Allgemeine IT-Bedingungen der gemäß ungarischem Recht gegründeten und ins Handelsregister des Landgerichts Győr unter der HR-Nr. 08-10-001840 eingetragenen AUDI HUNGARIA Zrt. – ab 01.05.2019 gültige Version

1. Geltungsbereich

1.1. Diese Allgemeinen IT-Bedingungen (nachstehend **„AIB“**) gelten für die von AUDI HUNGARIA Zrt. als Auftraggeber (nachstehend auch **„Auftraggeber“** oder **„AH“**) in Anspruch genommenen informationstechnologischen oder kommunikationstechnologischen Dienstleistungen (nachstehend **„IT“**-Dienstleistungen). 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 und 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 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.

4.3. 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 AH

Sicherheitsschulungen und Sensibilisierungstrainings sicherstellen, an denen diese Personen verbindlich teilzunehmen haben. Bei Vertragsleistungen, bei denen auch Informationen von AH 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 AH-Informationen haben und periodisch oder kontinuierlich an diese Daten herankommen können, zu bestimmen, zu dokumentieren und ihre Namen und Daten nachweisbar dokumentiert an AH zu übermitteln (unter Berücksichtigung der einschlägigen Datenschutzregelungen).

4.4. 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.

4.5. Zur schnellen, effizienten und einheitlichen Behandlung von Sicherheitsvorfällen hat der Partner die Incident-Management-Verfahren des Auftraggebers ab Beginn der jeweiligen Dienstleistung verbindlich einzuhalten. Der Partner hat den Auftraggeber in jedem Fall unverzüglich schriftlich über IT-Sicherheitsvorfälle zu unterrichten.

4.6. 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.

4.7. 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.

4.8. Alle Partner haben die Festlegungen nach Anlage 1 dieser AIB („IT-Sicherheitshandlungsleitlinien für externe Mitarbeiter und Partnerfirmen“) einzuhalten.

4.9. Alle Partner, die IT-Betriebsdienste erbringen, haben die Festlegungen nach Anlage 2 dieser AIB („IT-Sicherheitshandlungsleitlinien für Systembetreiber und Administratoren“) einzuhalten.

4.10. Alle Partner, die Softwareentwicklungsdienste erbringen, haben die Festlegungen nach Anlage 3 dieser AIB („IT-Sicherheitshandlungsleitlinien für Systementwickler“)

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: 01.05.2019, zu welchem Zeitpunkt die am 24.09.2018 erlassenen Allgemeinen IT-Vorschriften außer Kraft treten.

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

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

Bankverbindungen:
Commerzbank Budapest
HUF: 14220108-42431006-00000000
IBAN: HU47 14220108 42431006 00000000
(SWIFT: COBAHUHXXXX)

Commerzbank Ingolstadt
EUR: 72140052-192247500
IBAN: DE31 7214 0052 0192 2475 00
(SWIFT: COBADEFF721)

IT Sicherheitshandlungsleitlinien für Partnerfirmen

Version: 5.0 (11.05.2018)
Herausgeber: IT Sicherheit
Regelung Nr.: Übergeordnete Regelung 08

Geltungsbereich

Die Handlungsleitlinien gelten für Partnerfirmen (im Folgenden „Dienstleister" genannt), die Dienstleistungen für die AUDI HUNGARIA Zrt. (im Folgenden „ AUDI HUNGARIA" oder „Auftraggeber" genannt) erbringen.

Inhalt

1. Ziel

Die für die Nutzung von Informationen des Auftraggebers und/oder IT-Geräten (z. B. Personalcomputer, Workstations einschließlich mobiler Rechner wie Notebooks, Smartphones, Tablet-PCs, usw.) des Auftraggebers zu beachtenden IT-Sicherheitsregelungen für Partnerfirmen sind in diesen IT-Sicherheitshandlungsleitlinien definiert. Diese Handlungsleitlinien richten sich an die Geschäftsleitung der Partnerfirmen, deren Mitarbeiter sowie deren Erfüllungs-/Verrichtungshilfen (im Folgenden Auftragnehmer genannt).

Die IT-Sicherheitshandlungsleitlinien dienen dem Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Nachweisbarkeit von Informationen sowie der Wahrung der Rechte und Interessen des Auftraggebers und aller natürlichen und juristischen Personen, die mit AUDI HUNGARIA Zrt. in geschäftlicher Beziehung stehen bzw. für diese arbeiten.

2. Regelungen

2.1 Organisation der Informationssicherheit

2.1.1 Interne Organisation

Die Beschaffung und Installation der zur Verfügung gestellten Hard- und Software erfolgt ausschließlich in Zusammenarbeit mit den zuständigen Stellen (siehe Anhang 3.1, Ziff. 1.) nach den geltenden Genehmigungsverfahren.

Bezüglich der Nutzung der zur Verfügung gestellten Hard- und Software gelten die Regelungen (siehe Anhang 3.1, Ziff. 2.) von Audi Hungaria Zrt.

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 3.1, Ziff. 3.) erlaubt.

Der Einsatz oder das nachträgliche Verändern von Programmen des Auftraggebers ist nur zulässig, wenn diese von den zuständigen Stellen (siehe Anhang 3.1, Ziff. 3.) autorisiert sind.

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

Bezüglich des Mitbringens privater IT-Geräte gelten die Regelungen von Audi Hungaria.

Die Daten von Audi Hungaria sind von denen weiterer nicht zu Audi Hungaria gehörenden Kunden zu trennen.

Für die Speicherung sowie sonstige Verarbeitung und Nutzung von personenbezogenen Daten und von Daten, die der Geheimhaltung unterliegen, gelten die Regelungen von Audi Hungaria (siehe Anhang 3.1, Ziff. 4.).

Die Nutzung privat erworbener Programme oder Daten zu dienstlichen Zwecken ist verboten.

Der Einsatz von firmeneigener Software und Daten auf privaten IT-Geräten und Datenträgern ist nicht gestattet.

Der Einsatz von firmeneigener Software und Daten auf nicht freigegebenen Speichermedien (z. B. nicht freigegebene Fileservices/Cloud im Internet) ist nicht gestattet. (z.B.: SkyDrive, Google drive, Dropbox). Für weitere Informationen bitte mit IT Sicherheit kontaktieren: it-sicherheit at audi punkt hu.

2.1.2 Externe Beziehungen

Die Nutzung von IT-Geräten und Daten des Auftraggebers durch Mitarbeiter von Partnerfirmen bedarf der ausdrücklichen Zustimmung des auftraggebenden Fachbereichs. Dieser hat das Recht, die Nutzung jederzeit zu unterbinden (z. B. bei Missbrauch).

Der Kreis der autorisierten Mitarbeiter von Partnerfirmen muss durch den auftraggebenden Fachbereich festgelegt werden und ist möglichst klein zu halten.

Mitarbeiter von Partnerfirmen sind von ihrer Geschäftsleitung auf die Geheimhaltung im Sinne der bestehenden Vertraulichkeitsvereinbarung zu verpflichten. Dies gilt entsprechend für Mitarbeiter von Subunternehmen der Partnerfirmen. Dem auftraggebenden Fachbereich ist jederzeit Einsicht in diese Vereinbarungen zu gewähren.

Die Weitergabe von Daten an Dritte ist ausdrücklich untersagt, es sei denn der auftraggebende Fachbereich stimmt diesem Vorhaben schriftlich zu.

2.2 Management von organisationseigenen Werten

2.2.1 Regelungen für die Klassifizierung

Der Informationseigentümer ist verantwortlich für die Klassifikation seiner Informationen hinsichtlich Vertraulichkeit, Verfügbarkeit, Integrität und Nachweisbarkeit.

2.2.2 Vertraulichkeit

Informationen, die nicht zur allgemeinen Veröffentlichung bestimmt sind, sind nur den dafür Berechtigten zugänglich zu machen.

Folgende Stufen zur Klassifikation von Informationen hinsichtlich der Anforderungen an die Vertraulichkeit sind hierfür definiert:

Einstufung	Definition
Öffentlich	Informationen, die keinerlei Restriktionen unterliegen und z. B. vom Unternehmen in Zeitungen oder im Internet veröffentlicht werden. Die Verwendung von Unternehmensinformationen in der Öffentlichkeit bedarf der Zustimmung der zuständigen Stellen (siehe Anhang 3.1, Ziff. 5.). Beispiele: Pressemitteilungen, Produktkatalog für Kunden
Intern	Informationen, die nur für den internen Gebrauch und nicht für die allgemeine Öffentlichkeit bestimmt sind. Konsequenzen beim Verlust der Vertraulichkeit sind denkbar, jedoch geringfügiger Natur, z. B.: • Schadensersatzansprüche einzelner Personen oder Organisationen sind wenig wahrscheinlich Beispiele: Dienstliche Kommunikationsdaten (z.B. Telefon-Nr., E-Mail-Adresse), Vorgaben zum Arbeitsschutz, Arbeitsordnung

Vertraulich	Informationen, deren Kenntnis durch Unbefugte oder deren missbräuchliche Weitergabe oder Verwendung das Erreichen von Produkt- und Projektzielen gefährden kann und die daher nur einem begrenzten, berechtigten Personenkreis zugänglich gemacht werden dürfen. Konsequenzen beim Verlust der Vertraulichkeit sind wahrscheinlich und messbar, z. B.: • Verlust von Kunden • Rückgang von Verkaufszahlen / Umsatz • Schadensersatzansprüche einzelner Personen oder Organisationen Beispiele: Personenbezogene Daten, die über dienstliche Kommunikationsdaten hinausgehen (z.B. Gehaltsdaten), Budgetpläne, Revisionsberichte
Geheim	Informationen, deren Kenntnis durch Unbefugte oder deren missbräuchliche Weitergabe oder Verwendung das Erreichen von Unternehmenszielen nachhaltig gefährden kann und die daher einem äußerst restriktiven Verteiler und strikten Kontrollen unterliegen müssen. Eine Verletzung der Vertraulichkeit hat erhebliche Auswirkungen auf die Außenwirkung / das Erscheinungsbild des Unternehmens und/oder wirtschaftliche Konsequenzen, z. B.: • erheblicher Verlust von Kunden • deutliche Einbrüche bei Verkaufszahlen / Umsatz • massive Schadensersatzansprüche durch zahlreiche Personen oder Organisationen • Ausschluss aus bestimmten Märkten • nachteilige Auswirkungen auf das öffentliche Ansehen Beispiele: Besondere Arten personenbezogener Daten (z.B. Gesundheitsdaten), Cycle-Pläne, Vorstandsvorlagen, Pläne zur Unternehmensstrategie, Designbilder von neuen Prototypen

2.2.3 Integrität

Eine fehlerfreie Verarbeitung der Informationen sowie der Schutz vor unberechtigter Veränderung sind zu gewährleisten.

