1. Geltungsbereich

1.1. Diese Allgemeinen Informationstechnologie-Bedingungen (im Folgenden: "**AIB**") regeln die von der AUDI HUNGARIA Zrt. und/oder der AUDI HUNGARIA AHEAD Kft. (des Weiteren als „**Auftraggeber**“) in Anspruch genommenen Dienstleistungen der Informationstechnologie bzw. Kommunikationstechnologie (im Folgenden: "**IT**"), sowie die mit der Datenverwaltung und Datenverarbeitung verbundenen Tätigkeiten. Auch bei sonstigen Dienstleistungen und Verträgen sind die einschlägigen Bestimmungen dieser AIB entsprechend anzuwenden, soweit für den **Partner** zur Leistungserfüllung ein Zugriff auf die IT-Systeme des Auftraggebers gewährt wird oder der Partner in sonstiger Weise mit den IT-Systemen des Auftraggebers arbeitet und Zugriff auf Informationen oder Daten des Auftraggebers hat.

2. Erbringung der Vertragsleistungen

2.1. Die Begriffsbestimmung von **„Vertrag“** ist unter Ziffer I.7. der Allgemeinen Einkaufsbedingungen des Auftraggebers (nachstehend **„EKB“**) zu finden.

2.2. Ist der Gegenstand des Vertrages die Erstellung eines Ergebnisses, verpflichtet sich der Partner, die Leistungserbringung entsprechend zu dokumentieren und bei Bedarf den Auftraggeber über den Stand der Dienstleistung den Erwartungen des Auftraggebers entsprechend zu informieren.

2.3. Erhalten Mitarbeiter des Partners Zugriff auf IT-Systeme des Auftraggebers, so werden die Identifikationsdaten der Mitarbeiter bei einem verbundenen Unternehmen der AUDI AG oder der VOLKSWAGEN AG [nachstehend „Konzerngesellschaft(en)] verarbeitet und verwendet. Der Partner hat die vorherige schriftliche Zustimmung seiner betroffenen Mitarbeiter zur Datenverarbeitung wie oben beschrieben einzuholen und auf Wunsch des Auftraggebers diese Dokumente ihm vorzulegen; der Partner ist alleinverantwortlich für die Verletzung dieser Pflichten.

2.4. Sofern nicht in der Bestellung abweichend geregelt, wird der Partner alle erforderlichen Infrastrukturleistungen für den Auftraggeber ohne zusätzliche Kosten erbringen. Infrastrukturleistungen sind alle im Zusammenhang mit den Soft- und/oder Hardwareleistungen und/oder Anwendungen erforderlichen vorbereitenden Leistungen (wie Planung, Errichtung, Aufbau oder Installation von Systemen oder IT-Arbeitsplätzen).

2.5. Der Partner wird dem Auftraggeber auf Wunsch hin zu marktüblichen Konditionen Supportleistungen anbieten. Supportleistungen sind alle im Zusammenhang mit den Soft- und/oder Hardwareleistungen und/oder Anwendungen und/oder Infrastrukturleistungen erforderlichen begleitenden Leistungen wie Schulung, Beratung, Optimierung, Wartung/Pflege.

3. Lizenzbedingungen

3.1. Open-Source-Software

3.1.1. Eine Verwendung von Open-Source-Software im Rahmen der Vertragsleistungen ist nur mit der vorherigen schriftlichen Zustimmung des Auftraggebers gestattet.

3.1.2. Verwendet der Partner Open-Source-Software ohne die vorherige schriftliche Zustimmung des Auftraggebers, hat der Partner auf Wunsch des Auftraggebers die Open-Source-Software durch eine gleichwertige Closed-Source-Software zu ersetzen.

3.1.3. Der Partner stellt den Auftraggeber der Höhe nach unbegrenzt von allen Ansprüchen Dritter und damit verbundenen Kosten wegen der Verwendung von Open-Source-Software durch den Partner ohne vorherige schriftliche Zustimmung des Auftraggebers frei.

3.2. Click-Wrap-/Shrink-Wrap-Lizenzen

3.2.1. Click-Wrap-/Shrink-Wrap-Lizenzbedingungen werden gegenüber dem Auftraggeber in keinem Fall wirksam.

3.3. Lizenz-Audits

3.3.1. Legt der Partner dem Auftraggeber schriftlich einen hinreichend begründeten Verdacht dar, wonach Nutzungsrechte überschritten werden, die der Partner dem Auftraggeber an überlassener Software eingeräumt hat, so führt der Auftraggeber einen Lizenz-Audit (Überprüfungen der Einhaltung der Nutzungsrechteregelungen) hinsichtlich der betreffenden Software durch und erteilt dem Partner schriftlich Auskunft über das Ergebnis des Lizenz-Audits.

4. IT-Sicherheitsanforderungen

4.1. Der Partner wird bei der Erbringung der Vertragsleistungen den aktuellen Stand der Technik hinsichtlich Daten- und Systemsicherheit entsprechend dem Qualitätsniveau der ISO 9001 und der ISO 27000-Familie einhalten und dabei insbesondere die Systeme des Auftraggebers nach dem aktuellen Stand der Technik gegen unbefugte Zugriffe Dritter (z. B. Hackerangriffe) sowie gegen unerwünschte Datenübermittlung (z. B. Spam) sichern.

4.2. Der Partner ist bei der Erfüllung des Vertrages verpflichtet, die Vorschriften des Auftraggebers hinsichtlich der von ihm verwalteten und verarbeiteten Daten einzuhalten. Die Klassifizierung der im Rahmen des Vertrages betroffenen Daten wird in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit vom Auftraggeber durchgeführt (nachfolgend "Datenklassifizierung"). Die detaillierten Vorschriften für die Datenklassifizierung sind in der Anlage Nr. 1 der AIB enthalten. Die Relevanz des „Trusted Information Security Assessment Exchange” (im Weiteren TISAX genannt) wird ebenfalls im Rahmen der Festlegung der Datenklassifizierung und der Geheimhaltungspflicht bestimmt. Sollte die Bestellung / verträgliche Beauftragung gemäß Anfrageunterlagen ein TISAX-Testat

erfordern, verpflichtet sich der Partner, dieses nachzuweisen oder das TISAX-Testat zu erlangen. Der Zeitraum zu Erlangung des TISAX-Testats beträgt maximal 12 Monate nach Erhalt des Vertrages, außer das Verhandlungsprotokoll definiert eine hiervon abweichende Regelung. Bei einem TISAX-relevanten Vertrag ist der Partner verpflichtet, die TISAX-Kontrollprozesse des AUDI-Konzerns einzuhalten. Der Auftraggeber informiert den Partner schriftlich über die detaillierten Schritte des TISAX-Zertifizierungsprozesses sowie die zu ergreifenden Maßnahmen, basierend auf dem aktuell bestehenden TISAX-Zertifizierungsprozess.

4.3. Bei Bedarf durch Auftraggeber muss von dem Partner entwickelte bzw. zur Verfügung gestellte System durch Penetrationstest geprüfte Anforderungen aus die OWASP Application Security Verification Standard und OWASP Top Ten Project erfüllen. Der Penetrationstest wird entweder durch Auftraggeber, oder externe Partner der Auftraggeber durchgeführt. Auf Wunsch des Partners ist es möglich, das Ergebnis des vom Partner in Auftrag gegebenen Penetrationstests vorzulegen, das er mit dem Auftraggeber schriftlich zu vereinbaren und zu akzeptieren hat. Der vom Partner vorgelegte Penetrationstestprotokoll und Maßnahmenplan darf nicht älter als 1 Jahr sein.Der vom Partner vorgelegte und vom Auftraggeber schriftlich akzeptierte Penetrationstest kann den von dem Auftraggeber und/ oder seinem externen Partner durchgeführten Penetrationstest ersetzen. Der Partner verpflichtet sich bis zum Betriebsübergabe für die Abstellung und Abnahme durch Auftraggeber von allen, durch Penetrationstest aufgedeckte IT-Sicherheitsschwachstellen und Ergebnisse.

