Richtlinie zur Informationssicherheit für Lieferanten und IT-Dienstleister

Änderungen

Datum	*Version*	*Autor*	*Beschreibung*
14.05.2020	V000	M.Frik	Erste Version der Dokumentvorlage mit Kopf- und Fußzeile.
15.09.2020	V001	AP	Überarbeitung der Texte, Einfügen der Dienstleisterliste und Sicherheitsklassifizierung
12.04.2023	V002	PBA	Prüfung und Aktualisierung des Anwendungsbereichs
31.05.2023	V003	PBA	Erweiterung mit ABT SE
17.08.2026	V004	CDI	Anpassung an neue RL zu Dokumentierten Informationen

Inhaltsverzeichnis

1. Über das Verfahren

1.1. Ziel und Zweck

Diese Richtlinie definiert die Anforderungen an die Informationssicherheit bei der Zusammenarbeit mit Lieferanten, Dienstleistern und IT-Dienstleistern.
Ziel ist es, Informationen, Geschäftsprozesse, IT-Systeme und sonstige Unternehmenswerte vor Verlust, unbefugtem Zugriff, unbefugter Veränderung, Offenlegung, Missbrauch und Ausfall zu schützen.
Die Anforderungen dieser Richtlinie sollen insbesondere sicherstellen, dass Informationssicherheitsrisiken bereits bei der Auswahl und Beauftragung von Lieferanten berücksichtigt, während der Vertragslaufzeit überwacht und bei Beendigung der Geschäftsbeziehung kontrolliert reduziert werden.

1.2. Anwendungsbereich

Diese Richtlinie gilt für alle externen Organisationen und Personen, die im Auftrag der Unternehmen der ABT-Gruppe Leistungen erbringen und dabei unmittelbar oder mittelbar:

- auf Informationen des Unternehmens zugreifen
- personenbezogene Daten verarbeiten
- IT-Systeme oder Netzwerke nutzen
- Anwendungen entwickeln, betreiben oder warten
- Hardware, Software oder IT-Komponenten liefern
- Cloud-, Hosting-, Rechenzentrums- oder Managed-Services bereitstellen
- Gebäude, technische Anlagen oder sonstige Infrastruktur betreiben
- administrative oder technische Unterstützung leisten
- vertrauliche Geschäftsunterlagen erhalten
- sonstige Leistungen mit Einfluss auf die Informationssicherheit erbringen.

Die Anforderungen gelten unabhängig davon, ob die Leistung am Unternehmensstandort, beim Lieferanten, remote oder über Cloud-/Internetdienste erbracht wird.

1.3. Zuständigkeiten

Die Verantwortlichkeiten zwischen den Unternehmen der ABT-Gruppe und dem externen Dienstleister müssen eindeutig festgelegt, dokumentiert und umgesetzt werden.
Dies gilt insbesondere für Cloud- und Managed Services mit geteilten Verantwortlichkeiten.
Die Klassifizierung obliegt dem Verantwortlichen EDV-Leiter, der Geschäftsleitung und den jeweiligen verantwortlichen Fachbereichen (Informationseigner).

2. Verantwortlichkeiten

Geschäftsführung / Vorstand

- genehmigt diese Richtlinie
- stellt angemessene Ressourcen bereit
- trägt die Gesamtverantwortung für die Umsetzung

Informationssicherheitsbeauftragter (ISB)

- definiert Sicherheitsanforderungen
- unterstützt bei Risikobewertungen
- überwacht die Einhaltung der Richtlinie
- koordiniert Sicherheitsbewertungen und Audits

Einkauf
- berücksichtigt Informationssicherheit bei der Lieferantenauswahl
- stellt die erforderliche Vertragsdokumentation sicher
- führt bzw. koordiniert das Lieferantenmanagement

IT
- setzt technische Sicherheitsanforderungen um
- verwaltet externe Zugriffe
- überwacht technische Sicherheitsmaßnahmen
- unterstützt bei Sicherheitsvorfällen

Fachbereiche
- bewerten die geschäftliche Kritikalität von Dienstleistern
- definieren fachliche Anforderungen
- überprüfen die fortbestehende Notwendigkeit von Zugriffsrechten

