

Informationssicherheitspolitik

Kappel & Dierolf GmbH & Co. KG

Zweck und Geltung Wir ermöglichen verlässliche Arbeitsabläufe durch IT- und Cloud-Lösungen, Managed Services, Dokumentenmanagement sowie Druck- und Scanlösungen einschließlich Produktionsdruck. Dazu schützen wir Vertraulichkeit, Integrität und Verfügbarkeit eigener und anvertrauter Informationen in jeder Form.

Diese Politik gilt unternehmensweit für alle Beschäftigten, Prozesse und Systeme; externe Mitwirkende werden vertraglich entsprechend verpflichtet.

Führung und Sicherheitsziele Die Geschäftsführung verantwortet das Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001:2022, stellt Ressourcen bereit und legt Zuständigkeiten fest. Der Informationssicherheitsbeauftragte koordiniert die Umsetzung.

Diese Politik bildet den Rahmen für dokumentierte, soweit praktikabel messbare Sicherheitsziele. Die Geschäftsführung genehmigt Ziele, Verantwortliche, Maßnahmen und Termine; Kennzahlen zeigen Fortschritt und Wirksamkeit.

Risiken und Schutzmaßnahmen Wir bewerten Risiken regelmäßig und bei wesentlichen Änderungen, einschließlich relevanter physischer, Umwelt- und Klimarisiken. Schutzbedarf und Risiken bestimmen angemessene Maßnahmen nach dem Stand der Technik; Risikoverantwortliche genehmigen die Behandlung und akzeptieren Restrisiken dokumentiert. Die Erklärung zur Anwendbarkeit begründet die Auswahl der Maßnahmen. Wir erfassen Informationswerte und schützen sie über ihren Lebenszyklus. Schwerpunkte sind minimale Zugriffsrechte, sichere Administration und Fernwartung, Multifaktor-Authentifizierung, Verschlüsselung, Kundentrennung, physischer Schutz sowie sichere Datenlöschung bei Geräteübergabe. Sichere Beschaffung, Entwicklung und Änderungen, Überwachung sowie zeitnahe Schwachstellenbehandlung und Updates werden verbindlich geregelt. Cloud- und KI-Anwendungen, auch zur Belegverarbeitung, benötigen eine risikobasierte Freigabe und klare Vorgaben zum Datenschutz und Geheimnisschutz.

Menschen und Lieferkette Beschäftigte und Führungskräfte werden regelmäßig und aufgabenbezogen geschult. Alle beachten die Sicherheitsvorgaben und melden Verdachtsfälle unverzüglich über die festgelegten Meldewege.

Wir bewerten Lieferanten und Unterauftragnehmer risikobasiert, vereinbaren Sicherheits-, Nachweis- und Informationspflichten und überwachen deren Einhaltung. Für Kundenleistungen werden Zuständigkeiten und Sicherheitsanforderungen eindeutig vereinbart.

Verpflichtungen und NIS2 Wir verpflichten uns zur Erfüllung anwendbarer gesetzlicher, behördlicher und vertraglicher Informationssicherheitsanforderungen einschließlich Datenschutz. Dazu gehören vereinbarte Lieferkettenanforderungen NIS2-betroffener Kunden, angemessene Sicherheitsnachweise und Unterstützung bei deren Vorfallbearbeitung. Eine eigene gesetzliche Betroffenheit nach dem BSI-Gesetz prüfen wir gesondert und erfüllen daraus folgende Pflichten.

Vorfälle und Betriebsfortführung Wir regeln Erkennung, Bewertung, Eindämmung und Aufarbeitung von Sicherheitsvorfällen. Betroffene Kunden informieren wir unverzüglich nach den vereinbarten Verfahren so, dass sie ihre Meldepflichten erfüllen können.

Eigene gesetzliche Meldepflichten bleiben unberührt. Geschützte Datensicherungen, getestete Wiederherstellung sowie Notfall- und Krisenpläne mit gesicherter Kommunikation unterstützen vereinbarte Wiederanlaufziele.

Wirksamkeit und Verbindlichkeit Wir verpflichten uns zur fortlaufenden Verbesserung des ISMS. Kennzahlen, interne Audits und Managementbewertungen prüfen seine Wirksamkeit; Abweichungen werden behoben. Ergänzende Richtlinien und Prozesse konkretisieren diese Politik.

Sie wird mindestens jährlich und anlassbezogen überprüft, von der Geschäftsführung freigegeben, intern bekannt gemacht und relevanten interessierten Parteien öffentlich bereitgestellt.