4.4. Der Partner wird bei der Erbringung der Vertragsleistungen die IT-Sicherheitsanforderungen des Auftraggebers einzuhalten. Die Anforderungen finden sich in diesen AIB und deren Anlagen bzw. den für den Einzelvertrag geltenden speziellen Unterlagen.

4.5. Der Partner hat bei vollständiger Einhaltung der IT-Sicherheitsanforderungen seine eingeschalteten Erfüllungsgehilfen (hauptsächlich aber nicht ausschließlich: Arbeitnehmer, Subunternehmer, Beauftragte, sonstige Dritte) vor Zugriff auf die Systeme des Auftraggebers über deren Inhalt unterweisen. Den vom Partner eingeschalteten Personen, die mit Informationen arbeiten, wird Auftraggeber Sicherheitsschulungen und Sensibilisierungstrainings sicherstellen, an denen diese Personen verbindlich teilzunehmen haben. Bei Vertragsleistungen, bei denen auch Informationen vom Auftraggeber verarbeitet werden, hat der Partner nachweisbar dokumentiert eine Kontaktperson in IT-Sicherheitsfragen zu bestimmen (in Abhängigkeit vom Volumen der Vertragsleistungen dediziert oder nicht dediziert). Die Lieferanten haben die Personen, die an der jeweiligen Vertragsleistung beteiligt sind und Zugriff auf Informationen des Auftraggeber haben und periodisch oder kontinuierlich an diese Daten herankommen können, zu bestimmen, zu dokumentieren und ihre Namen und Daten nachweisbar dokumentiert an Auftraggeber zu übermitteln (unter Berücksichtigung der einschlägigen Datenschutzregelungen).

4.6. Der Partner ist verpflichtet, regelmäßig (mindestens jährlich) zu überprüfen, ob die Nutzungsrechte des Partners seinen Aufgaben entsprechen. Berechtigungen sollten bei Bedarf entsprechend angepasst werden. Der Partner informiert den Auftraggeber schriftlich über die Ergebnisse der Prüfung.

4.7. Die Sicherheitsanforderungen an provisorische Zeiträume der Vertragsleistungen (z. B. Transitionszeitraum) werden durch den Auftraggeber vom Zeitraum der kontinuierlichen Leistungserbringung getrennt behandelt; in diesen Zeiträumen hat der Partner unterschiedlichen Sicherheitsmaßnahmen und Kontrollmaßnahmen zu entsprechen.

4.8. Um Informationssicherheitsvorfälle schnell, effizient und einheitlich zu behandeln, müssen die Verfahren des Auftraggebers zum Management von Informationssicherheitsvorfällen vom Partner ab Beginn der jeweiligen Dienstleistung eingehalten werden. Der Partner ist verpflichtet, dem Auftraggeber (CERT-AudiHungaria@audi.hu) in allen Fällen von Informationssicherheitsvorfällen, die dem Auftraggeber zur Verfügung gestellten Dienste oder Daten betreffen, unverzüglich schriftlich zu informieren. Der Auftraggber informiert den Partner schriftlich über das Verfahren zum Management von Informationssicherheitsvorfällen und die zu ergreifenden Maßnahmen unter Berücksichtigung des aktuellen Informationssicherheitsvorfalls

4.9. Der Partner hat den Auftraggeber unverzüglich schriftlich über alle Änderungen zu informieren und diese Änderungen zu dokumentieren, die die für den Auftraggeber erbrachten Dienstleistungen betreffen können, so insbesondere, aber nicht ausschließlich:

- Änderungen im Kreis der mitwirkenden Personen des Partners;
- Nutzung neuer Technologien, Produkte oder Versionen;
- Änderung des Ortes der Leistungserbringung, sonstige Änderungen in der physischen Umgebung;
- Leistungserbringung für Dritte, die für den Auftraggeber erbrachte Dienstleistungen betreffen können.

4.10. Bei einem diesbezüglichen Bedarf des Auftraggebers hat der Partner schriftliche Berichte über bei ihm durchgeführte IT-Sicherheitsprüfungen vorzulegen, die in Zusammenhang mit Sicherheitsaspekten der für den Auftraggeber erbrachten Dienstleistungen stehen.

4.11. Alle Partner haben die Festlegungen nach Anlage 1 dieser AIB („Informationssicherheitshandlungsleitlinien für Partnerfirmen“) einzuhalten.

5. Revisionsklausel

5.1. Der Partner räumt dem Auftraggeber und/oder seinen externen Partnern und/oder der Konzernrevision der

VOLKSWAGEN AG das jederzeit auszuübende Recht ein, nach vorheriger Anmeldung:

- **sämtliche Daten zu Geschäftsvorfällen zwischen dem Partner und dem Auftraggeber;**
- **die IT-Sicherheitsdokumente (Regelungen, Arbeitsanweisungen usw.) und Prozesse des Partners und/oder seiner Erfüllungsgehilfen in Hinsicht auf die Einhaltung der IT-Sicherheitsvorschriften des Auftraggebers**

bei dem Partner bzw. seinen Erfüllungsgehilfen einzusehen und zu überprüfen.

6. Sonstiges

6.1. Sollten die Bestimmungen der vorliegenden AIB den EKB des Auftraggebers widersprechen, haben diese Vorschriften der AIB Vorrang.

6.2. Inkrafttreten: 01.07.2023, zu welchem Zeitpunkt die am 29.07.2021 erlassenen Allgemeinen IT-Vorschriften außer Kraft treten.

AUDI HUNGARIA Zrt.
Sitz: H-9027 Győr, Audi Hungária út 1.
Eingetragen im Handelsregister des Gerichtshofes Győr als Handelsgericht
Cg. 08-10-001840

Steuernummern:
Ungarische St.-Nr.: 23391475-2-08
Ungarische gem. St.-Nr.: HU23391475

AUDI HUNGARIA AHEAD Kft.

Sitz: H-9027 Győr, Audi Hungária út 1.
Eingetragen im Handelsregister des Gerichtshofes Győr als Handelsgericht
Cg. 08-09-035615

Steuernummern:
Ungarische St.-Nr.: 32230866-2-08
Ungarische gem. St.-Nr.: HU32230866

Anlage 1 der Allgemeinen IT-Bedingungen -

Informationssicherheitshandlungsleitlinien für Partnerfirmen

Version: 1.0 (30.05.2023)
Herausgeber: Rechtsservice
Richtlinienverantwortlicher: IT-Security
Regelung Nr.: Anlage Nr. 4 der Informationssicherheit Unternehmensrichtlinie U_2.024

Geltungsbereich

Die Regelungen der AUDI HUNGARIA Zrt. und/oder der AUDI HUNGARIA AHEAD Kft. (des weiteren „Auftraggeber“) sind gültig sowohl für die dienstleistende Partner (des weiteren „Auftragnehmer“) als auch dessen Subunternehmer (des weiteren „Beitragende“).

1 Zweck

In dieser Informationssicherheitshandlungsleitlinie werden die Regeln für Informationssicherheit definiert, die von Dienstleistern beim Umgang mit Informationen und IT-Geräten (z. B. PCs, Arbeitsplätze, Laptops, Smartphones oder Tablet-PCs) zu befolgen sind.

Dienstleister sind definiert als jeder Dritte, der Dienstleistungen für den Auftraggeber auf Basis vertraglicher Beziehungen erbringt. Diese Handlungsleitlinien richten sich an die Geschäftsleitung der Dienstleister, deren Mitarbeiter sowie deren Erfüllungs-/Verrichtungshilfen (im Folgenden Auftragnehmer genannt).