Lieferanten und IT-Dienstleister
- erfüllen die vertraglich vereinbarten Sicherheitsanforderungen
- schützen die ihnen anvertrauten Informationen
- melden Sicherheitsvorfälle
- unterstützen bei Audits und Sicherheitsmaßnahmen

3. Grundsätze

Bei der Zusammenarbeit mit externen Partnern gelten folgende Grundsätze:
- Sicherheitsanforderungen sind Bestandteil der Lieferanten- und Vertragsgestaltung
- Der Umfang der Zugriffsrechte ist auf das erforderliche Maß zu beschränken
- Informationen und Systeme sind entsprechend ihrer Schutzbedürftigkeit zu behandeln
- Dienstleister müssen geeignete technische und organisatorische Sicherheitsmaßnahmen nachweisen
- Sicherheitsvorfälle sind unverzüglich zu melden und gemeinsam zu bearbeiten
- Die Einhaltung vereinbarter Sicherheitsanforderungen ist regelmäßig zu überprüfen
- Unterauftragnehmer dürfen nur unter definierten Bedingungen eingesetzt werden
- Bei Beendigung der Zusammenarbeit sind Zugriffe zu entziehen und Unternehmensinformationen ordnungsgemäß zurückzugeben oder sicher zu löschen

4. Anforderungen an Sicherheitsnachweise

Abhängig von Risiko und Schutzbedarf können von Lieferanten und Dienstleistern geeignete Nachweise verlangen. Mögliche Nachweise sind insbesondere:
- TISAX®-Assessment bzw. TISAX®-Label
- VDA-ISA-Assessment
- ISO/IEC-27001-Zertifikat
- SOC-2-Bericht
- Penetrationstests
- Sicherheitskonzept
- technische und organisatorische Maßnahmen
- Business-Continuity- und Disaster-Recovery-Nachweise
- Nachweise über Schwachstellenmanagement
- Nachweise über Datenschutz und Auftragsverarbeitung

Die Art und der Umfang der Nachweise müssen dem Risiko angemessen sein.
Ein TISAX-Label ersetzt nicht automatisch die individuelle Bewertung des Dienstleisters durch ABT.

5. Risikoklassifizierung

Lieferanten und Dienstleister werden abhängig von ihrer Bedeutung und ihrem Informationszugriff in mindestens drei Risikoklassen eingestuft.

5.1. Kritische Lieferanten – hohes Risiko

Die Einstufung als kritisch erfolgt insbesondere bei:

- Zugriff auf besonders schützenswerte oder vertrauliche Informationen
- Verarbeitung umfangreicher personenbezogener Daten
- administrativem Zugriff auf produktive IT-System
- Betrieb kritischer IT-Infrastrukturen oder Anwendungen
- Abhängigkeit wesentlicher Geschäftsprozesse vom Dienstleister
- Cloud- oder Hosting-Leistungen für kritische Systeme
- potenziell erheblichen Auswirkungen eines Sicherheitsvorfalls

Für kritische Lieferanten sind eine vertiefte Sicherheitsprüfung und erhöhte vertragliche Anforderungen erforderlich.

5.2. Wesentliche Lieferanten – mittleres Risiko

Hierzu gehören Lieferanten mit begrenztem Zugriff auf Unternehmensinformationen oder IT-Systeme sowie Dienstleister, deren Ausfall oder Sicherheitsvorfall relevante, aber beherrschbare Auswirkungen hätte.

5.3. Standard-Lieferanten – geringes Risiko

Hierzu gehören Lieferanten ohne oder mit nur geringem Zugriff auf Unternehmensinformationen und IT-Systeme und ohne wesentliche Abhängigkeit für kritische Geschäftsprozesse.
Die Einstufung ist regelmäßig sowie bei wesentlichen Änderungen der Leistung zu überprüfen.

