Informationssicherheitsrichtlinie für Lieferanten und Dienstleister

Änderungen

Datum	*Version*	*Autor*	*Beschreibung*
02.11.2020	001	CDI	Einführung Dokument
05.09.2023	002	CDI	Review und Aktualisierung ABT SE

Inhaltsverzeichnis

1. Einleitung

Dieses Dokument beschreibt unsere Informationssicherheitsphilosophie und die von uns angestrebten Ziele. Wo möglich, verzichten wir auf technische Details und das genaue Vorgehen. Das Dokument soll einen Gesamtüberblick ermöglichen – detaillierte Informationen sind im Bedarfsfall direkt mit der QM-Abteilung zu klären.
Alle Anforderungen gelten für die ABT SE, die ABT Sportsline GmbH, die ABT e-Line GmbH (zur Vereinfachung wird in allen weiteren Dokumenten von der „ABT-Gruppe“ gesprochen) sowie deren Dienstleister oder Partner. Ausnahmen sind, eigene interne Dokumente der jeweiligen Firmen. Die Anforderungen dieses Dokumentes stellen wir vor allem an uns selber und erwarten dies auch in der Zusammenarbeit von unseren Partnern

1.1. Stellenwert der Informationssicherheit im Unternehmen

Unser Unternehmen ist auf IT-gestützte Prozesse im Unternehmen angewiesen. In dieser Situation ist es unerlässlich, Informationssicherheit zu gewährleisten um die nötige Zuverlässigkeit im geschäftlichen Alltag zu schaffen. Informationssicherheit ist integraler Bestandteil aller Geschäftsprozesse in der ABT-Gruppe und hat wesentlichen Einfluss auf die Qualität, sowie die Effizienz und Wirtschaftlichkeit der Arbeitsergebnisse des Unternehmens. Wir verstehen Informationssicherheit als unerlässlichen Kundenservice, der die Vertraulichkeit von Informationen schützt und die Verfügbarkeit unserer Prozesse gewährleistet.
Wir leben eine aktive Sicherheitskultur und fördern Informationssicherheit indem alle Mitarbeiter eingebunden, regelmäßig geschult und sensibilisiert werden. Der Mitarbeiter steht bei uns im Mittelpunkt der aktiven Sicherheitskultur.

1.2. Schutzziele

Das ISMS der ABT-Gruppe dient dem Schutz vor Gefahren, Bedrohungen und den damit verbundenen Schäden. Ziel ist es, in allen Kategorien Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Verbindlichkeit mit angemessenen Maßnahmen das Schutzziel „HOCH“ zu erreichen.
Die Ziele von Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Verbindlichkeit) können in verschiedenen Bereichen und Phasen eines Geschäftsprozesses durch die Bedarfsträger (z. B. „Informationseigentümer“) unterschiedlich priorisiert werden. Die Priorisierung wird entweder innerhalb von IT-Sicherheitskonzepten im Rahmen einer Risikobetrachtung vorgenommen und dokumentiert oder durch generelle Anforderungen (z. B. aus Gesetzen, Verordnungen und Verwaltungsvorschriften) festgelegt. Sie muss bei Bedarf im Rahmen von Revision und Audit entsprechend der aktuellen Sicherheitslage oder aufgrund anderer veränderlicher Bedürfnisse revisionssicher angepasst werden.
Die Priorisierung der Sicherheitsziele orientiert sich dabei an den bei einem IT-Sicherheitsvorfall zu erwartenden Schäden bei einem bestimmten Schadenszenario.
So kann z. B. bei einem Geschäftsprozess zu einem bestimmten Zeitpunkt die Vertraulichkeit von Informationen zum Schutz von Leib und Leben vor dem Ziel der Verfügbarkeit stehen, d. h. ein Fachverfahren wird nicht schnellstmöglich wieder in Betrieb gesetzt.
Im gleichen Geschäftsprozess bei einer anderen Sachlage oder in einem anderen Geschäftsprozess kann die Verfügbarkeit höher priorisiert werden als die Vertraulichkeit, um einen hohen finanziellen Schaden zu vermeiden, d. h. das betreffende Fachverfahren wird trotz zeitweisem Verlust der Vertraulichkeit schnellstmöglich mindestens in einen Notbetrieb überführt.

