Informationssicherheit
für Dienstleister

Richtlinie

Dokumentenlenkung

Bezeichnung:	VDA06_RL_Informationssicherheit für Dienstleister
Version:	1.0
Ausgabedatum:	27.02.2025
Klassifizierung:	Intern
Status:	Freigegeben
Ansprechpartner:	ISB
Freigabe durch:	Geschäftsführung

Änderungshistorie

Version	Datum	Autor	Kommentare
0.5	18.06.2020	SKR	Entwurf
0.6	11.02.2022	ATH	Überarbeitung
0.7	23.02.2022	ATH	Überarbeitung
0.8			
0.9			
1.0	27.02.2025	LKI/FWE	Freigegeben

Abkürzungsliste

Abkürzung	Beschreibung

Mitgeltende Dokumente

Inhaltsverzeichnis

1 Zweck

Richtlinie Informationssicherheit für Dienstleister
Dieses Dokument richtet sich an externe Dienstleister und Geschäftspartner (im Folgenden Dienstleister genannt) der inotec Kunststofftechnik GmbH. Die darin enthaltenen Anforderungen zur Informationssicherheit sind verbindlich einzuhalten. Die Richtlinie orientiert sich dabei an konkreten Vorgaben zur Informationssicherheit von Mitgliedern des Verbands der deutschen Automobilindustrie (VDA) an ihre Zulieferer. Zur Erfüllung der einzelnen Anforderungen gibt es nach Möglichkeit Verweise auf notwendige Dokumente oder technische Umsetzungen im Rahmen der gesetzten Standards (ISO 27001, VDA-ISA).

2 Allgemeine Anforderungen

2.1 Organisatorische Anforderungen

IT-Geräte und Software, welche Informationen der inotec Kunststofftechnik GmbH verarbeiten, müssen dem aktuellen Stand der Technik entsprechen und durch entsprechende Schutzmaßnahmen (z.B: Virenschutz, Verschlüsselung, starke Authentifizierung) abgesichert sein.
Die Weitergabe von Informationen an Dritte darf nur nach erfolgter Freigabe der inotec Kunststofftechnik GmbH erfolgen.
Außerdem ist die Einhaltung aller gesetzlichen Anforderungen zum Schutz von personenbezogener Daten sicherzustellen.
Die Verpflichtung zur Geheimhaltung auf Basis der bestehenden Geheimhaltungsvereinbarung muss vom Dienstleister bei seinen Mitarbeitern sensibilisiert und kontrolliert werden.
Die Verschlüsselung von Daten der inotec Kunststofftechnik GmbH auf mobilen Endgeräten ist zu gewährleisten. Länderspezifische Regelungen zur Verschlüsselung sind zu beachten. Sollte eine Verschlüsselung nicht möglich sein, so sind die Informationen auf vergleichbar wirksame Art und Weise zu schützen.
Die Rückgabe von Daten und Informationen der inotec Kunststofftechnik GmbH, sowie deren Löschung beim Dienstleister bei Vertragsende muss durch diesen durchgeführt werden. Dabei sind gesetzliche Aufbewahrungspflichten zu beachten.

2.2 Personalsicherheit

Verfügt der Dienstleister über Benutzerkennungen und Zugriffsrechte zu Systemen der inotec Kunststofftechnik GmbH, muss dieser eine regelmäßige Überprüfung der Benutzerkennungen und Zugriffsrechte durchführen. Werden Benutzerkonten nicht mehr benötigt, muss dies der inotec Kunststofftechnik GmbH mitgeteilt werden.
Werden Medien zur 2-Faktor-Authentifizierung verwendet, so müssen diese nach Beendigung des Auftrags oder nach Stilllegung eines Benutzerkontos an die inotec Kunststofftechnik GmbH zurückgegeben werden.
Der Dienstleister muss außerdem sicherstellen, dass ihm zu jeder Zeit bekannt ist, welche seiner Mitarbeiter für die inotec Kunststofftechnik GmbH arbeiten. Scheiden entsprechende

Mitarbeiter aus dem Unternehmen aus, ist sicherzustellen, dass ihre Benutzerkonten umgehend deaktiviert werden.