Folgende Stufen zur Klassifikation von Informationen hinsichtlich der Anforderungen an die Integrität sind hierfür definiert:

Einstufung	Definition
Gering	Eine Verletzung der Integrität hat keine absehbaren Auswirkungen auf die Geschäftstätigkeit oder auf die Außenwirkung / das Erscheinungsbild des Unternehmens.
Mittel	Eine Verletzung der Integrität hat nur geringe Auswirkungen auf die Geschäftstätigkeit und/oder nur geringe Auswirkungen auf die Außenwirkung / das Erscheinungsbild des Unternehmens. Konsequenzen sind denkbar, jedoch geringfügiger Natur, z. B.: • geringfügige Verzögerungen bei Arbeitsabläufen • Fehler / Störungen wirken sich nicht auf Arbeitsergebnisse aus (keine Produktionsausfälle) • Entscheidungen werden nicht beeinträchtigt • Schadensersatzansprüche einzelner Personen oder Organisationen sind wenig wahrscheinlich Beispiele: Standort-Pläne, Organigramme, einzelne interne Telefonnummern
Hoch	Eine Verletzung der Integrität hat spürbare Auswirkungen auf die Geschäftstätigkeit und/oder auf die Außenwirkung / das Erscheinungsbild des Unternehmens. Konsequenzen sind wahrscheinlich und messbar, z. B.: • Verlust von Kunden wahrscheinlich • Rückgang von Verkaufszahlen / Umsatz wahrscheinlich • Deutliche Verzögerungen bei Arbeitsabläufen • Fehler / Störungen wirken sich spürbar auf Arbeitsergebnisse aus (hohe Produktionsausfälle) bzw. wenige Serviceprozesse fallen aus • Entscheidungen werden beeinträchtigt / Fehlentscheidungen sind wahrscheinlich • Schadensersatzansprüche einzelner Personen oder Organisationen sind wahrscheinlich Beispiele: JIT Bestellungen, Presse-Mitteilungen, Inhalte des Internetauftritts, Daten für die Produktionssteuerung
Sehr hoch	Eine Verletzung der Integrität hat erhebliche Auswirkungen auf die Geschäftstätigkeit und/oder auf die Außenwirkung / das Erscheinungsbild des Unternehmens mit entsprechenden wirtschaftlichen Konsequenzen, z. B.: • erheblicher Verlust von Kunden

	• Schadensersatzansprüche durch zahlreiche Einzelpersonen oder Organisationen • deutliche Einbrüche bei Verkaufszahlen / Umsatz • Ausschluss aus bestimmten Märkten • erhebliche Verzögerungen bei Arbeitsabläufen • Fehler / Störungen wirken sich massiv auf Arbeitsergebnisse aus bzw. mehrere Serviceprozesse fallen aus (sehr hohe Produktionsausfälle) • Entscheidungen werden stark beeinträchtigt / Fehlentscheidungen Beispiele: finanzielle Berichterstattung (z. B. Jahresabschluss), Patentschriften, kryptografische Schlüssel, Gehaltsabrechnung

2.2.4 Nachweisbarkeit

Der Zugriff auf schützenswerte Informationen und die Durchführung von Transaktionen muss unbestreitbar sein.

Folgende Stufen zur Klassifikation von Informationen hinsichtlich der Anforderungen an die Nachweisbarkeit sind hierfür definiert:

Einstufung	Definition
Gering	Es gibt keine Anforderungen an Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit.
Mittel	Für ändernde Zugriffe müssen Art der Änderungen (Hinzufügen, Löschen, Ändern), durchführende Personen und Zeitpunkte nachvollziehbar sein.
Hoch	Für ändernde Zugriffe müssen Änderungen (inkl. Stand vor Änderung), durchführende Personen und Zeitpunkte nachvollziehbar sein.
Sehr hoch	Für lesende und ändernde Zugriffe müssen Änderungen (inkl. Stand vor Änderung), durchführende Personen und Zeitpunkte nachvollziehbar sein.

2.2.5 Verfügbarkeit

Informationen sind innerhalb eines vereinbarten Zeitraums zur Verfügung zu stellen.

Folgende Stufen zur Klassifikation von Informationen hinsichtlich der Anforderungen an die Verfügbarkeit sind hierfür definiert:

Einstufung	Definition

Gering	Das IT-System kann bezüglich Ausfall oder unzureichender Antwortzeit weniger als 95% verfügbar sein, ohne dass ein signifikanter Schaden (finanziell oder für das Image des Unternehmens) entsteht. Beispiel: Intranetanwendung mit allgemeinen Informationen für Mitarbeiter
Mittel	Das IT-System muss bezüglich Ausfall oder unzureichender Antwortzeit zu 95% verfügbar sein. Danach entsteht ein signifikanter Schaden (finanziell oder für das Image des Unternehmens). Beispiel: Bewerber-Portal
Hoch	Das IT-System muss bezüglich Ausfall oder unzureichender Antwortzeit 98% verfügbar sein, sonst droht ein signifikanter Schaden (finanziell oder für das Image des Unternehmens). Beispiele: Gehaltsabrechnung, Buchhaltung
Sehr hoch	Das IT-System muss bezüglich Ausfall oder unzureichender Antwortzeit zu 99% verfügbar sein, sonst droht ein signifikanter Schaden (finanziell oder für das Image des Unternehmens). Beispiel: IT-System, dessen Ausfall einen sofortigen Produktionsstillstand zur Folge hat Ein signifikanter Schaden ist dabei beispielsweise: • Verlust von Kunden • Schadensersatzansprüche durch zahlreiche Einzelpersonen oder Verbände • deutliche Einbrüche bei Verkaufszahlen / Umsatz • Ausschluss aus bestimmten Märkten • Fehler / Störungen wirken sich massiv auf Arbeitsergebnisse aus bzw. mehrere Serviceprozesse fallen aus (sehr hohe Produktionsausfälle)

2.2.6 Kennzeichnung von und Umgang mit Informationen

Informationen dürfen nur dem jeweils berechtigten Personenkreis zugänglich gemacht werden. Dies ist nur im Rahmen der vereinbarten Aufgabenstellungen sowie unter Einhaltung bestehender Regelungen zulässig. Dabei ist der Grundsatz "Kenntnis nur wenn nötig" ("Need-To-Know") anzuwenden.

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

Einstufung	**Vorgaben zum Umgang**

Öffentlich	• Kennzeichnung: Keine • Vervielfältigung und Weitergabe: Keine Einschränkungen • Speicherung: Keine Einschränkungen • Löschen: Keine Einschränkungen • Entsorgung: Keine Einschränkungen
Intern	• Kennzeichnung: Keine (oder Intern) • Vervielfältigung und Weitergabe: Nur an berechtigte Konzernmitarbeiter und berechtigte Dritte innerhalb des Aufgaben- oder Anwendungsbereichs • Speicherung: Vor unberechtigter Einsichtnahme schützen • Löschen: Nutzung der systemseitig vorhandenen bzw. zur Verfügung gestellten Löschfunktionen • Entsorgung: Ordnungsgemäße Entsorgung (siehe Anhang 3.1, Ziff. 6.)
Vertraulich	• Kennzeichnung: "Vertraulich". Kennzeichnung auf der ersten Seite des Dokumentes in elektronischer und gedruckter Form • Vervielfältigung und Weitergabe: Nur an einen begrenzten Bereich berechtigter Konzernmitarbeiter und berechtigter Dritter innerhalb des Aufgaben- oder Anwendungsbereichs. Dabei ist der Verteilende in der Verantwortung, geeignete Verteilungswege zu nutzen, um die Informationen und Daten vor unberechtigter Einsichtnahme bzw. unberechtigtem Mithören zu schützen (z. B. durch Verschlüsselung). • Speicherung: Nur einem begrenzten Bereich berechtigter Konzernmitarbeiter und berechtigter Dritter innerhalb des Aufgaben- oder Anwendungsbereichs zugänglich (z. B. durch geschlossene Benutzergruppen). Dafür sind geeignete Speicherorte bzw. Speichermedien zu nutzen. • Löschen: Nicht mehr benötigte Daten sind zu löschen. • Entsorgung: Ordnungsgemäße Entsorgung (siehe Anhang 3.1, Ziff. 6.)
Geheim	• Kennzeichnung: "Geheim". Kennzeichnung auf jeder Seite des Dokumentes. • Vervielfältigung und Weitergabe: Nur an einen äußerst begrenzten Bereich (z. B. namentliche Liste) berechtigter Konzernmitarbeiter und berechtigter Dritter innerhalb des

	Aufgaben- oder Anwendungsbereichs nach vorheriger Genehmigung des Informationseigentümers. Dabei sind die Daten, soweit technisch möglich nach dem aktuellen Stand der Technik, zu verschlüsseln. Sofern dies technisch nicht möglich ist, sind vergleichbare Schutzmaßnahmen einzusetzen. Zusätzlich sind weitere technische oder organisatorische Schutzmaßnahmen zu prüfen (z. B. Weitergabe- oder Druckverbot, Wasserzeichen). Es sind geeignete Vorkehrungen zu treffen, um ein Mithören zu verhindern (z. B. verschlüsselte Videokonferenz). • Speicherung: Nur einem äußerst begrenzten Bereich (z. B. namentliche Liste) berechtigter Konzernmitarbeiter und berechtigter Dritter innerhalb des Aufgaben- oder Anwendungsbereichs zugänglich (z. B. durch geschlossene Benutzergruppen). Dabei sind die Daten, soweit technisch möglich nach dem aktuellen Stand der Technik zu verschlüsseln. Sofern dies technisch nicht möglich ist, sind vergleichbare Schutzmaßnahmen einzusetzen. • Löschen: Nicht mehr benötigte Daten sind zu löschen. • Entsorgung: Ordnungsgemäße Entsorgung (siehe Anhang 3.1, Ziff. 6.)

Zuständig für die Kennzeichnung ist der Ersteller der Informationen.

Ist eine Information nicht gekennzeichnet, ist diese als "Intern" zu behandeln, es sei denn es liegt eine Zustimmung der zuständigen Stellen (siehe Anhang 3.1, Ziff. 5.) zur Veröffentlichung vor. In diesem Fall sind die Informationen als öffentlich zu behandeln.

Die Regelungen zum Umgang mit Informationen (Kennzeichnung, Vervielfältigung, Weitergabe, Speicherung, Löschen, Entsorgung) gelten auch für IT-Systeme (z. B. für Datenbanken, Backupmedien).

Die Einstufung von Informationen hinsichtlich Integrität, Nachweisbarkeit und Verfügbarkeit dient vorrangig der Ableitung von Sicherheitsanforderungen an Informationssysteme, die diese Informationen verarbeiten.

2.3 Personalsicherheit

Eine nicht mehr benötigte Benutzerkennung oder ein nicht mehr benötigtes Zugriffsrecht ist von dem jeweiligen Nutzer unverzüglich bei den jeweiligen auftraggebenden Stellen 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 sind zurückzugeben.

Der Verlust von an den Benutzer übergebenen IT-Geräten sowie von Medien zum Zwecke der Authentifizierung sind durch den Benutzer umgehend der auftraggebenden Stelle zu melden.

2.4 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.

IT-Geräte, die vertrauliche oder geheime Daten speichern oder bearbeiten, sind so aufzustellen, dass das Risiko eines Zugriffs und einer Einsicht durch Unbefugte minimiert wird.

Vom auftraggebenden Fachbereich bereitgestellte Geräte (z. B. Laptops, Mobiltelefone) dürfen nur mit dessen Genehmigung außerhalb des Werkes mitgenommen werden. Ein Verlust dieser IT-Geräte ist unverzüglich an die zuständigen Stellen zu melden (siehe Anhang 3.1, Ziff. 7.).

2.5 Betriebs- und Kommunikationsmanagement

2.5.1 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 3.1, Ziff. 8.)sind sofort zu benachrichtigen.

2.5.2 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), ist der Anwender selbst verantwortlich.

2.5.3 Handhabung von Speicher- und Aufzeichnungsmedien

Datenträger (z. B. CDs, DVDs, USB-Sticks, Festplatten) sind gegen Verlust, Zerstörung und Verwechslung sowie gegen den Zugriff Unbefugter zu sichern.