Zweck der Informationssicherheitshandlungsleitlinien ist der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Schutz der Rechte und Interessen des Auftraggebers und aller natürlichen und juristischen Personen, die eine Geschäftsbeziehung mit dem Auftraggeber eingehen und/oder Tätigkeiten für diesen ausführen.

Die Verantwortlichkeiten der Revision des Auftraggebers sind nicht Bestandteil dieser Regelung.

1.1 Abkürzungen und Definitionen

Abkürzung/Begriff	Erklärung
Ersteller von Informationen	Ersteller von Informationen ist die Person oder Gruppe von Personen, die bestimmte Informationen oder ein Dokument erstellt. Der Ersteller muss das Dokument/die Informationen entsprechend der durch den Informationseigentümer bestimmten Klassifikationsstufe klassifizieren/ kennzeichnen.
Informationseigentümer	Informationseigentümer ist die Person oder Gruppe von Personen, die vom Management als zuständig für die Wahrung der Vertraulichkeit bestimmter Informationen festgelegt wurde. Im Verlauf der Lebensdauer von Informationen kann es zu einem Wechsel des Informationseigentümers kommen.

2 Dokumentenstruktur und Zielgruppe

Dieses Dokument enthält drei Kapitel. Die folgende Tabelle führt die Dokumentenstruktur und die jeweilige Zielgruppe pro Kapitel auf.

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

Kapitel	Zielgruppe	Anmerkungen
3	Alle Dienstleister	Die Anforderungen dieses Kapitels sind von allen Dienstleistern einzuhalten. Weitere Anforderungen sind in Kapitel 4 und 5 enthalten. Diese müssen in Abhängigkeit von den Zugriffsmöglichkeiten auf Konzernnetzwerk und Konzernsysteme eingehalten werden.
4	Dienstleister, mit Zugriff auf das Konzernnetzwerk oder auf Konzern-Systeme	Zusätzlich müssen die Anforderungen aus Kapitel 3 eingehalten werden.
5	Dienstleister, ohne Zugriff auf das Konzernnetzwerk oder auf Konzern-Systeme	Zusätzlich müssen die Anforderungen aus Kapitel 3 eingehalten werden.

3 Allgemeine Anforderungen

Die folgenden Anforderungen müssen von allen Dienstleistern, entsprechend der Definition in diesem Dokument, eingehalten werden.

Anforderungen an den Auftraggeber sind nicht Bestandteil dieses Dokuments.

3.1 Organisatorische Anforderungen

Bezüglich des Mitbringens von IT-Geräten auf das Firmengelände oder in Sicherheitsbereiche des Auftraggebers, die nicht vom Auftraggeber gestellt sind, gelten die Regelungen der Auftraggeber.

Das Verwenden von Daten oder Software, die zum Auftraggeber gehören, auf IT-Systemen oder Speichergeräten die weder durch den Auftraggeber noch vom Dienstleister bereitgestellt oder freigegeben sind, ist nicht zulässig.

Das Verwenden von Daten oder Software der Auftraggeber auf nicht durch den Auftraggeber freigegebenen Fileservices oder Internet Cloud-Diensten ist nicht zulässig.

Die Weitergabe von Daten an Dritte ist nur mit schriftlicher Freigabe durch den Dateneigentümer des Auftraggebers gestattet.

Regelungen des Auftraggebers zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten (siehe Anhang, 7.2.1) müssen eingehalten werden.

Mitarbeiter des Dienstleisters müssen von ihrer Geschäftsleitung auf die Geheimhaltung im Sinne der bestehenden Vertraulichkeitsvereinbarung zwischen Auftraggeber und Auftragnehmer verpflichtet werden. Dem Auftraggeber ist jederzeit Einsicht in diese Vereinbarungen zu gewähren.

Falls Daten des Auftraggebers auf mobilen Systemen oder IT-Geräten gespeichert werden, sind diese mit dem aktuellen Stand der Technik entsprechender Hardware oder Software zu verschlüsseln. Zusätzliche Anforderungen zur Verschlüsselung und Authentifizierung befinden sich im Group Suppliers Portal (siehe Anhang, 7.2.2).

Vor Auslandsreisen sind die länderspezifischen Regelungen zum Einsatz von Sicherheitstechniken (z. B. Verschlüsselung) zu beachten.

Nach Vertragsende müssen Daten des Auftraggebers an den Auftraggeber übergeben werden und sind auf Geräten und Speichermedien des Dienstleisters zu löschen. Rechtliche Anforderungen (z.B. Aufbewahrungspflichten) sind zu beachten.

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

3.2 Personalsicherheit

Eine nicht mehr benötigte Benutzerkennung oder ein nicht mehr benötigtes Zugriffsrecht auf Daten des Auftraggebers ist von dem jeweiligen Nutzer unverzüglich bei den jeweiligen auftraggebenden Stellen (z.B. zuständiger Benutzeradministrator des Auftraggebers) zu melden, damit die entsprechende Sperrung/ Löschung erfolgen kann.

Nicht mehr benötigte Medien zur Identifizierung (z. B. Smartcards, SecurID-Karten) sind unverzüglich an die auftraggebende Stelle zurückzugeben.

Überlassene Geräte (z. B. Laptops) und Datenträger bzw. Speichermedien müssen nach Ablauf des Vertrags, oder wenn diese nicht mehr benötigt werden, an den Auftraggeber zurückgegeben werden.

Der Verlust von an den Benutzer übergebenen IT-Geräten sowie von Medien zum Zwecke der Authentifizierung sind durch den Benutzer umgehend der zuständigen Stelle des Auftraggebers (siehe Anhang, 7.2.3) zu melden.

3.3 Physische und umgebungsbezogene Sicherheit

IT-Geräte, die Daten des Auftraggebers speichern oder verarbeiten sind so zu verwenden, dass keine Unbefugten diese Daten einsehen oder darauf zugreifen können. Besondere Vorsicht ist bei der Verwendung mobiler Systeme geboten.

Vertrauliche und geheime Dokumente dürfen niemals unbeaufsichtigt gelassen werden, um Einsichtnahme durch Unberechtigte zu verhindern.

3.4 Management von organisationseigenen Werten

3.4.1. Regelungen für die Klassifikation

Eine Klassifikation findet anhand der drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit statt und muss für alle Informationen und alle informationsverarbeitenden IT-Systeme durchgeführt werden.

Der Auftragnehmer muss die Klassifikation nach Vertraulichkeit, Integrität und Verfügbarkeit (im Rahmen des Geltungsbereiches der Dienstleistungen) vom Auftraggeber anfordern.

Informationen (Schutzziel Vertraulichkeit) sind über ihre gesamte Lebensdauer hinweg gemäß den Maßnahmen, die ihrer Vertraulichkeitseinstufung entsprechen, vor unbefugtem Zugriff zu schützen. Vertraulichkeitseinstufungen können mit einem Ablaufdatum versehen werden.

Falls erforderlich, ist bei der Verarbeitung von Daten die Klassifikation in Bezug auf Integrität und Verfügbarkeit durch den jeweiligen Prozesseigentümer zu überprüfen und zu bestimmen. Diese Klassifikation ist regelmäßig, unter Einbeziehung des Informationseigentümers, zu evaluieren und gegebenenfalls anzupassen.

Die korrekte Klassifizierung muss vom Informationseigentümer bestätigt werden.

3.4.1.1. Vertraulichkeit

Informationen, die nicht für die Allgemeinheit bestimmt sind, dürfen nur den Personen zugänglich gemacht werden, die dazu berechtigt sind (Grundsatz „Kenntnis nur wenn nötig“).

Vorgaben für Ersteller und Eigentümer von Informationen:

- Neu erstellte Informationen und Daten sind durch den Ersteller (siehe 1.1 - Ersteller von Informationen) zu kennzeichnen.
- Der Informationseigentümer (siehe 1.1 - Informationseigentümer) ist verantwortlich für die Klassifikation.
- Der Ersteller muss die korrekte Klassifikation über den Informationseigentümer anfordern.
- Vertraulichkeitseinstufungen müssen für alle IT-Systeme erfolgen.