2.3 Physische und umgebungsbezogene Sicherheit

Das Einsehen und der Zugriff Unbefugter auf IT-Geräte (speziell mobile Endgeräte), welche Informationen der inotec Kunststofftechnik GmbH verarbeiten und speichern, sind zu verhindern.
Informationen der Klassifizierung „Vertraulich“ und „Streng vertraulich“ dürfen nie unbeaufsichtigt transportiert werden.
Informationsträger, welche sensible Informationen der inotec Kunststofftechnik GmbH enthalten, müssen entsprechend vor unbefugtem Zugriff geschützt werden (z.B. durch Verwahren in abgeschlossenen Schränken, Tresoren).

2.4 Management von organisationseigenen Werten

2.4.1 Regelungen für die Klassifizierung von Informationen

Der Dienstleister muss die Klassifizierung von Informationen auf Basis der Schutzziele der Informationssicherheit (s. 2.4.1.1 – 2.4.2.3) und die entsprechende Einstufung für die für ihn relevanten Informationswerte der inotec Kunststofftechnik GmbH kennen.
Der Dienstleister muss im Zweifelfall diese Klassifizierung bei der zuständigen Stelle bei inotec Kunststofftechnik GmbH in Erfahrung bringen und die Informationen anhand ihrer Klassifizierung entsprechend schützen.

2.4.1.1 Vertraulichkeit

Der Zugriff auf Informationen der inotec Kunststofftechnik GmbH darf nur für die dafür berechtigten Personen möglich sein.
Erstellt der Dienstleister für inotec Kunststofftechnik GmbH neue Informationen, so sind diese entsprechend explizit zu kennzeichnen (z.B. Kennzeichnung „Vertraulich“ oder „Streng vertraulich“ im Dokument oder auf dem Informationsträger).
Der Dienstleister muss die Einstufung für neue Informationen mit der zuständigen Stelle der inotec Kunststofftechnik GmbH abstimmen. Bis zur Einstufung ist die Information standartmäßig als „Vertraulich“ zu betrachten.

Stufen: Öffentlich, Intern, Vertraulich, Streng vertraulich

2.4.1.2 Integrität

Es ist zu gewährleisten, dass Informationen der inotec Kunststofftechnik GmbH Informationen vor unberechtigten, bzw. unbemerkten Änderungen ihres Inhalts geschützt sind.

Stufen: Gering, Mittel, Hoch, Sehr Hoch

2.4.1.3 Verfügbarkeit

Es ist zu gewährleisten, dass Informationen der inotec Kunststofftechnik GmbH zum benötigten Zeitpunkt stets zur Verfügung stehen.

Stufen: Gering, Mittel, Hoch, Sehr Hoch

2.4.2 Umgang mit Informationen

Informationen der inotec Kunststofftechnik GmbH sind über ihren gesamten Lebenszyklus vor unberechtigtem Zugriff zu schützen.
Die inotec Kunststofftechnik GmbH hat dazu konkrete Vorgaben für jede Klassifizierungsstufe zu Kennzeichnung, Vervielfältigung und Verteilung, Speicherung, Lagerung, Löschung, Entsorgung, Authentifizierung und Transport festgelegt.

Klassifikation Stufe Öffentlich:

- keine Einschränkungen

Klassifikation Stufe Intern:

- Kennzeichnung: implizit ohne Kennzeichnung oder „Intern“ (in Landessprache) auf der erster Seite,
- Vervielfältigung und Verteilung: nur berechtigte Mitarbeiter und Dritter im Rahmen der Tätigkeit bzw. des Anwendungsbereiches
- Speicherung: Schutz vor unbefugtem Zugriff
- Löschung: nicht mehr benötigte Daten müssen umgehend gelöscht werden
- Entsorgung: gesicherte Entsorgung, zuverlässige Überschreibung, physische Zerstörung der Informationsträger

Klassifikation Stufe Vertraulich:

- Kennzeichnung: „Vertraulich“ (in Landessprache) auf jeder Seite elektronisch oder gedruckt, Beachtung der Vorgaben zur Positionierung der Kennzeichnung
- Vervielfältigung und Verteilung: eingeschränkte Gruppe berechtigter Mitarbeiter und Dritter im Rahmen der Tätigkeit bzw. des Anwendungsbereiches
- Speicherung: Zugriff nur für eingeschränkte Gruppe berechtigter Mitarbeiter und Dritter im Rahmen der Tätigkeit (geschlossene Nutzergruppen), Verwendung geeigneter Speicherorte und –medien. Die Speicherung von vertraulichen Informationen sollte verschlüsselt erfolgen.
- Lagerung: in abgeschlossenen Möbeln oder abgeschlossenen Räumen, Öffnung nur für Berechtigte möglich
- Löschung: nicht mehr benötigte Daten müssen umgehend gelöscht werden
- Entsorgung: gesicherte Entsorgung, zuverlässige Überschreibung, physiche Zerstörung der Informationsträger gemäß gängiger Standards (z.B. DIN 66399, Sicherheitsstufe 4)
- Authentifizierung: vor dem Zugriff auf vertrauliche Informationen sollte eine starke Authentifizierung nach Stand der Technik gewährleistet sein
- Transport:
    - In Papierform: verschlossene neutrale Umschläge („persönlich“ bei Bedarf), Übergabe nur direkt an Empfänger
    - Auf Speichermedien: vertrauliche Informationen dürfen nur verschlüsselt transportiert werden

Klassifikation Stufe streng vertraulich:

- Kennzeichnung: Kennzeichnung: „streng vertraulich“ (in Landessprache) auf jeder Seite elektronisch oder gedruckt, Beachtung der Vorgaben zur Positionierung der Kennzeichnung, Seitenkennzeichnung mit „Seite x von y“
- Vervielfältigung und Verteilung: stark eingeschränkte Gruppe berechtigter Mitarbeiter und Dritter im Rahmen der Tätigkeit bzw. des Anwendungsbereiches, vorherige Genehmigung durch Informationseigentümer, weitere organisatorische oder technische Maßnahmen je nach Anwendungsfall (Verbot der Weiterleitung, Druckverbot, Wasserzeichen), Verhindern von Mithören (verschlüsselte Videokonferenzen)
- Speicherung: Zugriff nur für stark eingeschränkte Gruppe berechtigter Mitarbeiter und Dritte im Rahmen der Tätigkeit bzw. des Anwendungsbereiches, vorherige Genehmigung durch Informationseigentümer, Verschlüsselung nach Stand der Technik (falls eine Verschlüsselung nicht möglich ist, müssen die Informationen durch vergleichbar wirksame Maßnahmen geschützt werden), weitere organisatorische oder technische Maßnahmen je nach Anwendungsfall
- Lagerung: in versperrten Schränken mit separater Schließung,
- Löschung: nicht mehr benötigte Daten müssen umgehend gelöscht werden
- Entsorgung: gesicherte Entsorgung, zuverlässige Überschreibung, physische Zerstörung der Informationsträger gemäß gängiger Standards (z.B. DIN 66399, Sicherheitsstufe 5)
- Authentifizierung: Authentifizierung: vor dem Zugriff auf streng vertrauliche Informationen muss eine starke Authentifizierung nach Stand der Technik gewährleistet sein
- Transport:
    - In Papierform: verschlossene, neutrale Außenumschläge (kein Zusatz), zweiter innerer Umschlag mit Kennzeichnung „streng vertraulich“
    - Auf Speichermedien: streng vertrauliche Informationen dürfen nur verschlüsselt transportiert werden und sind währenddessen, wo möglich, zu beaufsichtigen.