Nicht mehr benötigte Datenträger sind einer sicheren Entsorgung zuzuführen (siehe Anhang 3.1, Ziff. 6.).

2.5.4 Austausch von Informationen

Bei allen Gesprächen über vertrauliche oder geheime Informationen, inklusive Telefongesprächen, ist darauf zu achten, dass diese nicht unbefugt mitgehört werden können.

Externe Faxnummern und E-Mail-Adressen sind aktuellen Kommunikationsverzeichnissen zu entnehmen oder vom Empfänger zu erfragen, um eine Fehlleitung der übertragenen Daten zu verhindern.

Vor einer Faxübertragung von vertraulichen Daten ist die Übertragung beim Kommunikationspartner telefonisch anzukündigen. Nach der Übertragung ist der ordnungsgemäße Empfang des Fax telefonisch zu kontrollieren. Die Faxbestätigung ist vom Versender nach der Übertragung aus dem Faxgerät zu entnehmen.

Es ist darauf zu achten, dass alle notwendigen und geeigneten Vorkehrungen getroffen werden (z. B. Verschlüsselung), die vor Einsichtnahme, Veränderung und Löschung der Informationen durch Unbefugte (das sind auch Angehörige des Familien- und Freundeskreises) beim Transport schützen.

Beim Transport von IT-Geräten und Datenträgern über die Werksgrenzen hinaus sind die Regelungen und Betriebsvereinbarungen von Audi Hungaria zu beachten.

Der Ersteller ist als Urheber einer E-Mail für den Inhalt und Verteiler verantwortlich, der Empfänger für die weitere Bearbeitung und die Weiterverteilung einer E-Mail.

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

2.6 Zugangskontrolle

2.6.1 Geschäftsanforderungen für Zugangskontrolle

Die Nutzung einer fremden Benutzerkennung ist grundsätzlich nicht zulässig.

Die Weitergabe von Medien zur Identifizierung (z. B. Smartcards, SecurID-Karten) ist grundsätzlich nicht zulässig.

Die Weitergabe des Kennwortes oder der PIN einer zur persönlichen Nutzung zugeordneten Benutzerkennung (sog. "personenbezogene Benutzerkennung") ist grundsätzlich nicht zulässig.

Die Wiederverwendung von personenbezogenen Benutzerkennungen durch verschiedene Personen (z. B. Schulungsteilnehmer, Praktikanten, Diplomanden) ist unter Einhaltung folgender Maßnahmen zulässig:

- Die Vergabe der Benutzerkennungen ist durch eine verantwortliche Person zu verwalten. Diese Person muss einen schriftlichen Nachweis führen, wer wann welche Benutzerkennung genutzt hat. Der Nachweis muss bei dieser Person abgelegt werden.
- Die Übernahme der Benutzerkennung ist durch den jeweiligen Nutzer schriftlich zu bestätigen. Die Bestätigung verbleibt bei der für die Benutzerkennung zuständigen Person.
- Bei Übergabe der jeweiligen Benutzerkennung muss das Kennwort vom jeweiligen Nutzer auf ein nur ihm bekanntes Kennwort abgeändert werden.
- Für die Aufbewahrung der Nachweise sind die gesellschaftsspezifischen Aufbewahrungsfristen zu beachten.

Benutzerkennungen, die von mehreren Personen gleichzeitig genutzt werden können, (sog. "Gruppenkennungen") sind grundsätzlich nicht zulässig, es sei denn, es können mit dieser

Benutzerkennung ausschließlich Applikationen aufgerufen werden, die eine eigene Benutzerverwaltung haben oder die nur lesenden Zugriff erlauben.

2.6.2 Benutzerverantwortung

Bei der Passwortfestlegung sind die folgenden Mindestforderungen zu beachten:

- Es ist eine mindestens 8-stellige Kombination aus mindestens 3 der folgenden 4 Kriterien zu verwenden:
    - Großbuchstaben
    - Kleinbuchstaben
    - Ziffern
    - Sonderzeichen
- Insbesondere dürfen keine trivialen Kombinationen (z. B. "AAAAAAAA") oder Aspekte aus dem persönlichen Umfeld (z. B. Namen, Geburtsdatum) verwendet werden.

Bei der Festlegung von Passwörtern zur Windows-Anmeldung sind mindestens 10-stellige Passwörter aus mindestens 3 der oben genannten 4 Kriterien zu verwenden. Dies können z.B. Merksätze (Passwort: "Sicher-ist-besser!") oder auch Abkürzungen und Verfälschung von Merksätzen (Merksatz "Morgens stehe ich früh auf und putze meine Zähne." wird zu Passwort: "Ms1fa&pmZ.") sein. (Die hier angegebenen Beispiele sind nicht als eigene Passwörter zu verwenden.)

Bei der Vergabe von PINs für Identifikationsmedien (z. B. Smartcards, SecurID-Karten) sind die folgenden Mindestforderungen zu beachten:

- Es ist eine mindestens 4-stellige Ziffernkombination für SecurID-Karten sowie eine mindestens 6-stellige Ziffernkombination für sonstige Medien (z. B. Smartcards) zu verwenden. Insbesondere dürfen keine trivialen Kombinationen (z. B. "111111") oder Aspekte aus dem persönlichen Umfeld (z. B. Geburtsdatum) verwendet werden.

Die folgenden Mindestforderungen beim Umgang mit personenbezogenen Passwörtern bzw. PINs (im Folgenden Passwörter genannt) sind zu beachten:

- Eine Speicherung von Passwörtern ist nur sicher verschlüsselt zulässig.
- Das Passwort muss bei der Erstnutzung und dann mindestens alle 90 Tage geändert werden (Dies gilt nicht für PIN’s).
- Das Passwort ist unverzüglich zu ändern, wenn der Verdacht besteht, dass es Dritten bekannt wurde.
- Das Ausspähen von Passwörtern ist nicht zulässig.
- Sofern Passwörter schriftlich hinterlegt werden müssen, sind diese vom Mitarbeiter in einem geschlossenem Umschlag an geeigneter Stelle (vor unerlaubtem Zugriff geschützt (z. B. Panzerschrank)) zu hinterlegen und bei jeder Änderung des Passwortes zu aktualisieren. Der verschlossene Umschlag ist vom jeweiligen Mitarbeiter zu unterschreiben. Die öffnungsberechtigten Personen sind auf dem Umschlag namentlich zu benennen. Wird es in besonderen Ausnahmefällen notwendig, das hinterlegte Passwort zu nutzen (z. B. bei Krankheit), so hat dies nach

dem " Mehr-Augen-Prinzip" zu geschehen. Jede Öffnung ist zu dokumentieren und dem Mitarbeiter mitzuteilen. Nach jeder Öffnung ist das Passwort vom Mitarbeiter unverzüglich zu ändern und erneut zu hinterlegen. IT-Systeme, die diesen Anforderungen genügen, sind ebenfalls zulässig (z. B. Passwortsafe).

Bei Verlassen des Systems im laufenden Betrieb (z. B. Pause, Besprechung) hat der Anwender eine Systemsperre (z. B. passwortgeschützter Bildschirmschoner) zu aktivieren.

Mitarbeiter, die Ihren Multifunktionsausweis zur Anmeldung an IT-Systeme benutzen, haben beim Verlassen des Systems den Ausweis aus dem Lesegerät zu entfernen.

2.6.3 Zugangskontrolle für Netze

2.6.3.1 Regelwerk zur Nutzung von Netzdiensten

Ein vom Unternehmen bereitgestelltes IT-Gerät darf nur dann und nur solange mit unternehmensfremden Netzwerken (z. B. Hot Spot, privates WLAN) verbunden werden, wenn dies zum Verbindungsaufbau mit dem Netzwerk von Audi Hungaria geschieht.

2.6.3.2 Geräteidentifikation in Netzen

Der nicht eingeschränkte Anschluss (z. B. durch Firewall) von IT-Geräten an das interne Netz (Intranet) ist nur dann gestattet, wenn diese von Audi Hungaria gestellt sind.

Soweit Daten vom Auftraggeber auf mobilen IT-Geräten oder mobilen Systemen des Auftragnehmers gespeichert sind, sind diese mittels Hardware und Software gemäß dem aktuellen Stand der Technik zu verschlüsseln.

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

2.7 Umgang mit Informationssicherheitsvorfällen

IT-Sicherheitsereignisse (z. B. auftretende Störungen, Verstöße gegen das IT-Sicherheitsregelwerk) sind sofort an die zuständigen Stellen (siehe Anhang 3.1, Ziff. 8.) zu melden.

Vermutete Verwundbarkeiten und Schwachstellen von IT-Systemen sind an die zuständigen Stellen (siehe Anhang 3.1, Ziff. 9.) zu melden.

Beim Verdacht auf Verlust von vertraulichen oder geheimen Informationen muss dies sofort an die zuständige Stelle gemeldet werden (siehe Anhang 3.1, Ziff. 9.).

2.8 Einhaltung von Vorgaben

Geistige Eigentumsrechte (z. B. Urheberrechte für Software, Dokumente und fremdes Bildmaterial, Rechte an Entwürfen, Warenzeichen, Patente und Quellcodelizenzen) sind zu wahren.

Insbesondere ist der Einsatz nicht lizenzierter Software (Raubkopien) gemäß geltender gesetzlicher Bestimmungen verboten.

Lizenzsoftware unterliegt gesetzlichen Bestimmungen zum Schutz des Urheberrechts (z. B. stellt die Vervielfältigung von Software, außer für Sicherungs- und Archivierungszwecke, einen Verstoß gegen das Urheberrecht dar). Verstöße gegen diese Bestimmungen können zu strafrechtlichen Maßnahmen sowie Unterlassungs- und Schadensersatzansprüchen führen.

Lizenzsoftware darf nur für den vereinbarten Zweck und ausschließlich nach den bestehenden Bestimmungen und den mit dem Hersteller getroffenen Lizenzvereinbarungen genutzt werden.

Die jeweiligen nationalen Gesetze und Regelungen für den Datenschutz sind einzuhalten.

Auftragnehmer sind von der Geschäftsleitung der Partnerfirma auf die gesetzlichen Regelungen für den Datenschutz zu verpflichten.

2.9 Verantwortlichkeiten

Abweichungen von diesen Handlungsleitlinien, die das Sicherheitsniveau senken, sind nur in Abstimmung mit den zuständigen Stellen (siehe Anhang 3.1, Ziff. 9.) und nur zeitlich begrenzt zulässig.