1.2.1. Schutz der Vertraulichkeit

In Abhängigkeit vom jeweiligen Schutzbedarf der Vertraulichkeit von Informationen sind angemessene organisatorische und technische Maßnahmen zu ergreifen und aufrecht zu erhalten. Eine Verletzung des für den Schutz der Vertraulichkeit jeweils definierten Schutzbedarfes ist durch entsprechende Maßnahmen zu unterbinden.
Dieses muss bei der längerfristigen Speicherung und revisionssicheren Vernichtung von Informationen, bei Aufbau und Anpassung der Infrastruktur der Informationsverarbeitung, bei der Nutzung von Informationen auf IT-Systemen, der Übertragung insbesondere über Datennetze außerhalb eigener Infrastrukturen und dem Transport mit mobilen Medien oder Systemen innerhalb und außerhalb des Geltungsbereiches dieser Richtlinie geschehen. Die gewählten Vorgehensweisen sind regelmäßig einer genauen Prüfung zu unterziehen und an die technologische Entwicklung sowie die Gefährdungslage anzupassen.
Der Zugriff auf Informationen ist unter besonderer Berücksichtigung des Rechtes auf informationelle Selbstbestimmung (Datenschutz) auf den mit ihrer Verarbeitung beauftragten Personenkreis zu beschränken ("need-to-know" Prinzip). Grundlage hierfür ist die Schutzbedarfsfeststellung.
Im Sinne einer Prävention sind Maßnahmen zur zentralen und dezentralen Schadsoftware- (z. B. Viren, Würmer, Trojaner, Rootkits) und Einbruchserkennung („Hacker“) flächendeckend zu etablieren. Der Nachweis der ordnungsgemäßen Funktion der gewählten Mechanismen muss möglich sein und erbracht werden.

1.2.2. Schutz der Integrität

Die Integrität von Informationen ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen.
In Abhängigkeit vom Schutzbedarf der Integrität von Informationen ist über eine angemessene Vorgehensweise zu entscheiden. Dieses muss bei der längerfristigen Speicherung von Informationen, bei Aufbau und Anpassung der Infrastruktur der Informationsverarbeitung, bei der Nutzung von Informationen auf IT-Systemen, bei der Übertragung über Datennetze und dem Transport mit mobilen Medien oder Systemen innerhalb und außerhalb des Geltungsbereichs dieser Richtlinie geschehen. Die gewählten Vorgehensweisen sind regelmäßig zu überprüfen und an die technologische Entwicklung sowie die Gefährdungslage anzupassen.
Die unbefugte Veränderung von Informationen ist durch den Einsatz entsprechender Mittel zu verhindern. Sicherung vor Schadsoftware und Einbruchserkennung sind hierbei wichtige, jedoch nicht ausschließliche Mechanismen. Der Nachweis der ordnungsgemäßen Funktion der gewählten Mechanismen muss möglich sein und mindestens stichprobenartig erbracht werden.

1.2.3. Schutz der Verfügbarkeit

Die Verfügbarkeit von Informationen ist gemäß ihres Schutzbedarfes durch geeignete technische und organisatorische Maßnahmen sicherzustellen.
In Abhängigkeit der erforderlichen Verfügbarkeit von Informationen ist über eine angemessene Vorgehensweise zu entscheiden. Dieses muss bei der längerfristigen Speicherung und vor der Vernichtung von Informationen, bei Aufbau und Anpassung der Infrastruktur zur Informationsverarbeitung, bei der Nutzung von Informationen auf IT-Systemen, der Übertragung über Datennetze und dem Transport mit mobilen Medien oder Systemen innerhalb und außerhalb des Geltungsbereichs dieser Richtlinie geschehen. Die gewählten Vorgehensweisen sind regelmäßig zu überprüfen und an die technologische Entwicklung sowie die Gefährdungslage anzupassen.
Durch den Einsatz entsprechender Sicherheitseinrichtungen ist eine Verminderung der Verfügbarkeit der IT und der verarbeiteten Informationen zu verhindern. Redundante IT-Infrastruktur, Datensicherung, Archivierung sowie die Absicherung gegen Schadsoftware und unbefugtes Eindringen in IT-Systeme und -Netze sind hierbei wichtige, jedoch nicht ausschließliche Mechanismen. Der Nachweis der Funktion der gewählten Mechanismen muss möglich sein und erbracht werden.