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

- Wenn eine Klassifikation noch nicht eindeutig ist, beispielsweise bei neu angelegten Dokumenten/IT-Systemen, ist die Einstufung „Vertraulich“ zu wählen.
- Der Informationseigentümer muss (spätestens bei der nächsten Überprüfung oder Aktualisierung) für interne, vertrauliche und geheime Informationen prüfen, ob deren Vertraulichkeitseinstufung noch korrekt ist, und sie entsprechend kennzeichnen.

Vorgaben für den Empfänger:
- Nicht gekennzeichnete Informationen und Daten gelten als intern.
- Im Falle von Zweifeln an der Klassifikation ist der Informationseigentümer zu kontaktieren.

Folgende Klassifikationsstufen sind in Bezug auf die Vertraulichkeit von Informationen definiert:

Klassifikation	Definition
Öffentlich	Informationen, die keinen Einschränkungen unterliegen und beispielsweise in der Presse oder im Internet veröffentlicht werden können. Die Verwendung von Unternehmensinformationen in der Öffentlichkeit bedarf der Zustimmung der zuständigen Stellen (siehe Anhang, 7.2.4). Beispiele: Pressemeldungen, Produktkataloge für Kunden
Intern	Informationen, deren Kenntnis durch Unbefugte oder deren missbräuchliche Weitergabe oder Verwendung nur geringen Einfluss auf das Erreichen von Produkt- und Projektzielen haben und daher einem berechtigten Personenkreis zugänglich gemacht werden dürfen. Vertraulichkeitsverstöße können negative Folgen haben, wenn auch eher geringfügiger Natur. Beispiel: • Schadenersatzforderungen durch Einzelpersonen oder Organisationen sind unwahrscheinlich Beispiele: geschäftliche Kommunikationsdaten (Telefonnummer oder E-Mail-Adresse),, betriebliche Vorgaben zum Arbeitsschutz, Arbeitsordnung
Vertraulich	Informationen, deren Bekanntgabe oder Offenlegung an unbefugte Personen das Erreichen von Produkt- und Projektzielen gefährden kann und die daher ausschließlich einer begrenzten Gruppe von Berechtigten zugänglich gemacht werden dürfen. Vertraulichkeitsverstöße führen voraussichtlich zu messbaren negativen Folgen, wie z. B.: • Verlust von Kunden • Rückgang von Verkaufs-/Umsatzzahlen • Schadenersatzforderungen durch Einzelpersonen oder Organisationen Beispiele: Personenbezogene Daten, die über dienstliche Kommunikationsdaten hinausgehen (z. B. Gehaltsdaten), Budgetplanungen, Revisionsberichte

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

Geheim	Informationen, deren Bekanntgabe oder Offenlegung an unbefugte Personen das Erreichen von Unternehmenszielen in hohem Maße gefährden kann und die daher nur einer äußerst restriktiven Verteilerliste zugänglich gemacht werden dürfen und strengen Kontrollen unterliegen müssen. Vertraulichkeitsverstöße haben erhebliche negative Auswirkungen auf das Image bzw. Erscheinungsbild des Unternehmens sowie wirtschaftliche Folgen, wie z. B.: • erheblicher Verlust von Kunden • starker Rückgang von Verkaufs-/Umsatzzahlen • Schadenersatzforderungen durch diverse Einzelpersonen oder Organisationen • Ausschluss aus bestimmten Marktgebieten • negative Effekte in der öffentlichen Wahrnehmung Beispiele: Besondere Arten personenbezogener Daten (z. B. Gesundheitsdaten), Cycle Pläne, strategische Unternehmenspläne, Entwurfszeichnungen von Prototypen

3.4.1.2. Integrität

Die fehlerfreie Verarbeitung von Informationen und der Schutz vor unbefugten Änderungen müssen sichergestellt werden.

Folgende Klassifikationsstufen sind in Bezug auf die Integrität von Informationen definiert:

Klassifikation	Definition
Gering	Eine Verletzung der Integrität hat keine vorhersehbaren Auswirkungen auf die geschäftlichen Tätigkeiten oder das Image bzw. Erscheinungsbild des Unternehmens.
Mittel	Eine Verletzung der Integrität hat nur geringe Auswirkungen auf die geschäftlichen Tätigkeiten und/oder das Image bzw. Erscheinungsbild des Unternehmens. Es kann zu negativen Folgen kommen, wenn auch in geringem Umfang. Beispiele: • leichte Verzögerungen bei Arbeitsabläufen • Fehler ohne Auswirkungen auf die Arbeitsergebnisse (keine produktiven Ausfallzeiten) • Entscheidungen werden nicht beeinträchtigt • Schadenersatzforderungen durch Einzelpersonen oder Organisationen sind unwahrscheinlich Beispiele: Standortpläne, Organigramme, einzelne interne Telefonnummern

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

Hoch	Eine Verletzung der Integrität hat spürbare Auswirkungen auf die geschäftlichen Tätigkeiten und/oder das Image bzw. Erscheinungsbild des Unternehmens. Es kommt voraussichtlich zu messbaren negativen Folgen, wie z. B.: • Verlust von Kunden ist wahrscheinlich • Rückgang von Verkaufs-/Umsatzzahlen ist wahrscheinlich • deutliche Verzögerungen bei Arbeitsabläufen • Fehler/Fehlfunktionen mit wahrnehmbaren Auswirkungen auf die Arbeitsergebnisse (hohe Produktionsausfälle) und/oder Ausfall einiger Serviceprozesse • Entscheidungen werden beeinträchtigt / Fehlentscheidungen sind wahrscheinlich • Schadenersatzforderungen durch Einzelpersonen oder Organisationen sind wahrscheinlich Beispiele: JIT-Aufträge, Pressemeldungen, Inhalte des Internetauftritts, Produktionssteuerungsdaten
Sehr hoch	Eine Verletzung der Integrität hat erhebliche Auswirkungen auf die geschäftlichen Tätigkeiten und/oder das Image bzw. Erscheinungsbild des Unternehmens sowie entsprechende Konsequenzen, wie z. B.: • erheblicher Verlust von Kunden • Schadenersatzforderungen durch diverse Einzelpersonen oder Organisationen • starker Rückgang von Verkaufs-/Umsatzzahlen • Ausschluss aus bestimmten Marktgebieten • deutliche Verzögerungen bei Arbeitsabläufen • Fehler/Fehlfunktionen mit schwerwiegenden Auswirkungen auf die Arbeitsergebnisse und/oder Ausfall mehrerer Serviceprozesse (sehr hohe produktive Ausfallzeiten) • Entscheidungen werden stark beeinträchtigt / falsche Entscheidungen Beispiele: Bilanzierung (z. B. Jahresabschluss), Patente, kryptographische Schlüssel, Gehaltsabrechnung

3.4.1.3. Verfügbarkeit

Informationen müssen innerhalb eines vereinbarten Zeitraums verfügbar sein.