3. Weiterführende Dokumentation, Anlagen

3.1 Referenzen

	Beschreibung
1.	Einkauf, IT, Controlling.
2.	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. Der Einsatz privater Software und Daten auf von dem Auftraggeber gestellten IT-Geräten ist nicht gestattet.
3.	Betroffene Abteilungen von IT
4.	Personenbezogene Daten, die in der Verwaltung von Audi Hungaria Zrt stehen, dürfen nur im Rahmen der dienstlichen Tätigkeiten verarbeitet und genutzt werden. Eine Übermittlung dieser Daten an unbefugte Dritte (z. B. Kunden, Partnerfirmenmitarbeiter, Mitarbeiter) ist nicht zulässig. IT-Geräte und Datenträger, auf denen personenbezogene, vertrauliche oder geheime Daten gespeichert sind, dürfen das Werksgelände der Audi Hungaria grundsätzlich nur verschlüsselt verlassen.
5.	Unternehmenskommunikation und Regierungsbeziehungen
6.	Personenbezogene, vertrauliche und geheime Papierdokumente sind in den Datenschutzcontainern zu entsorgen. Nicht mehr benötigte Datenträger sind zuverlässig durch Überschreiben zu löschen oder physikalisch zu zerstören.
7.	Sicherheitspolitik und Datenschutz

8.	IT Sicherheit: it-sicherheit@audi.hu
9.	IT Sicherheit: it-sicherheit@audi.hu

Informationstechnik (IT)-Sicherheitshandlungsleitlinien für Systembetreiber und Administratoren

Audi Hungaria

Version: 4.0 (11.05.2018)
Herausgeber: IT Sicherheit
Regelung Nr.: Übergeordnete Regelung 10

Geltungsbereich

Die Handlungsleitlinien gelten für Partnerfirmen (im Folgenden „Dienstleister" genannt), die Dienstleistungen für die AUDI HUNGARIA Zrt. (im Folgenden „ AUDI HUNGARIA" oder „Auftraggeber" genannt) erbringen.

Inhalt

1. Ziel

Die für die Nutzung von Informationen und IT-Geräten (z. B. Personalcomputer, Workstations einschließlich mobiler Rechner wie Notebooks, Smartphones, Tablet-PCs) zu beachtenden IT-Sicherheitsregelungen für Systembetreiber und Administratoren sind in diesen IT-Sicherheitshandlungsleitlinien definiert. Für den Schutz von Speicherprogrammierbaren Steuerungen (SPS) und Robotersteuerungen gelten innerhalb dieser Handlungsleitlinien ausschließlich die Regelungen im Anhang, Ziff. [1].

Die IT-Sicherheitshandlungsleitlinien dienen dem Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Nachweisbarkeit von Informationen sowie der Wahrung der Rechte und Interessen des Auftraggebers und aller natürlichen und juristischen Personen, die mit AUDI HUNGARIA Zrt. in geschäftlicher Beziehung stehen bzw. für diese arbeiten.

2. Regelungen

2.1 Organisation der Informationssicherheit

Die technische Anbindung einer Partnerfirma an das Konzernnetzwerk darf erst nach unterschriebener Vertraulichkeitsvereinbarung (siehe Anhang, Ziff. [3]) und dem Nachweis eines angemessenen Sicherheitsniveaus (z.B. gem. Self Assessment basierend auf dem Information Security Assessment" (ISA) des Verbandes der Automobilindustrie (VDA)) erfolgen.

2.2 Management von organisationseigenen Werten

Betriebsnotwendige IT-Systeme (siehe Anhang, Ziff. [4]) sind in einem Verzeichnis zu erfassen. Die Betriebsverantwortung für ein IT-System ist einer Organisationseinheit oder einer Person zuzuordnen.

Als betriebsnotwendig sind IT-Systeme einzustufen, deren Funktionsstörung den Fortbestand des Unternehmens ernsthaft gefährden könnte oder deren Wiederherstellung bzw. Wiederbeschaffung einen hohen Zeitaufwand und/oder hohe Kosten erfordern würde.

Dieses Verzeichnis der erfassten IT-Systeme hat mindestens die folgenden Angaben zu enthalten:

- Beschreibung der IT-Systeme einschließlich ihrer Schnittstellen zu anderen IT-Systemen,
- Verantwortliche Stelle oder Person,
- Zuordnung der IT-Systeme zu den Geschäftsprozessen,
- Betriebsstandort (z. B. Rechenzentrum),
- Geschäftsprozesszugehörigkeit,
- Klassifizierung der Daten und ggf. Hinweise auf besondere Schutzerfordernisse und -maßnahmen,
- Vorhandensein personenbezogener Daten,
- Informationseigentümer.

Die Verantwortung für Informationen hat der jeweilige Informationseigentümer. Dies gilt auch dann, wenn die Informationen über IT-Systeme bereitgestellt werden. Eine Delegation von einzelnen Aufgaben ist jedoch möglich.

2.3 Physische und umgebungsbezogene Sicherheit

Betriebsnotwendige IT-Systeme sind gegen Auswirkungen von Stromausfall zu schützen (z. B. durch unterbrechungsfreie Stromversorgung).

Versorgungsleitungen für Strom und Telekommunikation, welche Daten transportieren oder Informationssysteme versorgen, sind durch geeignete Maßnahmen (z. B. kontrollierter Zugang zu Verteilerräumen) vor Abhören und Beschädigung zu schützen.

Der Betreiber hat u. a. durch Wartung der Geräte sicherzustellen, dass die Verfügbarkeit von Daten gewährleistet ist, z.B.:

- Wartung von Geräten entsprechend der Herstellervorgaben
- Betrieb der Geräte in Übereinstimmung mit den vom Hersteller angegebenen Betriebs-parametern (Temperatur-,/Feuchtigkeitskontrolle, etc.)

Schutz der Geräte vor unbefugtem Zugriff, bzw. Manipulation und Beschädigung und vor schädlichen Umwelteinflüssen (Feuer-/Wasser-/Verschmutzungsschäden).

2.4Betriebs- und Kommunikationsmanagement

2.4.1 Verfahren und Verantwortlichkeiten

2.4.1.1 Dokumentierte Betriebsprozesse

Anweisungen, die für den Betrieb eines IT-Systems zu berücksichtigen sind, sind vom Betreiber zu erstellen und aktuell zu halten, z. B. in Form von Betriebshandbüchern, Funktions- oder Wartungsbeschreibungen. Bei Veröffentlichungen ist darauf zu achten, dass unberechtigten Dritten keine sicherheitsrelevanten Fakten (z. B. Firewallkonfiguration) bekannt gemacht werden. Die Dokumentation ist gemäß gesellschaftsspezifischer Regelungen (siehe Anhang, Ziff. [5]) zu archivieren. Der Systembetreiber muss sich an vorgegebene Betriebs-prozesse halten (z.B. Change-Prozess).

2.4.1.2 Änderungsverwaltung

Änderungen an produktiven IT-Systemen müssen über ein definiertes Verfahren geplant, getestet, genehmigt und dokumentiert werden, bevor sie im produktiven Betrieb umgesetzt werden.

Änderungsanträge (change requests) sind schriftlich zu dokumentieren (z. B. Änderungen an IT-Systemen durch den Informationseigentümer, Änderungen an der Infrastruktur oder an Anlagen durch den Betreiber) und von der verantwortlichen Stelle zu genehmigen.

Die Auswirkungen der geplanten Änderungen sind grundsätzlich an einem Testsystem zu untersuchen. Der Einsatz eines Testsystems ist in Abwägung des potentiellen Risikos mit dem dafür erforderlichen Aufwand zu planen. Im Notfall kann vom Betreiber ein beschleunigtes Verfahren im IT-Notfallplan (siehe Abschnitt "Sicherstellung des Geschäftsbetriebs (Business Continuity Management)") definiert werden. Dabei ist sicherzustellen, dass durch die Änderungen keine Sicherheitsmaßnahmen unterlaufen werden.

Das Sicherheitsniveau muss während und nach der Änderung erhalten bleiben. Wenn Risiken nicht ausgeschlossen werden können, hat die Planung auch eine Rückfalllösung vorzusehen und Kriterien vorzugeben, wann diese zum Tragen kommen soll.

Änderungen am IT-System sind zu protokollieren. Bei einer fehlgeschlagenen Änderung ist das IT-System möglichst in den ursprünglichen Zustand zu versetzen. Vor einer neuen Durchführung ist die Ursache festzustellen.

Alle von den Änderungen betroffenen Personen sind rechtzeitig zu informieren.

2.4.1.3 Aufteilung von Verantwortlichkeiten

Ausführende (z. B. Programmierung, Entwicklung) und kontrollierende (z. B. Audit, Abnahme) Tätigkeiten sind personell voneinander zu trennen bzw. im Einzelfall organisatorisch zu regeln.

Zudem sind Tätigkeiten dann zu trennen, wenn ohne eine Trennung ein erhöhtes Risiko einer willentlichen oder unwissentlichen Fehlhandhabung zu Lasten des Konzerns besteht („Mehr-Augen-Prinzip“).

Vor der Einführung von Software sind die Verantwortlichkeiten zu regeln (z. B. für die Erstellung von Pflichtenheften, die Produktvorauswahl, das Testen, das Freigeben, die Installation und den Betrieb).

2.4.1.4 Trennung von Entwicklungs-, Test- und Produktiveinrichtungen

Entwicklungs- und Testumgebungen sowie produktive IT-Systeme sind voneinander zu trennen. Eine Ausnahme bilden Anlagen im Produktionsumfeld, für die dies einen unverhältnismäßigen Aufwand bedeutet.

Entwicklung und Test von Software ist nur in der dafür vorgesehenen Entwicklungs-, bzw. Testumgebung zulässig. Dabei ist sicherzustellen, dass der produktive Betrieb nicht in Mitleidenschaft gezogen wird.

Für Tests sind sofern möglich Testdaten zu erzeugen (z. B. mittels eines Testdatengenerators).

Personenbezogene, vertrauliche oder geheime Daten sind vor der Übernahme von produktiven IT-Systemen in die Testsysteme so zu verfälschen, dass ein Rückschluss auf die Original-Daten nicht mehr möglich ist, sofern auf diese Daten Personen Zugriff erhalten, die diese nicht für die Erfüllung ihrer vertragsgegenständlichen Arbeiten benötigen.

Das Kopieren oder die Nutzung von Informationen aus laufenden IT-Systemen ist nur nach vorheriger Genehmigung durch den Informationseigentümer zulässig. Die kopierten Daten unterliegen den gleichen IT-Sicherheitsanforderungen wie die Original-Daten.

Benutzte Informationen aus laufenden IT-Systemen sind nach Durchführung der Tests zu löschen.

Zugriffsberechtigungen, die für laufende IT-Systeme gelten, müssen auch für Testanwendungen beachtet werden.

2.4.2 Management der Dienstleistungserbringung von Dritten

IT-sicherheitsbezogene Tätigkeiten sind grundsätzlich durch internes Personal zu erbringen. Falls dies nicht möglich ist, sind begleitende Kontrollmaßnahmen der Tätigkeiten der externen Dienstleister vorzusehen.

Bei Outsourcing oder Outtasking von administrativen und operativen Tätigkeiten sind begleitende Kontrollmaßnahmen der Tätigkeiten der externen Dienstleister vorzusehen.

2.4.3 Systemplanung und Abnahme

Die Kapazitätsanforderungen an ein IT-System sind während der Planung festzulegen.

Die Sicherheitsanforderungen an ein IT-System sind mit den Informationseigentümern während der Planung zu definieren und zu dokumentieren. Die Einführung eines neues Systems beinhaltet eine dokumentierte und abgenommene Betriebsübernahme durch die Systembetreiber.

Die Systemplanung (Fachkonzeption, Systemdesign, Systemrealisierung) und -abnahme (Systemeinführung) ist nach gültigen Systementwicklungsstandards der Audi Hungaria (Portfoliorunde-AA-1.7-G/FP-1-003) durchzuführen.

2.4.4 Schutz vor Schadsoftware und mobilem Programmcode

IT-Geräte, die von Schadsoftware befallen sind, sind unter Berücksichtigung möglicher Auswirkungen (z. B. Produktionsstillstand) vom Netzwerk zu trennen.

IT-Geräte und IT-Systeme sind gegen Angriffe und/oder Schadsoftware zu schützen, z.B. mittels einer von den zuständigen Stellen freigegebenen Virenschutzsoftware (siehe Anhang, Ziff. [6]) . Die entsprechenden Virensignaturen sind regelmäßig zu aktualisieren.