Im Interesse der Gesamtverfügbarkeit dürfen Teile der IT vom IT-Betrieb ausgeschlossen werden, wenn die IT-Sicherheitslage dieses erfordert. Dies gilt insbesondere auch für Systeme mit Informationen, deren Schutzbedarf größer als "*hoch*" eingestuft ist.

1.2.4. Gewährleistung der Authentizität

Die Authentizität von Informationen ist gemäß ihres Schutzbedarfes durch geeignete technische und organisatorische Maßnahmen sicherzustellen.
Hierzu muss die Echtheit von Informationen und ihrer Urheberschaft anhand charakteristischer Merkmale überprüfbar sein. Diese Überprüfung muss durch geeignete technische und organisatorische Maßnahmen vorgenommen werden. Ihre Anwendung und Einhaltung sind bei allen Schritten der Verarbeitung der Informationen ungeachtet der verwendeten Systeme, Kommunikationswege oder Übertragungsmedien einzuhalten. Der Nachweis der ordnungsgemäßen Funktion der gewählten Mechanismen muss möglich sein und erbracht werden.

1.2.5. Gewährleistung der Verbindlichkeit

Die Verbindlichkeit der Verarbeitung von Informationen muss in den Geschäftsprozessen bei allen Arbeitsschritten gewährleistet sein. Die Verarbeitungsvorgänge müssen hinsichtlich ihres Ablaufs nachvollziehbar und überprüfbar (revisionsfähig) sein. Hierbei ist das übergeordnete Ziel der Rechtsverbindlichkeit der Informationsverarbeitung einzuhalten.
Für Informationen mit "sehr hohem" Schutzbedarf müssen angemessene Maßnahmen zum Nachweis der Identität der Verarbeitung mit den vom Verarbeiter absichtlich vorgenommenen Aktionen ergriffen werden (z. B. Änderungshistorie). Die rechtlichen Rahmenbedingungen unter besonderer Berücksichtigung des Datenschutzes sind dabei besonders zu beachten.
Die verwendeten Verfahren zur Absicherung sind soweit wie möglich zu automatisieren, der Zugriff auf die gewonnenen Informationen ist besonders zu begrenzen.

2. Informationssicherheitsmanagement

2.1. ISMS

Die ABT-Gruppe betreibt zur Erreichung der selbst gesteckten Sicherheitsziele ein ISMS auf Basis der ISO 27001 und des VDA-ISA Katalogs (TISAX). Lieferanten die nicht nach der Vorgabe zertifiziert sind verpflichten sich die Anforderungen entsprechend der Normen zu beachten und nach besten Möglichkeiten umzusetzen. Ziel beider Parteien ist die Abwicklung nach den vorgegebenen Standards.

2.2. Fortlaufende Verbesserung

- Das ISMS wird regelmäßig auf Aktualität und Wirksamkeit überprüft. Hierzu gehören regelmäßige Audits und die Wirksamkeitsüberprüfung von Maßnahmen.
- Alle Mitarbeiter sind dazu verpflichtet, die Vorgaben zu beachten
- Das Unternehmen muss Wert darauf legen, technisch aktuelle Maßnahmen einzusetzen.
- Das Unternehmen fördert und propagiert das ISMS
- Alle Abweichungen werden im Detail analysiert, um Verbesserungen zu erarbeiten.
- Alle Mitarbeiter sind in das ISMS in einem dem Maße eingebunden, dass Sie Fehler oder Verbesserungsmaßnahmen melden können.

2.3. Verantwortlichkeiten

Um das ISMS fachgerecht zu betreuen, soll eine zentrale Stelle mit der Verantwortung betraut werden. Der zentrale Ansprechpartner (Informations-Sicherheits-Beauftragter – ISB) ist zu benennen und der ABT - Gruppe (Abteilung HSEQ) zu melden.