2.4.3 Austausch von Informationen

Ein Mithören unbefugter Personen bei jeglicher Audiokommunikation (z.B. Gespräche, Telefonate, Webmeetings) mit vertraulichen oder streng vertraulichen Informationen ist auszuschließen.
Fax und E-Mail-Verzeichnisse müssen gepflegt werden. Bei Unklarheit ist die aktuelle Adresse bzw. Nummer beim Empfänger zu erfragen.
Beim Mailversand ist der Absender für den Inhalt und die Verteilung verantwortlich. Danach hat der Empfänger die Verantwortung über die weitere Verarbeitung und Verteilung.
Es dürfen keine Ketten-E-Mails versendet oder weitergeleitet werden.

2.5 Umgang mit Informationssicherheitsvorfällen

Es muss eine unverzügliche Meldung aller Informationssicherheitsereignisse an den Informationssicherheitsbeauftragten der inotec Kunststofftechnik GmbH erfolgen, wenn deren Daten oder Systeme betroffen sind.
Außerdem muss eine unverzügliche Meldung bei vermuteten Verwundbarkeiten und Schwachstellen von IT-Systemen der inotec Kunststofftechnik GmbH erfolgen.
Eine sofortige Meldung an den Informationssicherheitsbeauftragten hat bei Verdacht auf Verlust von vertraulichen oder streng vertraulichen Informationen zu erfolgen. Die Meldung an den Informationssicherheitsbeauftragten muss über E-Mail an isb@inotec-kt.de erfolgen.

2.6 Compliance und Einhaltung gesetzlicher Verpflichtungen

Ein Compliance Management (Ressourcen, Kontrolle, Continuity, Schutz) zu allen Informationen, Hard- und Software der inotec Kunststofftechnik GmbH ist einzurichten.

2.6.1 Risikofrüherkennung

Zur Erkennung und Behandlung von Risiken und Bedrohungen für Daten und Systeme ist ein Prozess etabliert.

2.6.2 Geistiges Eigentum / Lizenzmanagement

Die Beachtung der Rechte zu geistigem Eigentum ist sicherzustellen.
Es darf keine unlizenzierte Software verwendet werden.
Bei lizenzierter Software sind die gesetzlichen Bestimmungen zu beachten. Der Einsatz darf nur entsprechend der Lizenzvereinbarungen erfolgen.

2.6.3 Datenschutz

Die Einhaltung landesspezifischer Gesetze zum Datenschutz ist sicherzustellen.

2.7 Vertragliche Compliance

Die Erfüllung aller vertraglichen Anforderungen der inotec Kunststofftechnik GmbH muss sichergestellt werden. Außerdem muss Einhaltung der vertraglichen Anforderungen regelmäßig überprüft werden.

2.8 Verstöße und Durchsetzung

Eine Prüfung und Ahndung von Verstößen gegen die Vorgaben zur Informationssicherheit muss erfolgen. Es gelten dabei die entsprechenden betrieblichen, vertraglichen und gesetzlichen der Vorschriften und Vereinbarungen.

2.9 Verantwortlichkeiten

Der Dienstleister muss der zuständigen Stelle der inotec Kunststofftechnik GmbH seinen zentralen Ansprechpartner für Informationssicherheit (z.B. Informationssicherheitsbeauftragter) mitteilen.

2.10 Auditrecht

Der Dienstleister ermöglicht der inotec Kunststofftechnik GmbH die Durchführung von Audits zur Prüfung der Einhaltung der Informationssicherheit.
Das Audit darf durch einen unbeteiligten, qualifizierten Dritten erfolgen.
Der Dienstleister hat bei Audits eine Mitwirkungspflicht.
Die Frist der Vorankündigung von Audits beträgt mindestens 48 Stunden.
Bei Vorliegen einer Zertifizierung nach ISO/IEC 27001 oder eines TISAX®-Labels kann auf die Durchführung von Audits verzichtet werden.

3 Zusätzliche Anforderungen für Auftragnehmer mit direktem Zugang zum internen Netzwerk der inotec Kunststofftechnik GmbH

3.1 Definition

Die folgenden Anforderungen gelten für Dienstleister der inotec Kunststofftechnik GmbH bei Nutzung von Endgeräten der inotec Kunststofftechnik GmbH und oder einer Anbindung an die IT-Systeme der inotec Kunststofftechnik GmbH (Remotezugänge, VPN-Zugänge, Direktanbindung, Partneranbindung).