2.4.5 Backup

Alle Verantwortlichen für IT-Systeme haben sicherzustellen, dass eine ausreichende Sicherung der Daten für eine angemessene Wiederherstellbarkeit der Informationen erfolgt.

Sicherungsverfahren sind zu planen, umzusetzen, zu testen, zu überwachen und zu dokumentieren.

Sicherungsdatenträger unterliegen den gleichen Sicherheitsanforderungen wie die Original-Daten (z. B. Schutz gegen Diebstahl und unbefugten Zugriff). Sie sind getrennt vom IT-System in einem separaten Brandabschnitt aufzubewahren. In Abhängigkeit des Schutzbedarfes ist eine externe Sicherung an einem anderen Standort vorzusehen.

Während der Dauer der Aufbewahrung der Daten ist eine Lesbarkeit und Nutzbarkeit der Informationen sicherzustellen.

Bei der Archivierung von Daten sind firmeninterne und gesetzliche Aufbewahrungsfristen einzuhalten (siehe Anhang, Ziff. [5]). Die Lesbarkeit von archivierten Datenträgern ist in angemessenen Zeitabständen zu überprüfen.

Die Wiederherstellung von gesicherten Daten ist regelmäßig auf Funktionsfähigkeit zu testen.

2.4.6 Management der Netzsicherheit

Unmittelbar nach der Installation einer Netzwerkkomponente (z. B. Router) sind vorhandene systemspezifische Schutzmechanismen (z. B. Passwortschutz) zu aktivieren. Sämtliche aktive Netzwerkkomponenten sind durch ein geeignetes Managementsystem zentral zu überwachen, um Fehlerzustände oder das Eintreten kritischer Ereignisse frühzeitig zu erkennen.

2.4.7 Elektronische Mitteilungen/Nachrichten (Messaging)

Der Systemverantwortliche ist für die Zuverlässigkeit von Kommunikationsdiensten (z. B. E-Mail) verantwortlich. Bei den E-Maildiensten ist folgendes zu beachten:

- Es muss nachvollziehbar sein, welche Person eine eMail versandt hat.
- Systembezogene E-Mails müssen einer verantwortlichen Personen zugeordnet werden können.
- Postfächer sind gegen Zugriffe Unbefugter zu schützen.

2.4.8 Öffentlich verfügbare Informationen

Öffentlich zugängliche IT-Systeme dürfen nur über sichere Netzübergangskomponenten Zugang zu internen Netzen haben.

Informationen, die über öffentlich zugängliche IT-Systeme bereitgestellt werden, sind durch geeignete Sicherheitsmaßnahmen (z. B. verschlüsselte Übertragung der Authentisierungsinformationen) vor unbefugter Veränderung zu schützen.

2.4.9 Überwachung

2.4.9.1 Auditprotokolle

Die Zugriffe der Benutzer auf IT-Systeme mit geheimen Informationen sind zu protokollieren. Die Protokolle sind entsprechend der betrieblichen Regelungen aufzubewahren.

Die Protokolle haben mindestens Folgendes zu enthalten:

eine eindeutige Identifikation der protokollierten Person (z. B. Name oder Kennung),

Aufzeichnungen von Systemzugriffsversuchen,

Aufzeichnungen von Zugriffen auf Daten und auf andere Ressourcen.

2.4.9.2 Überwachung der Systemnutzung

Protokollauswertungen haben regelmäßig im Rahmen von Audits und bei Verdacht auf IT-Sicherheitsvorfälle zu erfolgen.

Bei der Auswertung von Audit-/Aktivitätsprotokollen sind die notwendigen Genehmigungs-verfahren einzuhalten (siehe Anhang, Ziff. [7]).

2.4.9.3 Schutz von Protokollinformationen

Protokolle sind so zu speichern, dass die protokollierten Personen keinen ändernden oder löschenden Zugriff auf die Protokolldaten haben. Protokolle dürfen nicht manipuliert oder deaktiviert werden. Systemadministratoren dürfen das Aufzeichnen nicht unbemerkt deaktivieren können.

Sollten die Protokolle selbst geheime Informationen enthalten (z.B. bei Aufzeichnung der Daten vor und nach Veränderung, Übertragene Daten, etc.), so muss gewährleistet sein, dass die Protokolle lediglich von Personen eingesehen oder ausgewertet werden können, die über die erforderliche Authorisierung des Informationseigentümers verfügen.

2.4.9.4 Administrator- und Betreiberprotokolle

Die Tätigkeiten der Systembetreiber an IT-Systemen mit vertraulichen und/oder geheimen Informationen sind zu protokollieren.

Die Tätigkeiten der Systembetreiber zumindest an IT-Systemen mit geheimen Informationen sind so abzulegen, dass die protokollierten Personen mit erweiterten Rechten keinen ändernden oder löschenden Zugriff auf die Protokolldaten haben.

Die Protokolle haben mindestens Folgendes zu enthalten:

- eine eindeutige Identifikation der protokollierten Person (z. B. Name oder Kennung),
- Beginn und Beendigung der Tätigkeit am IT-System,
- Grund der Tätigkeit (z.B. Systemfehler, Change, Update),
- durchgeführte Maßnahmen.

2.4.9.5 Fehlerprotokolle

Von Benutzern gemeldete Fehler und Fehlfunktionen sind zu protokollieren. Die vom Betreiber veranlassten Maßnahmen zur Fehlerbehebung sind zu dokumentieren.

2.4.9.6 Zeitsynchronisation

Informationssysteme, mit denen Protokolldaten erhoben werden, müssen mittels einer genau vereinbarten Referenzzeit synchronisiert sein.

2.5 Zugangskontrolle

2.5.1 Geschäftsanforderungen für Zugangskontrolle

Für den Zugriff auf Informationen sind in Abhängigkeit von der Risikobewertung des Informationseigentümers Mechanismen zur Authentisierung und Autorisierung einzurichten. Dabei ist das vom Informationseigentümer festgelegte Rollen- und Rechtekonzept umzusetzen.

Die Beantragung einer Zugangs-/Zugriffsberechtigung für ein IT-System hat schriftlich mit dem Benutzerantrag oder über ein zu diesem Zweck freigegebenes IT-System zu erfolgen, der sowohl vom OE-Leiter als auch vom Informationseigentümer zu genehmigen ist. Alle Personen, die zur Benutzung eines Systems oder einer Applikation berechtigt sind, sind formal zu erfassen.

Für die Einrichtung einer Zugangs-/Zugriffsberechtigung ist die Genehmigung des Leiters der Organisationseinheit und des jeweiligen Informationseigentümers, mit Ausnahme zentraler Dienste (z.B. Intranet), erforderlich ("Mehr-Augen-Prinzip"). Eine Delegation der jeweiligen Genehmigung ist möglich.

Benutzerkennungen sind immer einer Person zuzuordnen.

Für Wartungszugänge genutzte Medien zur Identifizierung (z. B. Smartcards, SecurID-Karten) dürfen nur unter Einhaltung folgender Maßnahmen weitergegeben werden:

- Die Weitergabe ist durch eine verantwortliche Person zu dokumentieren. Diese hat dafür zu sorgen, dass ein schriftlicher Nachweis geführt wird, wer wann die Medien an wen weitergegeben hat.
- Für die Aufbewahrung der Dokumentation gilt dieselbe Frist wie für die Aufbewahrung von Benutzeranträgen.
- Es sind Verfahren für die Vergabe und die Rücksetzung von Passwörtern festzulegen und zu veröffentlichen.

2.5.2 Benutzerverwaltung

Administratorkennungen dürfen nur zu administrativen Aufgaben genutzt werden. Routinetätigkeiten, die kein Administrationsrecht erfordern, sind mit Benutzerkennungen mit eingeschränkten Rechten durchzuführen.

Für die Vergabe von Passwörtern und Medien zur Identifizierung (z. B. Smartcards, SecurID-Karten) sind Verfahren festzulegen und zu veröffentlichen.

Standardpasswörter der Hersteller sind unmittelbar nach der Installation von Systemen oder Software entsprechend den geltenden Passwortrichtlinien zu ändern.

Für die regelmäßige Überprüfung von Benutzerberechtigungen sind diese dem Leiter einer Organisationseinheit für seinen Zuständigkeitsbereich zur Verfügung zu stellen.

Für Mitarbeiter von Partnerfirmen sind Benutzerberechtigungen für die Dauer des Auftrages in den Systemen, soweit technisch möglich, zeitlich zu befristen (maximal ein Jahr).

Die folgenden Mindestforderungen bei der Passwortfestlegung sind zu beachten (dieser Absatz gilt nicht für PINs):

- Ein Passwortwechsel ist vom System grundsätzlich bei der Erstnutzung und dann mindestens alle 90 Tage zu erzwingen.
- Einem Ausprobieren von Benutzerkennungen und Passwörtern ist durch geeignete Maßnahmen zu begegnen (z. B. Verlängerung der Wartezeit nach jedem Fehlversuch und/oder eine Sperrung nach einer definierten Anzahl von Fehlversuchen).

- Bei der Authentisierung an Systemen, in denen vertrauliche oder geheime Daten gespeichert sind, sind Passwörter grundsätzlich sicher verschlüsselt zu übertragen. Falls dies nicht möglich ist, sind Einmalpasswörter zu verwenden.

Die folgenden Mindestforderungen beim Umgang mit Passwörtern sind zu beachten:

- Benutzerkennungen, die mehr als 400 Tage nicht genutzt wurden, sind zu sperren.
- Passwörter, die in Systemen voreingestellt sind, müssen durch individuelle Passwörter ersetzt werden.
- Eine Speicherung von Passwörtern in Dateien ist nur sicher verschlüsselt zulässig.
- Soweit technisch möglich, sind nach 5 Fehlversuchen der Account zu sperren, eine Passworthistorie von mindestens 5 Passwörtern und die Mindestanforderung an die Komplexität im jeweiligen System zu erzwingen.
- Jeder Benutzer muss sein Passwort grundsätzlich jederzeit ändern können.
- Bei der Eingabe darf das Passwort nicht im Klartext am Bildschirm angezeigt werden.

2.5.3 Benutzerverantwortung

Für administrative Benutzerkennungen, die personenbezogen zur Verwaltung von IT-Systemen auf der Basis von umfassenden Zugriffsrechten genutzt werden, ist für Passwörter eine mindestens 15-stellige Kombination aus mindestens 3 der folgenden 4 Kriterien zu verwenden:

- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen

Für Systembezogene Benutzerkennungen, welche zur automatisierten Anmeldung und Verarbeitung von einem System genutzt werden, ist für Passwörter eine mindestens 16-stellige Kombination aus mindestens 3 der folgenden 4 Kriterien zu verwenden:

- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen

Das Passwort muss dabei mindestens einmal jährlich geändert werden. Die Verfügbarkeit der Passwörter der systembezogenen Benutzerkennungen ist durch den Systemverantwortlichen sicherzustellen (z. B. durch Passworthinterlegung). Können die geforderten Einstellungen in einem System nicht vorgenommen werden, gelten die Vorgaben für Passwortlänge und Änderungsintervall.

2.5.4 Zugangskontrolle für Netze

Nur authentisierte und autorisierte Benutzer dürfen Zugang zum internen Konzernnetzwerk erhalten.

