kontinuierlichen Verbesserungsprozess ein.

3 Inkrafttreten

Die Richtlinie tritt zum 01.11.2019 in Kraft.
Freigegeben durch: Geschäftsführung Bonn, 26.10.2019, UNTERSCHRIFT GF