Folgende Klassifikationsstufen sind in Bezug auf die Verfügbarkeit von Informationen definiert:

Klassifikation	Definition
Gering	Die Verfügbarkeit des IT-Systems darf in Bezug auf Ausfall oder inakzeptable Antwortzeiten weniger als 95 % betragen, ohne dass es zu nennenswerten Beeinträchtigungen (finanzieller Art oder am Image des Unternehmens) kommt. Beispiel: Intranet-Anwendung mit allgemeinen Mitarbeiterinformationen
Mittel	Die Verfügbarkeit des IT-Systems muss in Bezug auf Ausfall oder inakzeptable Antwortzeiten mindestens 95 % betragen. Eine niedrigere Verfügbarkeit führt zu nennenswerten Beeinträchtigungen (finanzieller Art oder am Image des Unternehmens). Beispiel: Bewerberportal

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

Hoch	Die Verfügbarkeit des IT-Systems muss in Bezug auf Ausfall oder inakzeptable Antwortzeiten mindestens 98 % betragen. Eine niedrigere Verfügbarkeit führt zu nennenswerten Beeinträchtigungen (finanzieller Art oder am Image des Unternehmens). Beispiele: Gehaltsabrechnung, Buchhaltung
Sehr hoch	Die Verfügbarkeit des IT-Systems muss in Bezug auf Ausfall oder inakzeptable Antwortzeiten mindestens 99 % betragen. Eine niedrigere Verfügbarkeit führt zu nennenswerten Beeinträchtigungen (finanzieller Art oder am Image des Unternehmens). Beispiel: IT-System, dessen Ausfall einen unmittelbaren Produktionsstopp zur Folge hat Bei nennenswerten Beeinträchtigungen kann es sich z. B. handeln um: • Verlust von Kunden • Schadenersatzforderungen durch diverse Einzelpersonen, Organisationen oder Verbände • starker Rückgang von Verkaufs-/Umsatzzahlen • Ausschluss aus bestimmten Marktgebieten • Fehler/Fehlfunktionen mit schwerwiegenden Auswirkungen auf die Arbeitsergebnisse und/oder Ausfall mehrerer Serviceprozesse (sehr hohe produktive Ausfallzeiten)

3.4.2. Kennzeichnung von und Umgang mit Informationen

Informationen dürfen nur einer berechtigten Gruppe von Personen zum Zwecke der vereinbarten Tätigkeiten und unter Einhaltung der entsprechenden Regelungen zugänglich gemacht werden. Dabei ist der Grundsatz „Kenntnis nur wenn nötig“ zu befolgen.

Informationen müssen während des gesamten Lebenszyklus entsprechend ihrer aktuellen Vertraulichkeitseinstufung vor einem Zugriff durch Unberechtigte geschützt werden. Es gelten folgende Regelungen:

Klassifikation	Anforderungen
Öffentlich	• Kennzeichnung: keine/optional (z.B Vermerk im Impressum) • Es gelten die unternehmensinternen Vorgaben zur Positionierung der Klassifikations-Kennzeichnung. • Vervielfältigung und Verteilung: keine Einschränkungen • Speicherung: keine Einschränkungen • Löschung: keine Einschränkungen • Entsorgung: keine Einschränkungen
Intern	• Kennzeichnung: Angabe der Vertraulichkeitsstufe in Landessprache/keine oder „Intern“ auf der ersten Seite des Dokuments • Es gelten die unternehmensinternen Vorgaben zur Positionierung der Klassifikations-Kennzeichnung. • Vervielfältigung und Verteilung: nur an berechtigte Mitarbeiter des Konzerns und berechtigte Dritte im Rahmen der Tätigkeit bzw. des Anwendungsbereichs • Speicherung: Schutz vor unbefugtem Zugriff • Löschung: Nicht mehr benötigte Daten sind zu löschen. • Entsorgung: ordnungsgemäße Entsorgung (siehe Anhang, 7.2.5)

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

Vertraulich	• Kennzeichnung: Angabe der Vertraulichkeitsstufe in Landessprache/„Vertraulich“ auf jeder Seite des Dokuments in elektronischer und gedruckter Form. • Es gelten die unternehmensinternen Vorgaben zur Positionierung der Klassifikations-Kennzeichnung. • Vervielfältigung und Verteilung: nur an eine beschränkte Gruppe von berechtigten Mitarbeitern des Konzerns und berechtigte Dritte im Rahmen der Tätigkeit sowie des Anwendungsbereichs. Die Person, die die Informationen verteilt, ist für angemessene Verteilwege verantwortlich, um die Informationen und Daten vor unbefugtem Zugriff und/oder unbefugtem Mithören zu schützen (z. B. mithilfe von Verschlüsselung). • Speicherung: Zugriff nur für eine beschränkte Gruppe von berechtigten Mitarbeitern des Konzerns und berechtigte Dritte im Rahmen der Tätigkeit sowie des Anwendungsbereichs (z. B. durch geschlossene Nutzergruppen). Es sind geeignete Speicherorte und/oder Speichermedien zu verwenden. • Vertrauliche Dokumente müssen in versperrten Stahlmöbeln oder in versperrten Räumen, die nur von einer dafür berechtigten Personengruppe geöffnet werden können, aufbewahrt werden, wenn sie nicht benötigt werden. • Löschung: Nicht mehr benötigte Daten sind zu löschen. • Entsorgung: ordnungsgemäße Entsorgung (siehe Anhang, 7.2.5) • Authentifizierung: Starke Authentifizierung (siehe Anhang, 7.2.6) • Transport: Vertrauliche Dokumente und Speichermedien müssen in verschlossenen, neutralen Umschlägen versendet werden; bei Bedarf kann der Zusatz “persönlich” hinzugefügt werden. Dies bedeutet, dass der Umschlag nur direkt an den genannten Empfänger übergeben werden darf.
Geheim	• Kennzeichnung: Angabe der Vertraulichkeitsstufe in Landessprache/„Geheim“ auf jeder Seite des Dokuments • Es gelten die unternehmensinternen Vorgaben zur Positionierung der Klassifikations-Kennzeichnung. • Darüber hinaus sind alle Seiten mit „Seite x von y“ zu kennzeichnen. • Vervielfältigung und Verteilung: nur an eine äußerst begrenzte Gruppe (z. B. namentliche Liste) von berechtigten Mitarbeitern des Konzerns und berechtigte Dritte im Rahmen der Tätigkeit bzw. des Anwendungsbereichs und nach vorheriger Genehmigung durch den Informationseigentümer. Soweit technisch möglich, sind alle Daten nach aktuellem Stand der Technik zu verschlüsseln. Falls dies nicht möglich ist, sind vergleichbar starke Sicherheitslösungen zu verwenden. Je nach Anwendungsfall sind weitere technische bzw. organisatorische Schutzmaßnahmen zu verwenden (z. B. Verbot von Weiterleiten und Ausdrucken, Wasserzeichen). Zur Kommunikation sind geeignete Medien zu verwenden, die ein Mithören verhindern (z. B. verschlüsselte Videokonferenzen). • Speicherung: Zugriff nur für eine äußerst begrenzte Gruppe (z. B. namentliche Liste) von berechtigten Mitarbeitern des Konzerns und berechtigte Dritte im Rahmen der Tätigkeit sowie des Anwendungsbereichs (z. B. durch geschlossene Nutzergruppen). Soweit technisch möglich, sind alle Daten nach aktuellem Stand der Technik zu verschlüsseln. Falls dies nicht möglich ist, sind vergleichbar starke Sicherheitslösungen zu verwenden. • Geheime Dokumente müssen in versperrten Stahlmöbeln aufbewahrt werden. Es sind dabei separate Schließungen zu verwenden. Mobile Datenträger mit geheimen Informationen müssen in geeigneten Datensafes aufbewahrt werden. • Löschung: Nicht mehr benötigte Daten sind zu löschen. • Entsorgung: ordnungsgemäße Entsorgung (siehe Anhang, 7.2.5) • Authentifizierung: Starke Authentifizierung (siehe Anhang, 7.2.6) • Transport: Geheime Dokumente und Speichermedien müssen in neutralen, verschlossenen Außenumschlägen (ohne Zusätze wie “persönlich, geheim, etc.“) versendet werden. In diesen ist ein zweiter innerer Umschlag zu platzieren, welcher mit der Klassifikation “geheim” gekennzeichnet ist und die geheimen Dokumente enthält.

Die Vorgaben zum Umgang mit Informationen (Kennzeichnung, Vervielfältigung, Verteilung, Speicherung, Löschung und Entsorgung) gelten ebenfalls für IT-Systeme (z. B. Datenbanken und Sicherungsmedien).