Der Remotezugang ins interne Konzernnetzwerk (Intranet) ist mittels "Wissen und Besitz" zu schützen (z. B. PKI-Karte: dort ist "Wissen" die Kenntnis der PIN-Nummer und "Besitz" das Besitzen der Karte als solches). Die Datenübertragung ist mit einer sicheren Verschlüsselung zu schützen.

Im Netzwerk sind geeignete Maßnahmen zur Identifikation von Endgeräten zu ergreifen.

Nicht benötigte Dienste und Ports sind abzuschalten.

Basierend auf einer Risikobetrachtung ist eine Netzwerksegmentierung vorzunehmen und die zulässigen Kommunikationsbeziehungen festzulegen.

Netzwerke unterschiedlichen Schutzbedarfs sind an den Übergängen durch geeignete Netzwerksicherheitskomponenten (z. B. Intrusion Prevention System, Firewall) zu schützen.

2.5.5 Zugriffskontrolle auf Betriebssysteme

2.5.5.1 Verfahren für sichere Anmeldung

Der Zugriff auf IT-Systeme mit nicht öffentlichen Daten ist durch geeignete Verfahren (z.B. Authentisierung) auf die Nutzung durch befugte Anwender zu beschränken.

Pflicht der Systemverantwortlichen ist es, ein richtlinienkonformes, sicheres Anmeldeverfahren (z.B. starke Authentisierung mittels PKI-Karte) umzusetzen.

Einem Ausprobieren von Benutzerkennungen und Passwörtern ist durch geeignete Maßnahmen zu begegnen (z. B. Verlängerung der Wartezeit nach jedem Fehlversuch und/oder eine Sperrung nach einer definierten Anzahl von Fehlversuchen).

2.5.5.2 Benutzeridentifikation und Authentisierung

Administrative Tätigkeiten sind, soweit technisch möglich, stark zu authentisieren (2-Faktor-Authentisierung mittels Wissen und Besitz). Sofern dies technisch nicht möglich ist, sind alternative Schutzmechanismen (z.B. längeres Passwort) einzusetzen und mit den zuständigen Stellen abzustimmen (siehe Anhang, Ziff. [8]. Bei der Passwortvergabe/-änderung ist zu überprüfen, ob Passwörter gemäß den Passwortregelungen gebildet werden.

2.5.5.3 Systeme zur Verwaltung von Passwörtern

Die Systemverantwortlichen haben die Mindestforderungen bei der Passwortfestlegung (siehe "IT-Sicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter- ÜR-08") durch entsprechende Systemumsetzungen zu unterstützen.

Passwörter sind mindestens vertraulich klassifiziert und entsprechend zu behandeln, es sei denn der Eigentümer der Informationen, auf die hiermit zugegriffen werden kann, hat eine andere Einstufung in Richtung geheim vorgenommen. Es besteht erhöhter Schutzbedarf bei Passwörtern (Identitätsdiebstahl), daher ist eine Ablageverschlüsselung notwendig.

2.5.5.4 Verwendung von Systemwerkzeugen

Eine unautorisierte Veränderung von sicherheitsrelevanten System- und Anwendungseinstellungen, z. B. mit Hilfe von Systemwerkzeugen, ist mittels geeigneter Maßnahmen (z. B. Entzug von entsprechenden Rechten) zu unterbinden.

2.5.5.5 Session Time-out

Dialogsitzungen, die über einen längeren Zeitraum nicht mehr aktiv benutzt werden, sind zu deaktivieren oder durch geeignete Maßnahmen zu schützen.

2.5.6 Mobile Computing und Telearbeit

Ein vom Unternehmen bereitgestelltes IT-Gerät darf nur dann und nur solange mit unternehmensfremden Netzwerken (z. B. Hot Spot, privates WLAN) verbunden werden, wenn dies zum Verbindungsaufbau mit dem Konzernnetzwerk geschieht.

2.6 Beschaffung, Entwicklung und Wartung von Informationssystemen

2.6.1 Sicherheitsanforderungen von Informationssystemen

Vor Entwicklung und Einsatz von IT-Systemen sind die erforderlichen IT-Sicherheitsmaßnahmen zu identifizieren und umzusetzen.

Die Regelungen zum Umgang mit Informationen gelten auch für IT-Systeme (z. B. für Datenbanken, Backupmedien).

2.6.1.1 Schutz der Vertraulichkeit

Informationen müssen entsprechend ihrer Einstufung vor einem unberechtigten Zugriff geschützt werden. Aus der Einstufung bezüglich der Vertraulichkeit sind hierfür folgende Schutzmaßnahmen abzuleiten:

Einstufung	Definition
Öffentlich	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches)
Intern	Maßnahmen für "Öffentlich" plus: • Zugriffsschutz gemäß "Kenntnis, nur wenn nötig" • 1-Faktor-Authentisierung (z. B. User-ID und Passwort)
Vertraulich	Maßnahmen für "Intern" plus: • 2-Faktor-Authentisierung (z. B. Smartcard mit PIN) -insbesondere bei Zugriff auf Applikationen- oder eine weitere Absicherung wie zusätzlich authentisierte Ablageverschlüsselung (z. B. verschlüsselte Datei auf dem Fileshare, verschlüsselter USB-Stick) • Transportverschlüsselung
Geheim	Maßnahmen für "Vertraulich" plus: • 2-Faktor-Authentisierung (z. B. Smartcard mit PIN) -insbesondere bei Zugriff auf Applikationen • Transportverschlüsselung • Ablageverschlüsselung

2.6.1.2 Schutz der Integrität

Informationen müssen entsprechend ihrer Einstufung vor ungewollter Veränderung oder unberechtigter Manipulation geschützt werden. Aus der Einstufung bezüglich der Integrität sind hierfür folgende Schutzmaßnahmen abzuleiten:

Einstufung	Definition
Gering	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches)
Mittel	Maßnahmen für "Gering" plus: • Zugriffsschutz gemäß "Kenntnis, nur wenn nötig"

	• 1-Faktor-Authentisierung (z. B. User-ID und Passwort)
Hoch	Maßnahmen für "Mittel" plus: • Überprüfung von Eingabe- und Ausgabedaten sowie Kontrolle der internen Verarbeitung zur Fehlerreduktion und Vermeidung von Standardangriffen wie Buffer-Overflows und Einschleusen von ausführbahrem Code (z. B. Feldgrenzen-Überprüfung, Beschränkung von Feldern auf spezielle Bereiche)
Sehr hoch	Maßnahmen für "Hoch" plus: • 2-Faktor-Authentisierung (z. B. Smartcard mit PIN) für ändernde Zugriffe • Bildung und Überprüfung von digitalen Signaturen für abgelegte Daten oder vergleichbare Schutzmechanismen

2.6.1.3 Schutz der Nachweisbarkeit

Die Nachweisbarkeit von Zugriffen auf und Veränderungen an Informationen muss entsprechend ihrer Einstufung sichergestellt werden. Aus der Einstufung bezüglich der Nachweisbarkeit sind hierfür folgende Schutzmaßnahmen abzuleiten:

Einstufung	Definition
Gering	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches) • Standardsystemprotokollierung von aufgetretenen Fehlern, Anmeldeversuchen, etc.
Mittel	Maßnahmen für "Gering" plus: • Protokollierung von User-ID, Systemzeit und Art der Änderung (Hinzufügen, Löschen, Ändern) bei ändernden Zugriffen • 1-Faktor-Authentisierung (z. B. User-ID und Passwort) für ändernde Zugriffe
Hoch	Maßnahmen für "Mittel" plus: • Protokollierung von User-ID, Systemzeit und Änderung bei ändernden Zugriffen, in einer Weise, die den Stand vor Änderung erkennen lässt
Sehr hoch	Maßnahmen für "Hoch" plus: • Protokollierung von User-ID und Systemzeit für lesende Zugriffe • 2-Faktor-Authentisierung (z. B. Smartcard mit PIN) für lesende und ändernde Zugriffe

2.6.1.4 Schutz der Verfügbarkeit

Die Verfügbarkeit von IT-Systemen muss entsprechend ihrer Einstufung sichergestellt werden. Aus der Einstufung bezüglich der Verfügbarkeit sind hierfür folgende Schutzmaßnahmen abzuleiten:

Einstufung	Definition
Gering	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches) • Die Ausfallzeit darf mehr als 72 Stunden betragen. Dafür sind erforderliche Maßnahmen zu implementieren.
Mittel	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches) • Die Ausfallzeit darf maximal 72 Stunden betragen. Dafür sind erforderliche Maßnahmen zu implementieren.
Hoch	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches) • Die Ausfallzeit darf maximal 24 Stunden betragen. Dafür sind erforderliche Maßnahmen zu implementieren.
Sehr hoch	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches) • Die Ausfallzeit darf maximal 1 Stunde betragen. Dafür sind erforderliche Maßnahmen zu implementieren.

2.6.2 Kryptographische Maßnahmen

Kryptographische Schlüssel sind gegen Modifikation und Zerstörung zu schützen. Sofern Schlüssel Unbefugten bekannt geworden sind, sind sie auszutauschen. Der Kreis der Personen, die Zugriff auf die Schlüssel haben, ist möglichst klein zu halten und ist in einem Verzeichnis festzuhalten. Es ist sicherzustellen, dass benutzte Schlüssel mindestens so lange aufbewahrt werden, wie die mit ihrer Hilfe verschlüsselten oder signierten Dateien archiviert werden, soweit dies nicht durch ein zentrales Schlüsselmanagement (z. B. PKI) gewährleistet wird. Wenn Schlüsselmaterial nicht mehr verwendet wird, ist es nach einem sicheren Verfahren zu vernichten.

2.6.3 Sicherheit von Systemdateien

2.6.3.1 Kontrolle von Software im Betrieb

Die Installation von Software darf nur von autorisierten Personen (siehe Anhang, Ziff. [9]) durchgeführt werden.

Neue oder geänderte Programme für Produktivsysteme dürfen nur nach erfolgreichen Tests sowie nach Freigabe durch Informationseigentümer und Systembetreiber eingesetzt werden. Die Versions-/Korrekturstände der eingesetzten Software sind zu dokumentieren und gemäß gesellschaftsspezifischer Regelungen (siehe Anhang, Ziff. [10]) zu archivieren.

2.6.3.2 Zugangskontrolle zu Quellcode

Programmquellcode ist hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Nachweisbarkeit zu klassifizieren und entsprechend zu schützen.

2.6.4 Sicherheit bei Entwicklungs- und Unterstützungsprozessen

Die Sicherheit von Anwendungen darf durch den Einsatz von Administrationswerkzeugen und -protokollen nicht gefährdet werden.

Vor der Installation neuer Softwareversionen oder Patches ist durch Tests sicherzustellen, dass weder der Betrieb noch die Sicherheit durch die Änderungen gefährdet sind.

Bei Änderungen sind die betroffenen Beschreibungen der Benutzerverfahren und der Betriebsdokumentation anzupassen.

Wenn Änderungen an Softwarepaketen durchgeführt werden, sind die Auswirkungen auf bestehende Regelungen, Verträge und Sicherheitsmaßnahmen zu klären. Änderungen dürfen nur erfolgen, wenn dies lizenzrechtlich und aufgrund der Wartungsverträge zulässig ist.

2.6.5 Umgang mit Schwachstellen

Sicherheitsupdates und –patches sind in Abwägung der potentiellen Risiken zeitnah nach Ihrer Veröffentlichung zu testen und einzuspielen.