3.2 Anforderungen

3.2.1 Interne Organisation

Die Verwendung von IT-Geräten und Daten der inotec Kunststofftechnik GmbH darf nur nach deren Zustimmung erfolgen. Diese Zustimmung kann jederzeit zurückgezogen werden.
Die Installation von Hard- und Software darf nicht ohne die Genehmigung der zuständige Stelle der inotec Kunststofftechnik GmbH erfolgen.
Die Veränderung von IT-Geräten (z.B. Ein-Ausbau von Komponenten, Veränderung von Sicherheitseinstellungen) darf nur durch die zuständigen Stelle der inotec Kunststofftechnik GmbH erfolgen.
Der Einsatz oder die Veränderung von Programmen der inotec Kunststofftechnik GmbH darf nicht ohne vorherige Genehmigung erfolgen.
Auf IT-Geräten von der inotec Kunststofftechnik GmbH dürfen keine Fremddaten verarbeitet werden.
Der Dienstleister stellt sicher, dass Informationen, Programme und Geräte der inotec Kunststofftechnik GmbH nur für Unternehmenszwecke und im Rahmen der Beauftragung eingesetzt werden.
Es dürfen auf IT-Geräten der inotec Kunststofftechnik GmbH keine private Software oder private Daten genutzt werden.

3.2.2 Physische und umgebungsbezogene Sicherheit

Die sachgemäße Behandlung der IT-Geräte der inotec Kunststofftechnik GmbH und der Schutz vor Verlust und Veränderung ist durch den Dienstleister sicherzustellen.
Es sind die Herstellervorschriften zu beachten.
Die Mitnahme von IT-Geräten der inotec Kunststofftechnik GmbH vom Firmengelände darf nur mit Genehmigung der zuständigen Stelle erfolgen.

3.2.3 Schutz vor Schadsoftware

IT-Geräte und Datenträger der inotec Kunststofftechnik GmbH dürfen bei Verdacht auf Schadsoftware nicht genutzt werden. Es muss unverzüglich eine Meldung an die zuständige Stelle erfolgen.

3.2.4 Backup

Die Datenspeicherung soll möglichst auf zugeordneten Netzlaufwerken erfolgen.
Die anderweitige Backup Speicherung (z.B. lokal) ist nicht gestattet.
Die Backupdaten und -medien unterliegen denselben Regeln wie originale Daten.

3.2.5 Zugangskontrolle

3.2.5.1 Geschäftsanforderungen für Zugangskontrolle

Es besteht ein Verbot von Verwendung der Benutzerkennung oder des Kontos anderer Personen.
Es besteht ein Verbot der Weitergabe von Identifikationsmitteln.
Es besteht die Pflicht zur Geheimhaltung und ein Verbot der Weitergabe der persönlichen Benutzerkennung (Passwörter, PINs).
Es besteht ein Verbot von Speichern oder Aufschreiben von Passwörtern, außer über verifizierte Methoden (z.B. KeePass).
Es muss eine sofortige Änderung von Passwort oder PIN bei Verdacht auf Kompromittierung erfolgen.
Es muss eine Änderung temporärer Passwörter bei der Erstanmeldung erfolgen.
Es muss eine Änderung der Passwörter nach spätestens einem Jahr erfolgen.
Es besteht ein Verbot von Ausspähen von Passwörtern
Passwörter sind stets vertraulich zu behandeln.
Falls eine schriftliche Aufbewahrung von Passwörtern notwendig ist, gelten die folgenden Regeln:

- Passwort im versiegelten Umschlag im Tresor
- entsprechende Aktualisierung ist sichergestellt
- Umschlag durch Mitarbeiter abgezeichnet,
- Namensliste für zum Öffnen berechtigte Personen ist vorhanden
- Dokumentation und Bericht jeder Öffnung
- Umgehende Änderung des Passwort nach Öffnung
- Einsatz alternative IT-Systeme mit entsprechender Funktionalität für die beschriebenen Regeln zulässig

Es besteht die Pflicht der Systemsperre durch Benutzer beim Verlassen eines Systems im laufenden Betrieb.