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

3.4.3. Handhabung von Speicher- und Aufzeichnungsmedien

Datenträger (wie z. B. CDs, DVDs, USB-Sticks und Festplatten) sind vor Verlust, Zerstörung und Verwechslung sowie vor unbefugtem Zugriff zu schützen.

Nicht mehr benötigte Datenträger sind auf sichere Weise zu entsorgen (siehe Anhang, 7.2.5).

3.4.3.1. Austausch von Informationen

Bei allen Gesprächen (einschließlich Telefonaten, Video- und Webkonferenzen), die vertrauliche oder geheime Informationen betreffen oder enthalten, ist sicherzustellen, dass diese nicht unberechtigt mitgehört werden können.

Faxnummern und E-Mail-Adressen sind aktuellen Verzeichnissen zu entnehmen oder beim Empfänger zu erfragen, um fehlerhafte Übertragungen zu vermeiden.

Für den Transport von IT-Geräten und Datenträgern außerhalb der Werksgrenzen des Auftraggebers sind die Regelungen der Auftraggeber zu befolgen (siehe Anhang, 7.2.7).

Für den Inhalt und die Verteilung einer E-Mail ist der Absender verantwortlich. Für die weitere Verarbeitung und Verteilung der Empfänger.

Die Erstellung und der Versand von Ketten-E-Mails ist unzulässig.

3.5 Umgang mit Informationssicherheitsvorfällen

Informationssicherheitsereignisse (z. B. auftretende Störungen, Verstöße gegen das Informationssicherheitsregelwerk), welche Daten oder Systeme des Auftraggebers betreffen sind unverzüglich der zuständigen Stelle zu melden (siehe Anhang, 7.2.8).

Vermutete Verwundbarkeiten und Schwachstellen von IT-Systemen sind unverzüglich der zuständigen Stelle zu melden (siehe Anhang, 7.2.9). Die Prüfung von Verwundbarkeiten und Schwachstellen (z.B. Penetration Testing) darf nur durch die zuständige Stelle erfolgen (siehe Anhang, 7.2.10).

Beim Verdacht auf Verlust von vertraulichen oder geheimen Informationen muss dies sofort an die zuständige Stelle gemeldet werden (siehe Anhang, 7.2.11).

3.6 Compliance und Einhaltung gesetzlicher Verpflichtungen

Durch den Dienstleister ist ein Compliance Management unter Beachtung rechtlicher und betrieblicher Anforderungen (inklusive Resourcenmanagement, internes Kontrollsystem, IT Continuity Management und Schutz von Informationen) einzurichten. Dies muss alle Informationen, Hard- und Software des Auftraggebers umfassen.

Das Compliance Management muss die folgenden Punkte beinhalten.

3.6.1. Risikofrüherkennung

Ein Prozess zur frühen Erkennung von Risiken und potenziellen Bedrohungen für IT-Systeme und Daten muss implementiert sein.

Vorbeugende Tätigkeiten und Maßnahmen müssen getroffen werden, um erkannte Risiken zu behandeln.

3.6.2. Geistiges Eigentum / Lizenzmanagement

Alle Rechte geistigen Eigentums (z. B. Urheberrechte an Software, Dokumenten und Grafiken, Entwurfsrechte, Handelsmarken, Patente und Quellcode-Lizenzen) sind zu beachten und einzuhalten.

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

Die Verwendung nicht lizenzierter Software (Raubkopien) ist nicht zulässig.

Für lizenzierte Software gelten die gesetzlichen Bestimmungen hinsichtlich Urheberrechte (z. B. verstößt das Anfertigen von Kopien, ausgenommen zu Sicherungs- und Archivierungszwecken, gegen die Urheberrechte).

Verstöße gegen diese Bestimmungen können eine strafrechtliche Verfolgung nach sich ziehen und einstweilige Verfügungen oder Schadenersatzforderungen zur Folge haben.

Lizenzierte Software darf nur zum vereinbarten Zweck unter Einhaltung geltender Vorschriften und Lizenzvereinbarungen mit dem Hersteller verwendet werden.

3.6.3. Datenschutz

Die jeweiligen landesspezifischen Gesetze und Vorschriften zum Datenschutz (siehe Anhang, 7.2.12) sind einzuhalten.

Auftragnehmer müssen von der Geschäftsführung des jeweiligen Dienstleisters auf die Einhaltung der gesetzlichen Datenschutzvorgaben (siehe Anhang, 7.2.12) verpflichtet werden.

3.6.4. Vertragliche Compliance

Die IT-Organisation des Dienstleisters muss die vertraglichen Anforderungen des Auftraggebers erfüllen. Es müssen Maßnahmen implementiert sein um sicherzustellen, dass die eigenen organisatorischen Regelungen des Dienstleisters überprüft und aktuell gehalten werden, so dass die aktuellen vertraglichen Anforderungen abgebildet sind.

3.6.5. Internes Regelwerk

Dienstleister müssen ihren Mitarbeitern Regelungen und Verhaltensgrundsätze vorgeben, um die Einhaltung der Anforderungen und den angemessenen Umgang mit Informationen sowie Hard- und Software des Auftraggebers sicherzustellen.

3.7 Verstöße und Durchsetzung

Verstöße gegen die Informationssicherheitshandlungsleitlinien müssen individuell entsprechend der geltenden betrieblichen, vertraglichen und rechtlichen Vorschriften und Vereinbarungen geprüft und geahndet werden.

4 Zusätzliche Anforderungen für Auftragnehmer mit direktem Zugang zum internen Konzernnetzwerk

4.1 Definition

Die folgenden Anforderungen müssen von allen Dienstleistern eingehalten werden, die zu einer der folgenden Kategorien gehören:

- Dienstleister, denen Clients (Endgeräte) von einer Volkswagen Konzerngesellschaft zur Verfügung gestellt werden.
- Dienstleister, die über Remotezugänge (z.B. TravelX, Safe, Secure i.Do-Client) oder andere VPN-Lösungen mit direktem Zugriff auf das Volkswagen Corporate Backbone (CBB) angebunden sind.
- Dienstleister, die direkt über das CBB angebunden sind.
- Dienstleister, die über PFN (Central supplier network (CSN)) an das CBB angebunden sind.

Diese Dienstleister können sich sowohl auf dem Gelände der eigenen Firma, als auch auf dem Gelände einer Konzerngesellschaft befinden.

4.2 Anforderungen

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

4.2.1. Interne Organisation

Dienstleister dürfen die Bereitstellung oder Installation von Hardware und Software nur über den für sie zuständigen Fachbereich (Fachbereich des Auftraggebers) durchführen oder initiieren.

Bezüglich der Nutzung der zur Verfügung gestellten Hard- und Software gelten die Regelungen der Auftraggeber (siehe Anhang, 7.2.13).

Das Öffnen des IT-Gerätes und das Durchführen von Veränderungen an der Hardware (z. B. Ein-/Ausbau von Festplatten, Speicherbausteinen) sowie manuelle Veränderungen der Sicherheitseinstellungen (z. B. Browsereinstellungen) ist nur den zuständigen Stellen (siehe Anhang, 7.2.14) gestattet.

Der Einsatz oder das nachträgliche Verändern von Programmen des Auftraggebers ist nur zulässig, wenn diese von den zuständigen Stellen (siehe Anhang, 7.2.14) genehmigt wird.

Auf den zur Verfügung gestellten IT-Geräten sind keine Daten von weiteren Kunden, die nicht zum Konzern gehören, zu verarbeiten.

Das Verwenden von IT-Geräten oder Daten des Auftraggebers durch Mitarbeiter des Dienstleisters erfordert die ausdrückliche Zustimmung des Auftraggebers. Der Auftraggeber ist ermächtigt, jederzeit den Zugriff oder die Benutzung zu untersagen (z.B. bei Missbrauch).