2.7 Sicherstellung des Geschäftsbetriebs (Business Continuity Management)

Unvorhergesehene oder unerwartete Ereignisse, die einen Ausfall von IT-Systemen über eine nicht tolerierbare Zeit und einen Schaden für Geschäftsprozesse zur Folge haben, werden im Folgenden einheitlich als IT-Notfall bezeichnet.

Zur Aufrechterhaltung des kontinuierlichen Geschäftsbetriebs sind Maßnahmen zu etablieren, um kritische IT-Geschäftsprozesse zu identifizieren und zu bewerten.

Es sind vorsorgliche Maßnahmen zu ergreifen, damit unerwartete Ereignisse (z. B. Ausfälle) keine IT-Notfälle zur Folge haben. Ferner sind Maßnahmen zu bestimmen, die bei Eintritt von IT-Notfällen durchzuführen sind.

Die Maßnahmen müssen sich an den Anforderungen der Geschäftsprozesse orientieren. Mit Hilfe von Risikoanalysen sind mögliche Schadensfälle bezüglich der Eintrittswahrscheinlichkeit und der Schadenshöhe zu bewerten. Dabei sind alle Geschäftsprozesse zu betrachten und nicht ausschließlich auf informationsverarbeitende Einrichtungen zu beschränken. Zusätzlich ist auch eine Business Impact Analyse durchzuführen.

Die maximal zu akzeptierenden Ausfallzeiten und der maximal zulässige Datenverlust von geschäftskritischen informationsverarbeitenden IT-Systemen sind zu definieren und zu dokumentieren.

Es sind IT-Notfallpläne zu entwickeln, die definieren, wann ein IT-Notfall eingetreten ist und das Vorgehen im IT-Notfall regeln. Sie haben in komprimierter Form alle entscheidungsrelevanten Angaben zu enthalten, um im IT-Notfall die notwendigen Schritte einzuleiten. Dabei sind auch die Maßnahmen zu beschreiben, die bei einem Übergang von einem Not- in einen Regelbetrieb erforderlich sind. Die Maßnahmen sind nachvollziehbar zu beschreiben.

Mit Hilfe der IT-Notfallpläne muss schnell entschieden werden können, welche Maßnahmen durch welche Verantwortliche in welcher Reihenfolge durchzuführen sind.

Die für IT-Notfallmaßnahmen verantwortlichen Mitarbeiter sowie ihre Vertreter sind namentlich und als Funktion in den IT-Notfallplänen anzugeben und ihre Erreichbarkeit ist sicherzustellen. Alle Personen, die über den IT-Notfall zu informieren sind, sind festzulegen.

IT-Notfallpläne sind in die Notfallpläne der Geschäftsprozesseigentümer zu integrieren.

Die Sicherstellung des kontinuierlichen Geschäftsbetriebes ist mit folgenden Maßnahmen und Techniken regelmäßig (jährlich) zu überprüfen, sofern das IT-System als geschäftskritisch identifiziert wurde:

- Planspiele von IT-Notfallszenarien,
- Simulationen zur Schulung des Personals auf ihre Rollen im Krisenmanagement,
- Technische Tests zur Wiederherstellung von Informationssystemen,
- Test der Wiederherstellung des Betriebs,
- Prüfen der Vertragserfüllung von externen Dienstleistern,
- regelmäßige IT-Notfallübungen,
- IT-Notfallpläne sind aktuell zu halten.

2.8 Einhaltung von Vorgaben

Beim Einsatz von Verschlüsselung und/oder von elektronischen Signaturen (siehe Anhang, Ziff. [11]) insbesondere über Ländergrenzen hinweg sind die länderspezifischen Regelungen für den Import/Export/Zugriff von bzw. auf Hardware/Software/Informationen zu beachten.

Bei Fragen zu den länderspezifischen Regelungen sind die zuständigen Stellen (siehe Anhang, Ziff. [12]) zu kontaktieren.

Jeder Betreiber von IT-Systemen hat seine IT-Systeme stichprobenartig auf die Einhaltung der sicherheitsrelevanten Vorschriften und Richtlinien zu überprüfen und zu dokumentieren.

Mechanismen und Tools zur Systemüberwachung (z. B. die Auditfunktion der Betriebssysteme) sind einzurichten und zu nutzen. Dafür vorgeschriebene Genehmigungsverfahren sind zu beachten (siehe Anhang, Ziff. [7]).

Die Betreiber von IT-Systemen sind verpflichtet, bekannt gewordene Sicherheitslücken der IT-Systeme durch geeignete Maßnahmen zu schließen.

Das uneingeschränkte Prüfungsrecht der internen Revision ist hiervon nicht betroffen.

Auditanforderungen/-aktivitäten sind sorgfältig zu planen (insbesondere für Produktivsysteme), um das Risiko von Störungen der Geschäftsprozesse zu minimieren.

Folgende Punkte sind zu beachten:

- Der Anwendungsbereich der Prüfungen ist zu vereinbaren und zu kontrollieren.
- Die Prüfungen sind auf nur lesenden Zugriff für Software und Daten zu begrenzen.
- IT-Ressourcen sind für die Prüfungen zu identifizieren und verfügbar zu machen.
- Sämtliche Verfahren, Anforderungen und Zuständigkeiten sind zu dokumentieren.

Um einen Missbrauch oder die Kompromittierung des Audittools zu verhindern, darf der Zugriff auf Systemauditools nur für autorisiertes Personal möglich sein.

2.9 Verantwortlichkeiten

Abweichungen von diesen Handlungsleitlinien, die das Sicherheitsniveau senken, sind nur in Abstimmung mit den zuständigen Stellen (siehe Anhang 3, Ziff. 8.) und nur zeitlich begrenzt zulässig.

3. Weiterführende Dokumentation, Anlagen

Dokument	Beschreibung
Ziff. 1.	Speicherprogrammierbare Steuerungen (SPS) und Robotersteuerungen sind in verschließbaren Schränken aufzubewahren oder durch entsprechende anderweitige geeignete Maßnahmen zu sichern. Der Zugang ist nur Berechtigten zu ermöglichen. Speicherprogrammierbare Steuerungen (SPS) und Robotersteuerungen sind in Netzen zu betreiben, in denen nur die Kommunikation erlaubt ist, die für den Betrieb unbedingt erforderlich ist
Ziff. 2.	Die Bekanntgabe von Informationen hinsichtlich Änderungen bzw. Aktualisierungen erfolgen ausschließlich über das Audi Hungaria mynet
Ziff. 3.	Die dafür relevanten Dokumente und Informationen sind im mynet: OE Rechtsservice und Compliance Seite
Ziff. 4.	Ein IT-System ist ein Gesamtsystem bestehend aus sämtlichen Hardware- und Software-Komponenten inklusive deren Kommunikationsbeziehungen untereinander.
Ziff. 5.	Die Dokumentation ist gemäß Richtlinie Nr. 022 des Vorstands der AUDI HUNGARIA Zrt. - Aufbewahrung von Unterlagen zu archivieren
Ziff. 6.	Die Freigabe von Virenschutzsoftware erfolgt durch das Viren Competence Center (VCC).
Ziff. 7.	Personenbezogene Audits sind schriftlich vom Datenschutzgremium genehmigen zu lassen. Die Einbindung der zuständigen Personalleitung und des Betriebsrats ist sicherzustellen.
Ziff. 8.	Verantwortlichkeit: Organisationseinheit (OE) IT-Sicherheit
Ziff. 9.	Verantwortlichkeit: Mitarbeiterinnen und Mitarbeiter, die aufgrund ihrer definierten Aufgabenstellung, Installationsrechte genehmigt erhalten haben, z. B.IT Infrastruktur und Office Services team, Keyuser
Ziff. 10.	Die Versions-/Korrekturstände sind gemäß Nr. 022 des Vorstands der AUDI HUNGARIA Zrt. - Aufbewahrung von Unterlagen zu archivieren.
Ziff. 11.	Nationale Gesetze zur Anerkennung der elektronischen Signatur: In Ungarn gilt das elektronische Signaturgesetz. Hier sind die nationalen gesetzlichen Rahmenbedingungen für den Einsatz elektronischer Signaturen beschrieben. Das an die EU-Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vom 13.12.1999 [ECRL99/93/EK] angepasste Gesetz über Rahmenbedingungen für

	elektronische Signaturen und zur Änderung weiterer Vorschriften [SigG01] ist am 12.06.2001 in Kraft getreten und löst das Signaturgesetz von 1997 ab. Das Gesetz soll Rahmenbedingungen schaffen, bei deren Einhaltung eine qualifizierte elektronische Signatur als mindestens gleichwertig sicher zu einer eigenhändigen Unterschrift angesehen werden kann. Es enthält Festlegungen darüber, wann qualifizierte elektronische Signaturen nach dem Signaturgesetz der handschriftlichen Unterschrift gleichgestellt sind. Im Ergebnis wird digitalen Signaturen nach dem Signaturgesetz auch vor Gericht eine hohe Sicherheit zugebilligt
Ziff. 12.	Verantwortlichkeit: OE Rechtsservice und Compliance.

IT Sicherheitshandlungsleitlinien für Systementwickler

Version: 4.0 (11.05.2018)
Herausgeber: IT Sicherheit
Regelung Nr.: Übergeordnete Regelung 10

Geltungsbereich

Die Handlungsleitlinien gelten für Partnerfirmen (im Folgenden „Dienstleister" genannt), die Dienstleistungen für die AUDI HUNGARIA Zrt. (im Folgenden „ AUDI HUNGARIA" oder „Auftraggeber" genannt) erbringen.

Inhalt

1. Ziel

Die für die Nutzung von Informationen und IT-Geräten (z. B. Personalcomputer, Workstations einschließlich mobiler Rechner wie Notebooks, Smartphones, Tablet-PCs) zu beachtenden IT-Sicherheitsregelungen für Systementwickler sind in dieser Arbeitsanweisung definiert.

Die IT-Sicherheitshandlungsleitlinien dienen dem Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Nachweisbarkeit von Informationen sowie der Wahrung der Rechte und Interessen des Auftraggebers und aller natürlichen und juristischen Personen, die mit AUDI HUNGARIA Zrt. in geschäftlicher Beziehung stehen bzw. für diese arbeiten.

2. Regelungen

2.1Management von organisationseigenen Werten

Die Verantwortung für Informationen hat der jeweilige Informationseigentümer. Dies gilt auch

dann, wenn die Informationen über IT-Systeme bereitgestellt werden. Eine Delegation von einzelnen Aufgaben ist jedoch möglich.

2.2Betriebs- und Kommunikationsmanagement

IT-sicherheitsbezogene Tätigkeiten sind grundsätzlich durch internes Personal zu erbringen. Falls dies nicht möglich ist, sind begleitende Kontrollmaßnahmen der Tätigkeiten der externen Dienstleister vorzusehen.

- Die Kapazitätsanforderungen an ein IT-System sind während der Planung festzulegen.
- Die Sicherheitsanforderungen an ein IT-System sind mit den Informationseigentümern während der Planung zu definieren und zu dokumentieren.
- Die Systemplanung (Fachkonzeption, Systemdesign, Systemrealisierung) und Abnahme (Systemeinführung) ist nach gültigen Systementwicklungsstandards des Konzerns (z. B. Systementwicklungsprozess (SEP)) durchzuführen.
- Informationen, die über öffentlich zugängliche IT-Systeme bereitgestellt werden, sind durch geeignete Sicherheitsmaßnahmen (z.B. verschlüsselte Übertragung der Authentisierungsinformationen) vor unbefugter Veränderung zu schützen.