6. Sicherheitsanforderungen

Folgende Sicherheitsanforderungen gelten für IT-Dienstleister mit Zugriff auf das interne Netzwerk:

- Zugriff wird wenn möglich von statischen IP-Adressen über die Firewall reglementiert
- Verbindungen werden ausnahmslos nach dem aktuellen Stand der Technik verschlüsselt aufgebaut und mit angemessener Identifikation und Authentifizierung versehen
- Falls statische IP nicht möglich, wird der Zugriff nur über Teamviewer gewährt und der Zugriff wird für den gesamten Zeitraum von einem IT-Mitarbeiter überwacht.
- Kennwörter sowie Zugriffsbeschreibungen dürfen ausnahmslos in verschlüsselten Datenbanken (z.B. Keepass etc.) gespeichert werden
- Einsatz zertifizierter Produkte (CC, ITSEC, etc.) und Sicherheitstechnologien
- Einsatz dedizierter Systeme
- Trennung von Test- und Produktionssystemen
- Trennung von eigenen Netzwerken und Kundennetzwerken
- Authentifizierung von IT-Systemen im Netzwerk
- Schutz der Vertraulichkeit, der Authentizität und Integrität transportierter Daten
- Schutz vor maliziösen Code (Viren, Trojaner)

7. Technische und organisatorische Sicherheitsmaßnahmen

Lieferanten und IT-Dienstleister müssen angemessene technische und organisatorische Maßnahmen umsetzen.
Dazu gehören insbesondere:

7.1. Schutz vor Schadsoftware

Systeme und Endgeräte müssen durch geeignete Schutzmaßnahmen gegen Schadsoftware und andere bekannte Bedrohungen geschützt werden.

7.2. Patch- und Schwachstellenmanagement

Sicherheitsrelevante Schwachstellen sind risikoorientiert und innerhalb angemessener Fristen zu beheben. Kritische Sicherheitsupdates müssen priorisiert behandelt werden.

7.3. Verschlüsselung

Vertrauliche und besonders schützenswerte Informationen sind bei Übertragung über unsichere oder öffentliche Netze angemessen zu verschlüsseln. Eine Verschlüsselung gespeicherter Daten ist risikobasiert vorzusehen.

7.4. Protokollierung und Überwachung

Sicherheitsrelevante Aktivitäten, insbesondere administrative Zugriffe und Zugriffe auf kritische Systeme, sind angemessen zu protokollieren und zu überwachen.

7.5. Datensicherung

Für relevante Systeme und Daten sind angemessene Backup- und Wiederherstellungsverfahren vorzusehen. Die Wiederherstellbarkeit muss regelmäßig überprüft werden.

7.6. Sichere Entwicklung

Bei Entwicklung oder Änderung von Software im Auftrag von ABT sind angemessene Maßnahmen für eine sichere Softwareentwicklung anzuwenden. Dazu gehören insbesondere Code-Reviews, Schwachstellenanalysen, sichere Entwicklungsumgebungen und geeignete Tests.

8. Informations- und Sicherheitsvorfälle

Lieferanten und IT-Dienstleister müssen Sicherheitsvorfälle, die ABT oder dessen Informationen und Systeme betreffen können, unverzüglich melden.
Die Meldung muss – soweit verfügbar – mindestens folgende Informationen enthalten:

- Zeitpunkt und Art des Vorfalls
- betroffene Systeme und Informationen
- bekannte oder vermutete Auswirkungen
- bereits eingeleitete Maßnahmen
- Ansprechpartner für die weitere Koordination

Der Dienstleister muss bei der Untersuchung, Eindämmung und Beseitigung des Vorfalls angemessen unterstützen.
Die vertraglich vereinbarten Meldefristen und gegebenenfalls gesetzlich vorgeschriebenen Fristen sind einzuhalten.

9. Unterauftragnehmer

Der Einsatz von Unterauftragnehmern mit Zugriff auf Unternehmensinformationen oder IT-Systeme bedarf der vorherigen Zustimmung von ABT, sofern vertraglich nichts anderes geregelt ist.
Der beauftragte Dienstleister muss sicherstellen, dass seine Unterauftragnehmer mindestens gleichwertige Informationssicherheitsanforderungen erfüllen.
Der Dienstleister bleibt für die Einhaltung der vereinbarten Sicherheitsanforderungen durch seine Unterauftragnehmer verantwortlich.