4.2.2. Physische und umgebungsbezogene Sicherheit

Die zur Verfügung gestellten Geräte sind sachgemäß zu behandeln und vor Verlust oder unbefugter Veränderung zu schützen.

Die Vorschriften des Herstellers zum Schutz der Geräte sind einzuhalten.

Durch den Auftraggeber zur Verfügung gestellte Geräte (z.B. Laptops, Mobiltelefone) dürfen nur nach erfolgter Genehmigung vom Werksgelände des Auftraggebers mitgenommen werden.

4.2.3. Schutz vor Schadsoftware und mobilem Programmcode

Bei Verdacht auf Befall durch Schadsoftware dürfen betroffene IT-Geräte und Datenträger nicht weiter benutzt werden. Die zuständigen Stellen (siehe Anhang, 7.2.9) sind sofort zu benachrichtigen.

4.2.4. Backup

Daten sollten auf den zugeordneten Netzlaufwerken gespeichert werden und nicht auf der lokalen Festplatte, da nur im Netzwerk eine zentrale und automatische Datensicherung gewährleistet ist.

Für die Sicherung der Daten, die nicht auf zentralen Netzlaufwerken gespeichert sind (z.B. lokale Festplatte, mobile Datenträger) oder Systemen mit vergleichbarer Funktionalität (z.B. eRoom, SharePoint), ist der Anwender selbst verantwortlich.

Backupdaten und Medien zur Sicherung sind so zu behandeln, wie die originalen Daten.

4.2.5. Zugangskontrolle

4.2.5.1. Geschäftsanforderungen für Zugangskontrolle

Folgende Vorgaben sind durch alle Nutzer zu befolgen:

Allgemeine Anforderungen

- Die Verwendung der Benutzerkennung oder des Kontos einer anderen Person ist nicht gestattet.
- Die Weitergabe von Identifikationsmitteln (z. B. SmartCards oder SecurID-Karten) ist nicht gestattet.

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

- Passwörter oder PINs einer Benutzerkennung, die zur persönlichen Verwendung bestimmt ist (bezeichnet als „persönliche Benutzerkennung“, sind geheim zu halten und dürfen nicht weitergegeben werden.
- Das Speichern oder das Aufschreiben von Passwörtern (z. B. auf Papier, über Mobilgeräte oder in Dateien) ist nicht zulässig, sofern dies nicht als sichere Methode festgelegt ist (siehe Anhang, 7.2.15).
- Sobald der Verdacht der Kompromittierung oder des Bekanntwerdens eines Passworts oder einer PIN besteht, ist dieses bzw. diese unverzüglich zu ändern.
- Temporäre Passwörter (z. B. für neue Konten) sind bei der ersten Anmeldung zu ändern.
- Alle Passwörter oder PINs sind bei der ersten Verwendung zu ändern sowie spätestens nach einem Jahr (Letzteres gilt nur für Passwörter).
- Das Ausspähen von Passwörtern ist nicht gestattet.
- Passwörter sind mindestens als vertraulich zu klassifizieren.
- Wenn Passwörter schriftlich aufbewahrt werden müssen, sind sie durch den Mitarbeiter in einem versiegelten Umschlag an einem geeigneten Ort zu verwahren, der vor unrechtmäßigem Zugriff geschützt ist (z. B. einem Tresor). Bei jeder Änderung ist das verwahrte Passwort entsprechend zu aktualisieren. Der versiegelte Umschlag ist durch den jeweiligen Mitarbeiter abzuzeichnen. Die Personen, die berechtigt sind, den Umschlag zu öffnen, müssen namentlich benannt werden, da es in Ausnahmefällen (z. B. bei Krankheit) nötig sein kann, das verwahrte Passwort zu verwenden. Dabei ist die sogenannte „Zwei-Personen-Regel“ zu befolgen. Jede Öffnung ist zu dokumentieren und dem Mitarbeiter zu berichten. Nach jeder Öffnung muss der Mitarbeiter das Passwort umgehend ändern und wieder sicher verwahren. Als Alternative sind IT-Systeme zulässig, die eine entsprechende Funktionalität gewährleisten (z. B. elektronische Passwort-Tresore).
- Bei Unterbrechung der Bildschirmarbeit im laufenden Betrieb (z. B. Pause, Besprechung) muss der Anwender eine Systemsperre (z. B. passwortgeschützter Bildschirmschoner) aktivieren.
- Anwender, die ihren Multifunktionsausweis zur Anmeldung an IT-Systemen benutzen, haben beim Verlassen des Systems den Ausweis aus dem Lesegerät zu entfernen.

4.2.5.2. Generierung von Passwörtern

Bei der Generierung eines Passworts müssen folgende Anforderungen erfüllt werden:

- Es ist Mitarbeitern (des Auftragnehmers) nicht gestattet, zum Zugriff auf Systeme des Auftraggebers, ein identisches Passwort für berufliche und private Zwecke zu verwenden.
- Es ist Mitarbeitern (des Auftragnehmers) nicht gestattet, ein identisches Passwort für Systeme, die vom Volkswagen-Konzern bereitgestellt werden, und Systeme, die von Dritten bereitgestellt werden (z. B. Anwendungen, Registrierungsdienste im Internet), zu verwenden.
- Die von Systemen erzwungene Mindestlänge für Passwörter ist einzuhalten. Sie richtet sich nach den Vorgaben der entsprechenden Regelung (siehe Anhang, 7.1.2).
- Triviale Passwörter (z.B. „Test123456“) oder Passwörter mit persönlichem Bezug (z. B. Namen, Geburtsdatum) sind nicht zulässig.
- Erfordern bestimmte Systeme oder Anwendungen komplexere Passwörter ((siehe Anhang, 7.1.2), dann sind diese Vorgaben zu erfüllen.
  Hinweis: Für ein sicheres Passwort können Sie Eselsbrücken oder Abkürzungen sowie Verfälschungen verwenden (Beispiel: „Jeden Tag gehe ich ins Bad und wasche mich gründlich“ wird zum Passwort „JTg11B&wmg“).
  Alternativ erzeugt eine Kombination aus vier Wörtern (z.B. „SonneHolzTeeZeit“) ein sehr starkes Passwort, das leicht zu merken ist. Die hier aufgeführten Beispiele dürfen nicht als tatsächliche Passwörter verwendet werden.

4.2.5.3. PINs zum Entsperren von Smartphones und Tablets

Es gelten die in Kapitel 4.2.5.2 beschriebenen Anforderungen.

4.2.5.4. PINs für Authentifizierungs-Smartcards

Es gelten die in Kapitel 4.2.5.2 beschriebenen Anforderungen.

4.2.5.5. Gruppenkennungen

Die Wiederverwendung bestimmter Gruppenkennungen durch mehrere Personen (z. B. Schulungsabteilung, Praktikanten, Hochschulabsolventen) ist unter Einhaltung folgender Voraussetzungen zulässig:

- Die Zuweisung der Benutzerkennung erfolgt durch eine zuständige Person. Diese Person protokolliert schriftlich, wer welche Benutzerkennung zu welchem Zeitpunkt benutzt, und archiviert das entsprechende Protokoll.

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

- Der Erhalt der Benutzerkennung ist durch den jeweiligen Nutzer schriftlich zu bestätigen. Diese Bestätigung wird durch die für die Benutzerkennung zuständige Person verwahrt.
- Nach Erhalt der Benutzerkennung ist das Passwort durch den jeweiligen Nutzer in ein nur ihm bekanntes Passwort zu ändern.
- Nach Rückgabe der entsprechenden Benutzerkennung ist das Passwort durch die zuständige Person in ein nur ihr bekanntes Passwort zu ändern.
- Für die Archivierung der Protokolle gelten die unternehmensspezifischen Archivierungsfristen.