3.2.5.2 Generierung von Passwörtern

Es besteht ein Verbot der Verwendung identischer Passwörter von Privat.
Es besteht ein Verbot der Verwendung identischer Passwörter von Drittsystemen.
Es besteht die Pflicht der Einhaltung der Mindestlänge von Passwörtern.
Es besteht ein Verbot von trivialen Passwörtern und Passwörtern mit persönlichen Bezug.
Es besteht die Pflicht der Erfüllung der entsprechenden Vorgaben, wenn komplexe Passwörter gefordert sind.

3.2.5.3 PINs zum Entsperren von Smartphones und Tablets

Die Vorgaben sind identisch zu den Vorgaben zu Passwörtern.

3.2.5.4 PINs für Authentifizierungs-Smartcards

Die Vorgaben sind identisch zu den Vorgaben zu Passwörtern.

3.2.5.5 Gruppenkennungen

- Gruppenkennungen sind zulässig unter den folgenden Voraussetzungen:
    - Zuweisung der Benutzerkennung durch einen Zuständigen, Sicherstellung von Protokollierung und Archivierung
    - Schriftliche Bestätigung des Erhalts durch Nutzer, Sicherstellung der Archivierung
    - Änderung des Passworts nach Erhalt der Benutzerkennung durch Nutzer
    - Änderung des Passworts nach Rückgabe der Benutzerkennung durch Zuständigen
    - Beachtung der Archivierungsfristen

3.2.6 Zugangskontrolle für Netze

3.2.6.1 Regelwerk für die Nutzung von Netzdiensten

IT-Geräte der inotec Kunststofftechnik GmbH dürfen nur zum sicheren Verbindungsaufbau zu internen Netzwerken (z.B. via VPN) mit öffentlichen Netzwerken verbunden sein.
Die Trennung der Verbindung hat sofort zu erfolgen, wenn diese nicht mehr benötigt wird.

3.2.6.2 Geräteidentifikation in Netzen

Eine Uneingeschränkte Verbindung zu internen Netzen der inotec Kunststofftechnik GmbH ist nur nach erfolgter Freigabe der inotec Kunststofftechnik GmbH gestattet.

4 Zusätzliche Anforderungen für Auftragnehmer ohne direkten Zugang zum internen inotec Kunststofftechnik GmbH Netzwerk

4.1 Definition

Die folgenden Anforderungen gelten für Dienstleister der inotec Kunststofftechnik GmbH ohne Nutzung von Endgeräten der inotec Kunststofftechnik GmbH und ohne eine Anbindung an IT-Systeme der inotec Kunststofftechnik GmbH (Remotezugänge, VPN-Zugänge, Direktanbindung, Partneranbindung), falls dennoch Datenaustausch mit der inotec Kunststofftechnik GmbH erfolgt.

4.2 Anforderungen

4.2.1 Interne Organisation

- Es muss eine Trennung von Daten der inotec Kunststofftechnik GmbH von Daten Dritter erfolgen (z.B. durch entsprechendes Rechtemanagement).
- Eine Verhinderung von unbefugtem Zugriff Dritter muss sichergestellt sein (z.B. durch Verschlüsselung).
- Die Übernahme der Klassifizierung der Informationen der inotec Kunststofftechnik GmbH muss erfolgen.
- Die Umsetzung angemessener Maßnahmen zur Wahrung der Informationssicherheit muss gewährleistet sein.
- Der Zugriff auf Daten der inotec Kunststofftechnik GmbH muss nach dem Prinzip „Kenntnis nur bei Bedarf“ („Need-to-Know-Prinzip“) erfolgen.

5 Verantwortlichkeiten und Abweichungen

Die Einhaltung der Anforderungen in diesem Dokument ist durch alle Dienstleister der inotec Kunststofftechnik GmbH zu gewährleisten.
Abweichungen sind nur nach Rücksprache mit der zuständigen Stelle bei inotec Kunststofftechnik GmbH erlaubt.