2.3Zugangskontrolle

Für den Zugriff auf Informationen sind in Abhängigkeit von der Risikobewertung des Informationseigentümers Mechanismen zur Authentisierung und Autorisierung einzurichten. Dabei ist das vom Informationseigentümer festgelegte Rollen- und Rechtekonzept umzusetzen. Pflicht der Systemverantwortlichen ist es, ein richtlinienkonformes, sicheres Anmeldeverfahren (z.B. starke Authentisierung mittels PKI-Karte) umzusetzen.

Einem Ausprobieren von Benutzerkennungen und Passwörtern ist durch geeignete Maßnahmen zu begegnen (z. B. Verlängerung der Wartezeit nach jedem Fehlversuch und/oder eine Sperrung nach einer definierten Anzahl von Fehlversuchen).

Die Systemverantwortlichen haben die Mindestforderungen bei der Passwortfestlegung durch entsprechende Systemumsetzungen zu unterstützen.

Passwörter sind mindestens vertraulich klassifiziert und entsprechend zu behandeln, es sei denn der Eigentümer der Informationen, auf die hiermit zugegriffen werden kann, hat eine andere Einstufung in Richtung geheim vorgenommen. Es besteht erhöhter Schutzbedarf bei Passwörtern (Identitätsdiebstahl), daher ist eine Ablageverschlüsselung notwendig.

Dialogsitzungen, die über einem längeren Zeitraum nicht mehr aktiv benutzt werden, sind zu deaktivieren oder durch geeignete Maßnahmen zu schützen.

2.4 Beschaffung, Entwicklung und Wartung von Informationssystemen

2.4.1 Sicherheitsanforderungen von Informationssystemen

Vor Entwicklung und Einsatz von IT-Systemen sind die erforderlichen IT-Sicherheitsmaßnahmen (z. B. Systemhärtung, Patchmanagement) zu identifizieren und umzusetzen.

Die Regelungen zum Umgang mit Informationen gelten auch für IT-Systeme (z. B. für Datenbanken, Backupmedien).

2.4.1.1 Schutz der Vertraulichkeit

Informationen müssen entsprechend ihrer Einstufung vor einem unberechtigten Zugriff geschützt werden. Aus der Einstufung bezüglich der Vertraulichkeit sind hierfür folgende Schutzmaßnahmen abzuleiten:

Einstufung	Definition
Öffentlich	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches)
Intern	Maßnahmen für "Öffentlich" plus:

	• Zugriffsschutz gemäß "Kenntnis, nur wenn nötig" • 1-Faktor-Authentisierung (z. B. User-ID und Passwort)
Vertraulich	Maßnahmen für "Intern" plus: • 2-Faktor-Authentisierung (z. B. Smartcard mit PIN) - insbesondere bei Zugriff auf Applikationen- oder eine weitere Absicherung wie zusätzlich authentisierte Ablageverschlüsselung (z. B. verschlüsselte Datei auf dem Fileshare, verschlüsselter USB-Stick) • Transportverschlüsselung
Geheim	Maßnahmen für "Vertraulich" plus: • 2-Faktor-Authentisierung (z. B. Smartcard mit PIN) - insbesondere bei Zugriff auf Applikationen • Transportverschlüsselung • Ablageverschlüsselung

2.4.1.2 Schutz der Integrität

Informationen müssen entsprechend ihrer Einstufung vor ungewollter Veränderung oder unberechtigter Manipulation geschützt werden. Aus der Einstufung bezüglich der Integrität sind hierfür folgende Schutzmaßnahmen abzuleiten:

Einstufung	Definition
Gering	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches)
Mittel	Maßnahmen für " Gering" plus: • Zugriffsschutz gemäß "Kenntnis, nur wenn nötig" • 1-Faktor-Authentisierung (z. B. User-ID und Passwort)
Hoch	Maßnahmen für " Mittel" plus: • Überprüfung von Eingabe- und Ausgabedaten sowie Kontrolle der internen Verarbeitung zur Fehlerreduktion und Vermeidung von Standardangriffen wie Buffer-Overflows und Einschleusen von ausführbarem Code (z. B. Feldgrenzen-Überprüfung, Beschränkung von Feldern auf spezielle Bereiche)
Sehr hoch	Maßnahmen für "Hoch" plus : • 2-Faktor-Authentisierung (z. B. Smartcard mit PIN) für ändernde Zugriffe

	• Bildung und Überprüfung von digitalen Signaturen für abgelegte Daten oder vergleichbare Schutzmechanismen

2.4.1.3 Schutz der Nachweisbarkeit

Die Nachweisbarkeit von Zugriffen auf und Veränderungen an Informationen muss entsprechend ihrer Einstufung sichergestellt werden. Aus der Einstufung bezüglich der Nachweisbarkeit sind hierfür folgende Schutzmaßnahmen abzuleiten:

Einstufung	Definition
Gering	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches) • Standardsystemprotokollierung von aufgetretenen Fehlern, Anmeldeversuchen, etc.
Mittel	Maßnahmen für "Gering" plus: • Protokollierung von User-ID, Systemzeit und Art der Änderung (Hinzufügen, Löschen, Ändern) bei ändernden Zugriffen • 1-Faktor-Authentisierung (z. B. User-ID und Passwort) für ändernde Zugriffe
Hoch	Maßnahmen für "Mittel" plus: • Protokollierung von User-ID, Systemzeit und Änderung bei ändernden Zugriffen, in einer Weise, die den Stand vor Änderung erkennen lässt
Sehr hoch	Maßnahmen für "Hoch" plus: • Protokollierung von User-ID und Systemzeit für lesende ugriffe • 2-Faktor-Authentisierung (z. B. Smartcard mit PIN) für lesende und ändernde Zugriffe

2.4.1.4 Schutz der Verfügbarkeit

Die Verfügbarkeit von IT-Systemen muss entsprechend ihrer Einstufung sichergestellt werden. Aus der Einstufung bezüglich der Verfügbarkeit sind hierfür folgende Schutzmaßnahmen abzuleiten:

Einstufung	Definition
Gering	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches) • Die Ausfallzeit darf mehr als 72 Stunden betragen. Dafür sind erforderliche Maßnahmen zu implementieren.

Mittel	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches) • Die Ausfallzeit darf maximal 72 Stunden betragen. Dafür sind erforderliche Maßnahmen zu implementieren.
Hoch	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches) • Die Ausfallzeit darf maximal 24 Stunden betragen. Dafür sind erforderliche Maßnahmen zu implementieren.
Sehr hoch	• Systemhärtung (nur benötigte Dienste, aktuelle Sicherheitspatches) • Die Ausfallzeit darf maximal 1 Stunde betragen. Dafür sind erforderliche Maßnahmen zu implementieren.

2.4.2 Korrekte Verarbeitung in Anwendungen

Die Sicherheit von IT-Systemen ist durch die Umsetzung der Maßnahmen, die gültige Systementwicklungsstandards des Konzerns (z. B. SEP) fordern, zu gewährleisten.

Bezüglich der Beratung bei der Einführung von IT-Systemen gelten die Regelungen und Betriebsvereinbarungen der jeweiligen Konzerngesellschaft (siehe Anhang, Ziff. [1]).

2.4.3 Kryptographische Maßnahmen

Grundsatzentscheidungen über Strategie, Einsatz und Handhabung kryptographischer Maßnahmen sind durch die zuständigen Stellen (siehe Anhang, Ziff. [2]) zu treffen.

Beim Einsatz von Verschlüsselungsprodukten ist das "Book of Standards" zu berücksichtigen.

Beim Einsatz anwendungsspezifischer Verschlüsselungssoftware müssen geeignete Tools zur Umschlüsselung bereitgestellt werden.

Zertifikate haben eine zeitlich begrenzte Gültigkeit. Vor Ablauf der Gültigkeit eines Signaturzertifikats (Schlüsselverwendung "content commitment" bzw. "non repudiation") müssen damit signierte Daten mit einem länger gültigen Schlüssel übersigniert werden.

2.4.4 Sicherheit von Systemdateien

2.4.4.1 Schutz von Test-Daten

Entwicklungs- und Testumgebungen sowie produktive IT Systeme, mit Ausnahme von Anlagen, sind voneinander zu trennen.

Für Tests sind sofern möglich Testdaten zu erzeugen (z. B. mittels eines Testdatengenerators).

Der Test von Software ist nur in der dafür vorgesehenen Testumgebung zulässig. Dabei ist sicherzustellen, dass der produktive Betrieb nicht in Mitleidenschaft gezogen wird.

Personenbezogene, vertrauliche oder geheime Daten sind vor der Übernahme von produktiven IT-Systemen in die Testsysteme so zu verfälschen, dass ein Rückschluss auf die Original-Daten nicht mehr möglich ist, sofern auf diese Daten Personen Zugriff erhalten, die diese nicht für die Erfüllung ihrer vertragsgegenständlichen Arbeiten benötigen.

Das Kopieren oder die Nutzung von Informationen aus laufenden IT-Systemen ist nur nach vorheriger Genehmigung durch den Informationseigentümer zulässig. Die kopierten Daten unterliegen den gleichen IT-Sicherheitsanforderungen wie die Original-Daten.

Benutzte Informationen aus laufenden IT-Systemen sind nach Durchführung der Tests zu löschen.

Zugriffsberechtigungen, die für laufende IT-Systeme gelten, müssen auch für Testanwendungen beachtet werden.

2.4.4.2 Zugangskontrolle zu Quellcode

Programmquellcode ist zu klassifizieren und entsprechend zu schützen.

2.4.5 Sicherheit bei Entwicklungs- und Unterstützungsprozessen

Alle Abläufe und Vorgänge, die IT-Systeme berühren, sind so zu gestalten, dass das jeweils angestrebte IT-Sicherheitsniveau ganzheitlich erreicht und beibehalten wird.

Formale Änderungskontrollverfahren (Change Management) sind durchzuführen. Sie müssen sicherstellen, dass Sicherheit und Überwachungsverfahren der IT-Systeme nicht durch Änderungen kompromittiert werden.

Wenn Änderungen an gekauften Softwarepaketen durchgeführt werden, sind die Auswirkungen auf bestehende Regelungen und Sicherheitsmaßnahmen zu klären. Änderungen dürfen nur erfolgen, wenn dies lizenzrechtlich und aufgrund der Wartungsverträge zulässig ist.

2.5 Einhaltung von Vorgaben

Beim Einsatz von Verschlüsselung und/oder von elektronischen Signaturen. insbesondere über Ländergrenzen hinweg sind die länderspezifischen Regelungen für den Import/Export/Zugriff von bzw. auf Hardware/Software/Informationen zu beachten.

Bei Fragen zu den länderspezifischen Regelungen sind die zuständigen Stellen (siehe Anhang, Ziff. [3]) zu kontaktieren.

2.6 Verantwortlichkeiten

Abweichungen von diesen Handlungsleitlinien, die das Sicherheitsniveau senken, sind nur in Abstimmung mit den zuständigen Stellen (siehe Anhang 3, Ziff. 2.) und nur zeitlich begrenzt zulässig.

3. Weiterführende Dokumentation, Anlagen

Dokument	Beschreibung
Ziff. 1	IT-Systeme, die mitbestimmungspflichtige Tatbestände beinhalten, sind in den BR-EDV-Ausschüssen zu beraten.
Ziff. 2	IT Sicherheit Bereich
Ziff. 3	Rechtswesen Bereich
Ziff. 4	AH Datenschutz Gremium