Benutzerkennungen, die gleichzeitig durch mehrere Personen verwendet werden können (sogenannte „Gruppenkennungen"), sind nur dann zulässig, wenn diese Benutzerkennungen ausschließlich das Ausführen von Anwendungen erlauben, die über eine separate Benutzerverwaltung verfügen, einschließlich einer personenbezogenen Authentifizierung, und auf Lesezugriffe beschränkt sind.

4.2.6. Zugangskontrolle für Netze

4.2.6.1. Regelwerk zur Nutzung von Netzdiensten

Ein vom Auftraggeber bereitgestelltes IT-Gerät darf nur dann und nur solange mit unternehmensfremden Netzwerken (z. B. Hot Spot, privates WLAN; ausgenommen Mobilfunknetze) verbunden werden, wenn dies zum Verbindungsaufbau mit dem Konzernnetzwerk (über Remote-Zugriff/VPN) geschieht. Direktes "Surfen" usw. ist nicht zulässig (ausgenommen mit Mobilfunknetzen verbundene Smartphones und Tablets).

Wird die Verbindung nicht mehr benötigt, ist diese zu trennen.

4.2.6.2. Geräteidentifikation in Netzen

Uneingeschränkte Verbindungen von Kommunikationsgeräten (z.B. ohne Firewalls) an das interne Netz (Intranet) sind nur gestattet, wenn diese vom Konzern oder von Gesellschaften gestellt sind, an denen der Konzern oder eine seiner Gesellschaften mehrheitlich beteiligt ist.

5 Zusätzliche Anforderungen für Auftragnehmer ohne direkten Zugang zum internen Konzernnetzwerk

5.1 Definition

Die in Kapitel 5 enthaltenen Anforderungen müssen von allen Dienstleistern eingehalten werden, die zu einer der folgenden Kategorien gehören:

- Dienstleister, die keinen direkten Zugang zum Netzwerk einer Konzerngesellschaft haben
- Dienstleister, die keine Endgeräte zur Verfügung gestellt bekommen, die einer Volkswagen Konzerngesellschaft gehören und lediglich Endgeräte verwenden, die der Firma des Dienstleisters gehören.
- Dienstleister, die nicht über Secure Partner, remote access oder eine andere VPN Lösung angebunden sind.
- Für virtuelle Desktoplösungen, die nur die Übertragung von Bildschirminhalten und zugehörigen Steuerungsdaten erlauben, gelten die Anforderungen, die in diesem Kapitel definiert sind.
- Diese Dienstleister tauschen Daten mit Auftraggeber aus.

Diese Dienstleister befinden sich am Standort ihres Unternehmens und sind an die Regularien ihres Unternehmens gebunden.

5.2 Anforderungen

5.2.1. Interne Organisation

Daten von Konzerngesellschaften müssen von Daten Dritter und besonders von den Daten anderer Kunden des Dienstleisters (z.B. über ein Rechtemanagement) getrennt sein. Daten dürfen nicht für Dritte zugreifbar sein (z.B. durch Verschlüsselung umzusetzen).

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

Die Klassifikation des Auftraggeber muss auf das Klassifikationsschema des Dienstleisters abgebildet werden um sicherzustellen, dass alle erforderlichen Sicherheitsmaßnahmen umgesetzt werden.

Dienstleister müssen die Informationssicherheits-Anforderungen aus dem ihnen zur Erfüllung der Aufgabe übergebenem Regelwerk durch angemessene Sicherheitsmaßnahmen in ihrem eigenen Unternehmen abbilden.

Zugriff auf Daten des Auftraggebers darf Mitarbeitern des Dienstleisters nur nach dem Need-to-know-Prinzip (Kenntnis nur bei Bedarf) gewährt werden.

6 Verantwortlichkeiten

Diese Regelung ist von allen Dienstleistern, entsprechend der Definition in diesem Dokument, einzuhalten.

Abweichungen von diesen Handlungsleitlinien, die das Sicherheitsniveau senken, sind nur temporär und nach Rücksprache mit den zuständigen Stellen (siehe Anhang 7.2.16) und dem Auftraggeber zulässig.

7 Anhang

7.1 Mitgeltende Dokumente

7.1.1. Unternehmensrichtlinie U_2.024 - Anlage Nr. 6 Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren

7.1.2. 03.01.05 Identity und Access Management

7.2 Unternehmensspezifische Ausprägungen

7.2.1. Die Verarbeitung (z.B. Erhebung, Nutzung, Löschen) von personenbezogenen Daten (z. B. Name, Telefonnummer, Mailadresse, Geburtsdatum) ist nur zulässig unter Einhaltung der gesetzlichen und Unternehmens-Vorschriften zum Schutz Personenbezogenen Daten

Personenbezogene Daten, die bei der Auftraggeber gespeichert sind, dürfen nur im Rahmen der dienstlichen Tätigkeiten, lediglich für den dienstlichen Zweck verarbeitet und genutzt werden. Eine Übermittlung dieser Daten an unbefugte Dritte (z. B. Kunden, Partnerfirmenmitarbeiter, Mitarbeiter) ist nicht zulässig.

Die für die Klassifikation von personenbezogenen Daten relevanten Informationen sind im Audi Mynet unter Gesellschaften/Audi Hungaria / Organisation / Zentrale Funktionen / IT Sicherheit

IT-Geräte und Datenträger, auf denen personenbezogene, vertrauliche oder geheime Daten gespeichert sind, dürfen das Werksgelände der Auftraggeber grundsätzlich nur verschlüsselt verlassen.

7.2.2. http://www.vwgroupsupply.com

7.2.3. AUDI HUNGARIA Service Desk, Tel. 1400.

7.2.4. Verantwortlichkeit: Organisationseinheit (OE) Unternehmenskommunikation und Regierungsbeziehungen

7.2.5. Personenbezogene, Vertrauliche und geheime Papierdokumente sind gesichert zu entsorgen (z. B. in Datenschutzcontainern). Nicht mehr benötigte Datenträger sind zuverlässig durch Überschreiben zu löschen oder physikalisch zu zerstören.

7.2.6. Die Dokumente von dem Auftraggeber, die unter die Geheimhaltung liegen, sind nur die im Unternehmensrichtlinie U_2.024 - Anlage Nr. 6 Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren Kapitel 8.1 beschriebenen Authentifizierungsverfahren gemäß deren Eistufung anzuwenden.

7.2.7. IT-Geräte und Datenträger, auf denen personenbezogene, vertrauliche oder geheime Daten der Auftraggeber gespeichert sind, dürfen das Werksgelände der Auftraggeber grundsätzlich nur verschlüsselt verlassen.

7.2.8. AUDI HUNGARIA Service Desk, Tel. 1400

KSU-Klasse wählen

[X] KSU 2.1 / Aufbewahrungsfrist: 7 Jahre ab Ereignis

[ ] KSU __ (abhängig von den beschriebenen Inhalten)

Datenklassifizierung

[ ] Öffentlich [X] Intern [ ] Vertraulich [ ] Geheim

7.2.9. Organisationseinheit (OE) IT Security

7.2.10. Organisationseinheit (OE) IT Security

7.2.11. IT Security, Datenschutzbeauftragte, Know-how Schutz

7.2.12. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) – „GDPR"; Sowie der 2011. CXII Gesetzt über den Informations-Selbstbestimmungsrecht und Informationsfreiheit, und weitere, relevante Gesetzte.

7.2.13. Jeder Auftragnehmer ist dafür verantwortlich, dass Informationen, Programme und IT-Geräte nur für Unternehmenszwecke und im Rahmen der jeweiligen Aufgabenstellung ordnungsgemäß eingesetzt und genutzt werden.

7.2.14. Verantwortlichkeit: Solution Center Infrastructure/End User Computing

7.2.15. Empfohlen wird die Verwendung von Passwort Safes wie z.B. KeePass

7.2.16. It-Sicherheit@audi.hu