- Anforderungen
    - Die benannte Person besitzt zur Wahrnehmung seiner Aufgabe eine hervorgehobene organisatorische Rolle, in der er direkt an die Unternehmensleitung berichtet.
    - Die Person verfügt über angemessenes Wissen und Qualifikationen im Bereich Informationssicherheit.
    - Die Verantwortung für das Thema Informationssicherheit wird schriftlich berufen.

Alle Mitarbeiter die in das Projekt eingebunden sind, sind dazu angehalten den ISB zu unterstützen. Dazu gehört:

- **Geschäftsführung**:
  - Bereitstellung der nötigen Ressourcen für das ISMS
  - Unterstützung des ISB bei der Kommunikation gegenüber anderen Mitarbeitern
  - Förderung der fortlaufenden Verbesserung
  - Festlegung und Kommunikation der Informationssicherheitsziele gemeinsam mit dem ISB
- **Führungskräfte**
  - Leben einer Vorbildrolle, um Informationssicherheit gegenüber Mitarbeitern förderlich zu kommunizieren
  - Weiterleiten von Verbesserungsvorschlägen an den ISB
  - Einbeziehen des ISB bei Veränderungen im Betriebsablauf, die die Informationssicherheit betreffen
- **IT-Leiter**
  - Besonders enge Zusammenarbeit mit dem ISB zur Erreichung der Sicherheitsziele
  - Unterstützung des ISB mit Ressourcen zur Umsetzung der Sicherheitsziele
- **Datenschutzbeauftragter**
  - Bezieht den ISB bei Änderungen, die die Informationssicherheit betreffen, mit ein
  - Stimmt Sicherheitsmaßnahmen wo möglich mit dem ISB ab
- **Alle Mitarbeiter**
  - Melden von Informationssicherheitsvorfällen und Unregelmäßigkeiten
  - Einhalten der vorgeschriebenen Richtlinien

2.4. Risikomanagement

Zur Identifikation von Risiken innerhalb des ISMS wird ein Risikomanagementsystem durch den ISB betrieben. Das Risikomanagement dient zur Identifikation und Bewertung von Risiken. Der ISB ist verpflichtet, bei Risiken, die vorher definierte Schwellwerte überschreiten, Gegenmaßnahmen einzuleiten.

3. Maßnahmen und Anforderungen

3.1. Zugang zu Informationen und Systemen

Ziel: Steuerung und Einschränkung des Zugangs zu System und Informationen.

Die Verantwortlichkeiten für Informationssicherheit sind innerhalb der Organisation und relevanten Geschäftspartnern bekannt und für ihre Aufgaben qualifiziert.
Innerhalb der Organisation wird einem Informationssicherheitskonzept gefolgt, über welches alle Mitarbeiter informiert sind. Verantwortlich für die Umsetzung in den einzelnen Bereichen sind die jeweiligen Bereichsleiter. Notwendige Ressourcen zur Gewährleitung der Informationssicherheit sind ermittelt und werden den Mitarbeitern zur Verfügung gestellt.

3.1.1. Zugänge

- Die Vergabe von Rechten erfolgt, wenn möglich, in Bezug auf die organisatorische Rolle wie z.B. Bereichsleiter, Abteilungsleiter, etc., um eine konsistente Rechtevergabe zu ermöglichen.
- Erteilte Rechte werden dokumentiert und regelmäßig kontrolliert.
- Privilegierte Rechte werden nach besonders sorgfältiger Prüfung erteilt und ebenfalls regelmäßig auf Notwendigkeit überprüft.

3.1.2. Passwörter und Anmeldedaten

Alle Zugänge zu Systemen und Informationen werden mit personalisierten Anmeldedaten geschützt. Es ist die Erstellung sicherer Passwörter und die Nutzung eines Passwortmanagers für Zugänge zu fördern, die nicht über Singe-Sign-on (SSO) bereitgestellt werden können.