10. Datenschutz

Werden personenbezogene Daten durch einen Lieferanten oder IT-Dienstleister verarbeitet, sind die Anforderungen der geltenden Datenschutzgesetze einzuhalten.
Insbesondere sind – soweit erforderlich – Regelungen zu folgenden Punkten zu treffen:

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Kategorien personenbezogener Daten
- Kategorien betroffener Personen
- technische und organisatorische Maßnahmen
- Umgang mit Datenschutzverletzungen
- Unterauftragnehmer
- Löschung bzw. Rückgabe personenbezogener Daten
- Unterstützung bei Betroffenenrechten und sonstigen gesetzlichen Verpflichtungen.

11. Überprüfungen

ABT ist berechtigt, die Einhaltung vereinbarter Informationssicherheitsanforderungen risikoorientiert zu überprüfen.
Geeignete Nachweise können beispielsweise sein:

- Zertifikate
- Selbstauskünfte
- Sicherheitsfragebögen
- Penetrationstests
- Auditberichte
- technische Nachweise

Bei kritischen Dienstleistern sind regelmäßige Überprüfungen vorzusehen.
Festgestellte Sicherheitsmängel sind innerhalb einer angemessenen Frist zu beheben. Bei wesentlichen oder wiederholten Verstößen sind geeignete Eskalationsmaßnahmen einzuleiten.

12. Business Continuity Management

Lieferanten, deren Leistungen für wesentliche oder kritische Geschäftsprozesse erforderlich sind, müssen über angemessene Maßnahmen zur Aufrechterhaltung und Wiederherstellung ihrer Leistungen verfügen.
Hierzu können insbesondere gehören:

- Business-Continuity-Pläne
- Notfall- und Wiederanlaufverfahren
- redundante Systeme
- Datensicherungen,
- Ausweichstandorte
- Wiederherstellungstests
- definierte Wiederherstellungszeiten und Wiederherstellungspunkte

Für kritische Dienstleistungen sind die entsprechenden Anforderungen vertraglich festzulegen.

13. Physische Sicherheit

Sofern Dienstleister Zugang zu Unternehmensstandorten, Rechenzentren oder sonstigen schützenswerten Bereichen erhalten, sind die hierfür geltenden Zutritts- und Sicherheitsregelungen einzuhalten.
Unbefugten Personen darf kein Zugang zu schützenswerten Bereichen ermöglicht werden.

14. Umgang mit Unternehmensinformationen

Unternehmensinformationen dürfen ausschließlich für den vereinbarten Geschäftszweck verarbeitet werden.
Lieferanten und IT-Dienstleister müssen insbesondere:

- Informationen vor unbefugtem Zugriff schützen
- Informationen nicht ohne Genehmigung an Dritte weitergeben
- Informationen nicht für eigene Zwecke verwenden
- Kopien auf das erforderliche Maß beschränken
- vertrauliche Informationen sicher übertragen und speichern
- Aufbewahrungs- und Löschfristen einhalten

15. Beendigung der Zusammenarbeit

Bei Beendigung eines Vertrags sind sämtliche Zugriffe des Dienstleisters zu deaktivieren.
Unternehmensinformationen und sonstige Unternehmenswerte sind zurückzugeben oder – sofern vereinbart und zulässig – sicher zu löschen.
Auf Verlangen ist die Löschung angemessen nachzuweisen.
Dabei sind insbesondere zu berücksichtigen:

- Benutzerkonten
- VPN- und Remote-Zugänge
- API-Schlüssel und Zugangsdaten
- Zertifikate und Tokens
- Datenträger
- Dokumente und Kopien
- Cloud- und SaaS-Zugänge
- Backups, soweit diese nach den vereinbarten Löschfristen betroffen sind

16. Verstöße

Verstöße gegen diese Richtlinie sind unverzüglich an den Informationssicherheitsbeauftragen zu melden.
Je nach Schwere des Verstoßes können Maßnahmen wie Nachbesserung, Einschränkung oder Sperrung von Zugängen, zusätzliche Sicherheitsauflagen, Eskalation an die Geschäftsführung oder vertraglich vereinbarte Konsequenzen erforderlich sein.

17. Inkrafttreten

Diese Richtlinie tritt ab 01.09.2026 in Kraft und ist von allen betroffenen internen Stellen sowie im Rahmen der vertraglichen Vereinbarungen von den relevanten Lieferanten und IT-Dienstleistern zu beachten.