3.2. Personalsicherheit

Ziel: Vor, während und nach Beschäftigung sind sicherheitsrelevante Anforderungen an die Beschäftigung sichergestellt.

Es besteht eine Verpflichtung zur Geheimhaltung und Vertraulichkeit, welchen jeder Mitarbeiter mit Unterzeichnen seines Arbeitsvertrages zustimmt oder gesondert unterschreibt. Diese Verpflichtungen reichen über das Arbeitsverhältnis hinaus.
Außerdem verpflichten sich Mitarbeiter die mit dem Projekt vertraut sind dazu, die Richtlinien zur Informationssicherheit einzuhalten.
Verantwortlichkeiten und Pflichten für den Umgang mit sensiblen Informationen sind vertraglich festgelegt.
Eine Vorgehensweise bei Verstößen gegen vertragliche Inhalte mit Informationssicherheitsrelevanz ist im Vertrag beschrieben und somit jedem Mitarbeiter bekannt.

3.2.1. Sensibilisierung und Schulung

Um Mitarbeiter in die Belange der Informationssicherheit einzubinden und zu sensibilisieren sind Schulungen von Mitarbeitern durchzuführen. Dazu gehört:

- Regelmäßige (mindestens jährliche) Schulungen
- Zielgruppenorientierte Ausrichtung der Schulungen
- Bereitstellen von nötigen Informationen an einer zentralen Stelle in leicht verständlicher Form
- Neue Mitarbeiter werden über sämtliche Richtlinien zur Informationssicherheit und über die Risiken beim Umgang mit Information und deren Verarbeitung geschult und sensibilisiert

3.3. Lieferantenbeziehungen

Ziel: Lieferantenbeziehungen gewährleisten das gleiche Informationssicherheitsniveau wie bei internen Vorgängen.

Auftragnehmer, die folgende Bedingungen erfüllen:

- Verarbeitung sensibler Informationen
- Wartung, Bereitstellung oder Entwicklung sensibler IT-Systeme oder Dienste
- Zutrittsberechtigung zu Räumen, in denen sensible Informationen verarbeitet werden

Unterliegen unter anderem folgende Bedingungen:

- Vertragsbedingungen und Produkte werden im Sinne der Sicherheitsanforderungen geprüft.
- Je nach Tätigkeit wird der Lieferant auf eine Geheimhaltungsvereinbarung bzw. Sicherheitsrichtlinie verpflichtet.
- Der Lieferant kann regelmäßig auf die Einhaltung von getroffenen Vereinbarungen überprüft werden.
- Das Unternehmen unterstützt den Lieferanten bei der Umsetzung und Einhaltung der Sicherheitsmaßnahmen.

3.4. Handhaben von Informationen

Ziel: Informationswerte sind über Ihren kompletten Lebenszyklus hinweg angemessen geschützt.

Verantwortlichkeiten für die Informationssicherheit in der Organisation sind definiert, dokumentiert und zugewiesen. Die verantwortlichen Mitarbeiter sind entsprechend für ihre Aufgabe qualifiziert. Ansprechpartner sind innerhalb der Organisation und relevanten Geschäftspartnern bekannt

- Das Unternehmen führt ein Assetinventar (Werteinventar), das aus einer übergeordneten Sichtweise relevante Informationswerte des Unternehmens klassifiziert.

- Informationen und Dokumente werden klassifiziert, um die Geheimhaltungsstufe sichtbar zu machen und den angemessenen Umgang zu ermöglichen. Informationen werden in folgendem System klassifiziert:
  - Öffentlich
    - Zugang zu diesen Informationen beeinträchtigt das Unternehmen keinesfalls. Diese Informationen unterliegen keinerlei Restriktionen und werden z.B. vom Unternehmen in Zeitungen oder im Internet veröffentlicht. Die Verwendung von Unternehmensinformationen in der Öffentlichkeit bedarf der Zustimmung der Presse-Abteilung.
  - Intern
    - Zugang durch Dritte oder nicht vertrauenswürdige Vertragspartner kann einen geringen Schaden oder Ansehensverlust zur Folge haben. Dazu zählen alle Informationen, die nur für den internen Gebrauch und nicht für die Öffentlichkeit bestimmt sind.

  - Vertraulich
    - Zugang zu Informationen durch Dritte oder unberechtigte Mitarbeiter kann einen erheblichen Schaden zur Folge haben. Personenbezogene Daten (Stammdaten) sind – wenn nicht als geheim gekennzeichnet – immer vertraulich zu behandeln.
  - Geheim / Streng vertraulich
    - Zugang durch unbefugte und nicht berechtigte richtet einen unumkehrbaren Schaden an. Dazu zählen Informationen, deren Kenntnis durch Unbefugte oder deren missbräuchliche Weitergabe oder Verwendung das Erreichen von Unternehmensziele nachhaltig gefährden kann und die daher einem äußerst restriktiven Verteiler und strikten Kontrollen unterliegen müssen.

- Die Klassifizierungsstufe bestimmt ebenfalls den zulässigen Umgang (Verwendung) mit Dokumenten und Informationen über den Lebenszyklus hinweg.
- Informationen werden sicher vernichtet, um Einsicht durch Dritte zu verhindern. Näheres ist der zugehörigen Richtlinie zu entnehmen.

3.5. Definition der Verantwortlichkeiten zwischen IT und externen Dienstleistern

- IT-Dienste und Dienstleistungen sind identifiziert, dokumentiert und erfüllen alle relevanten Sicherheitsanforderungen. Regelmäßig durchgeführte Audits, sowie Schulungen gewährleisten eine Einhaltung der Vorgaben.
- Die Liste unserer IT-Dienstleister mit allen relevanten Informationen zu Dienstkonfigurationen, relevanten Nachweisen der Dienstleister, etc. sind über die Dokumente „Sicherheitsanforderungen an IT-Dienstleister“ und „Liste IT-Dienstleister“ abrufbar

3.6. Kommunikationssicherheit

Ziel: Unternehmensnetze und Kommunikationsnetze sind angemessen geschützt.

Unternehmensnetze und Kommunikationsnetze innerhalb der Organisation sind angemessen geschützt. Dafür sind verschiedene Maßnahmen, wie z.B. Zugangsbeschränkungen, Verschlüsselung von Netzwerkverbindungen und Firewall-Systeme etabliert. Diese Sicherheitsmaßnahmen werden regelmäßig und sorgfältig von geschultem Personal überprüft.

3.6.1. Zugangsbeschränkungen zu projektbezogenen Daten

- Alle Netzwerke werden im Zugang durch den Einsatz von Verfahren, die der Geräteautorisierung dienen, beschränkt, so dass nur unternehmensinterne Geräte Zugang zum Unternehmensnetzwerk erhalten.

3.6.2. Kryptografie

Alle externen Verbindungen werden kryptografisch gesichert. Hierzu gehört unter anderem:

- HTTPS-Datenverkehr für Web-Ressourcen bei externem Zugriff
- Wartungsverbindungen (SSH, RDP)
- Kabellose Netze (W-Lan mit WPA2)

Das Verschlüsselungskonzept bestimmt, dass sämtliche externe Verbindungen verschlüsselt werden.

3.7. Physische Sicherheit

Ziel: Steuerung und Einschränkung des Zutritts zu Räumlichkeiten. Erreichen eines Schutzes von schutzbedürftigen oder kritischen Informationen.

3.7.1. Zutrittssteuerung / Zugriffsrechte

- Die Vergabe von Zutrittsrechten erfolgt, wenn möglich, in Bezug auf die organisatorische Rolle im Projekt wie z.B. Projektleitung, Bereichsleitung, etc. um eine konsistente Rechtevergabe zu ermöglichen.
- Zutrittsrechte werden dokumentiert und regelmäßig überprüft.
- Sofern ein Mitarbeiter das Unternehmen verlässt oder sich sein Aufgabenbereich ändert, wird sichergestellt, dass die Zutrittsrechte entsprechend angepasst werden.

3.7.2. Sicherung von Infrastruktur und sensibler Bereiche

- Zentrale und sensible Infrastruktur wie z.B. der Serverraum wird besonders geschützt, so ist z.B. Zutritt für Gäste untersagt, ebenso Foto-, Video- und Tonaufnahmen.
- Der Zutritt zum Serverraum ist nur dem IT-Personal und weiteren, von der IT geschulten Personen möglich.
- Der Besuch durch Dritte in Sicherheitszonen wird dokumentiert und erfolgt begleitet durch einen befugten Mitarbeiter.
- Dieses Vorgehen ist auch auf weitere sensible Bereiche anzuwenden. Sicherheitsbereiche sind in den Bauplänen kenntlich gemacht (siehe Bauplan mit Sicherheitszonen).

- Zur Sicherung der Organisation wird der Außenbereich einschließlich Kundenparkplatz und Einfahrt, sowie der komplette Werkstattbereich inkl. Entwicklung, Karosserie videoüberwacht
- Außerdem wird täglich automatisch die Alarmanlage zwischen 21:30 bis 05:30 Uhr aktiviert
- Mehr Information zu weiteren Sicherheitsbereichen ist im Dokument „Richtlinie zur Arbeit in Sicherheitsbereichen“ hinterlegt.

3.7.3. Entsorgung von Geräten und Datenträgern (Punkt 8.1. – 8.4.)

- Alle Datenträger, Geräte und Dokumente, die interne oder vertrauliche Informationen haben, werden ordnungsgemäß vernichtet oder gelöscht, bevor diese entsorgt oder weiterverkauft werden oder in anderer Form den Kontrollbereich des Unternehmens verlassen (siehe Dokument ISMS_08.V02 Entsorgungsrichtlinie).
- Es obliegt der Verantwortung des Bereichs- oder Abteilungsleiters, die sachgemäße Löschung bzw. Vernichtung beim IT-Leiter zu beauftragen

3.7.4. Entsorgung von Akten und Dokumenten

Ziel: Kontrollierte Vernichtung von Akten und Dokumenten, die projektbezogene Daten und Informationen enthalten

- Alle Dokumente und Akten, die projektbezogene Daten (Firmen, Nahmen, technische Unterlagen, etc.) enthalten müssen mindestens nach Klassifizierung S2 / P4 vernichtet werden

3.7.5. Schutz der Anlieferungs- und Versandbereiche vor unbefugtem Zutritt

Es ist sichergestellt, dass alle Zugänge zu geschützten Zonen, darunter der Anlieferungs- und Versandbereich vor unbefugtem Zutritt geschützt wird. Dazu zählt z.B. die Trennung des Bereichs von anderen Bereichen. Zutritt nur für identifiziertes und berechtigtes Personal.

3.8. Betriebssicherheit

3.8.1. Aktualisierungen

Das regelmäßige Aktualisieren von Systemen ist in der heutigen Zeit üblich und wird gefördert.

- Aktualisierungen werden zeitnah eingespielt.
- Die Priorisierung erfolgt auf Grund von Dringlichkeit, Risiko durch Sicherheitslücken und Testbedarf.

3.8.2. Schwachstellen

Werden Sicherheitslücken, für die keine Behebung in Form einer Aktualisierung vorhanden ist, identifiziert, kann der Zugang zu Diensten oder Systemen eingeschränkt werden, bis das Problem behebbar ist.

3.8.3. Backups

Alle Systeme werden regelmäßig gesichert. Die Datensicherung erfolgt unter folgenden Gesichtspunkten:

- Datensicherungen erfolgen automatisch und an zwei getrennten Standorten.
- Datensicherungen sind in besonderem Maße vor Verlust, Änderung oder unberechtigten Zugriff geschützt.
- Datensicherungen müssen mindestens einmal am Tag erfolgen, die Wiederherstellung ebenfalls innerhalb von 24 Stunden möglich sein.
- Datensicherungen und die Wiederherstellungsprozedur werden regelmäßig getestet
- Gesetzliche Anforderungen werden eingehalten (z.B. werden Logs von Backups überprüft, etc.)
- Definition Ereignis-Logs

Regelmäßige Durchführungen von Audits durch den entsprechend qualifizierten Informationssicherheitsbeauftragten bzw. Auditor erfolgen rechtzeitig und nach Abstimmung mit Betreiber und Nutzer der entsprechenden IT-Systeme. Zu den Anforderungen an die Auditierung von IT-Systemen zählt die regelmäßige und nachvollziehbare Überprüfung. Die Audit-Planung erfolgt im Rahmen der ISO-Audit-Planung. Termine sind rechtzeitig mit den Beteiligten festgelegt. Die Überprüfung der ISMS-Anforderungen erfolgt mit den internen Audits zur ISO-9001. Folgende Punkte sollen mit abgeprüft werden:

- aus den Ergebnissen werden Maßnahmen abgeleitet,
- es erfolgt eine Nachverfolgung der abgeleiteten Maßnahmen
- für Abweichungen werden weitere Maßnahmen definiert, deren Änderung im Rahmen der regelmäßigen ISO-9001 Überprüfung kontrolliert werden
- Ergebnisse werden nachvollziehbar in einem Audit- bzw. Management-Bericht gespeichert
- Die Leistungserbringung durch Dienstleister wird regelmäßig überwacht und überprüft. Interne und externe Audits folgen demselben Prozess. Zusätzlich wird bei externen Dienstleistern auch die Einhaltung vertraglicher Vereinbarungen überprüft.

3.8.4. Schutz vor Schadprogrammen

Alle Systeme sind vor Schadprogrammen und weiteren Gefahren zu schützen

- Einsatz einer Software mit Endpunktschutz, die zentrale Verwaltung und Einsicht möglich.
- Einsatz einer netzwerkseitigen und clientseitigen Firewall.
- Regelmäßiger Scan aller Systeme und Analyse der Protokolle

3.8.5. Protokollierung und Überwachung

Sicherheitsrelevante Ereignisse wie fehlgeschlagene Log-Ins oder Einbruchversuche werden gesammelt, mit Zugriffsrechten besonders geschützt und wenn nötig analysiert, um sicherheitsrelevante Vorkommnisse aufzuklären.

3.8.6. Cloud-Dienste

Cloud-Dienste unterliegen dem gleichen Sicherheitsniveau wie andere Dienste oder Systeme des Unternehmens. Die Erfüllung des Sicherheitsniveaus kann durch vertragliche Zusicherung (siehe Lieferantenbeziehungen) gewährleistet werden.

3.8.7. Uhrensynchronisation

Alle Uhren von IT-Systemen werden zentral mit einem einzigen Zeitserver synchronisiert.

3.9. Anschaffung und Entwicklung von Systemen

Ziel: Neu entwickelte oder angeschaffte Systeme erfüllen unsere Anforderungen an Informationssicherheit.

3.9.1. Softwareentwicklung

Die Entwicklung von Software und Systemen, intern oder durch Dritte, berücksichtigt folgende Aspekte:

- Sicherheitsanforderungen an Quellcodeverwaltung und Entwicklungsumgebung
- Sicherheitsanforderungen an das Produkt
- Test der Sicherheitsanforderungen
- Umgang mit Testdaten

3.10. Reaktion auf Sicherheitsvorfälle

Ziel: Auf Sicherheitsvorfälle wird angemessen reagiert und die Erfahrungen genutzt, um das ISMS und den Angriffsschutz zu verbessern.
Die Aufgaben sind unter anderem:

- Überwachen von Systemen und Datenströmen auf verdächtige Aktivitäten
- Koordination von Reaktionen auf Sicherheitsvorfälle
- Erkenntnisse aus Vorfällen fließen in die laufende Verbesserung der Systemsicherheit ei

3.11. Business Continuity Management

Ziel: Sicherstellen der Handlungsfähigkeit in Ausnahmesituationen.

Das Unternehmen identifiziert mit Hilfe des Risikomanagements mögliche Gefahrensituationen für das Unternehmen und konstruiert Notfallpläne und Maßnahmen, die in diesen Fällen die Handlungsfähigkeit des Unternehmens aufrechterhalten. Dieser besteht aus dem ISB, EDV und QM. Bei Bedarf werden die betroffenen Bereiche mit einbezogen und die Geschäftsführung über Maßnahmen und Prozesse informiert.