Richtlinie zur Informationssicherheit der Sörensen Hydraulik GmbH

Status Veröffentlicht

Herausgeber Sörensen Hydraulik GmbH

Geltungsbereich Diese Handlungsleitlinien gelten für die Sörensen Hydraulik GmbH mit den Standorten

- Hamburg
- Ulfborg / Dänemark

Sie sind von allen Mitarbeitern und Auftragnehmern anzuwenden und einzuhalten.

Inhaltsverzeichnis

Der Schutz der Informationen, die im Rahmen der Geschäftstätigkeit entstehen, erstellt, zur Verfügung gestellt, verarbeitet, ausgetauscht oder in sonstiger Weise benutzt werden, ist für die Sörensen Hydraulik GmbH von existentiell wichtiger Bedeutung.
Bei der Umsetzung der Regelungen dieser Richtlinie sind weitergehende Festlegungen, die sich z.B. aus Gesetzen, Gesetzen gleichzusetzenden Vorschriften oder betrieblichen Regelungen ergeben, zu beachten.

1. Inhalt der Arbeitsanweisung

Diese Arbeitsanweisung regelt die Richtlinien und Vorgehensweisen der Sörensen Hydraulik GmbH hinsichtlich der Informations- und Telekommunikationssicherheit. Sie ist verbindlich geltend für alle Mitarbeiter des Unternehmens, die ihre Verhaltensweise entsprechend daran ausrichten müssen.
Die Richtlinie zur Informationssicherheit dient dem Schutz der Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, der Nachweisbarkeit von Handlungen sowie der Wahrung der Rechte und Interessen aller natürlichen und juristischen Personen, die mit der Sörensen Hydraulik GmbH in geschäftlicher Beziehung stehen bzw. für diese arbeiten.

2. Organisation der Informationssicherheit

Für die Organisation der Informationssicherheit ist die Geschäftsführung der Sörensen Hydraulik GmbH gesamtverantwortlich. Sie trifft die Regelungen hierzu und ist für die Umsetzung gesamtverantwortlich.

Dies beinhaltet, dass die gesamte Organisation der Sörensen Hydraulik GmbH gemäß diesem Standard agiert und sie Berücksichtigung in allen Geschäftsprozessen finden.
Insbesondere bei der Auswahl geeigneter Geschäftspartner und Mitarbeiter sind als Basis die Richtlinien zur Informationssicherheit zu Grunde zulegen. Die Geschäftsführung ist für die Analyse und Bewertung der jeweiligen Partner und Mitarbeiter verantwortlich. Die Einweisung der jeweiligen Personen zur Einhaltung dieser Standards ist verpflichtend.

Jeder Mitarbeiter der Sörensen Hydraulik GmbH ist seinerseits für die Einhaltung der Regelungen und Handlung gemäß der Richtlinien und Anweisungen verantwortlich.

3. Geheimhaltungsvereinbarung

Jeder Mitarbeiter oder Geschäftspartner ist zu einer Geheimhaltungsvereinbarung verpflichtet, die standardgemäß im Anstellungs- oder Projekt- bzw. Rahmenvertrag unterzeichnet wird.

4. Inventarisierung

Vermögenswerte im Unternehmen müssen gemäß den gesetzlichen Anforderungen im Anlagespiegel aufgeführt und inventarisiert werden. Die IT Komponenten in Sörensen Hydraulik GmbH sind gelistet (Nutzer, Hardware und Software) unter SharePoint.

5. Datenklassifikation

Die Klassifikation der Daten/Informationen und dessen Umgang werden gemäß der folgenden Tabelle durchgeführt:

Kategorie	Definition	Vorgaben zum Umgang
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 Geschäftsführung *Beispiele: Pressemitteilungen, Produktkatalog für Kunden*	**Kennzeichnung:** Keine **Vervielfältigung und Weitergabe:** Keine Einschränkungen **Speicherung:** Keine Einschränkungen **Löschen:** Keine Einschränkungen **Entsorgung:** Keine Einschränkungen
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 Kommunikation, nicht vertrauliche Entwicklungsergebnisse etc.*	**Kennzeichnung:** Keine (oder Intern) **Vervielfältigung und Weitergabe:** Nur an berechtigte Mitarbeiter 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

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. *Beispiele: Personenbezogene Daten, die über dienstliche Kommunikationsdaten hinausgehen (z.B. Gehaltsdaten), Budgetpläne, Revisionsberichte, Entwicklungsergebnisse, Auswertungen etc.*	**Kennzeichnung:** "Vertraulich". Kennzeichnung auf der ersten Seite des Dokumentes in elektronischer und gedruckter Form. **Vervielfältigung und Weitergabe:** Die Einsicht der Daten/Informationen ist nur für berechtigte Mitarbeiter und berechtigter Dritter innerhalb des Aufgaben- oder Anwendungsbereichs bestimmt. Ein Austausch per Datenträger (wie USB-Stick, externe Festplatte etc.) darf nur in Ausnahmefällen und wenn erforderlich dann verschlüsselt erfolgen. Die Daten sind nach dem Austausch umgehend von den Datenträgern zu löschen. Ein Ausdruck oder papiergebundener Transport der Daten ist zu vermeiden, falls dennoch erforderlich müssen die Seiten unmittelbar nach Verwendung vernichtet werden (Shredder etc.). Der E-Mail-Austausch ist ausschließlich nur durch gesicherte Verbindungen, z.B. mittels TLS- Verschlüsselung erlaubt. Alternativ dürfen Dateien gezippt und passwortgeschützt werden. Das zugehörige Passwort muss hierbei über einen weiteren Übertragungskanal wie SMS oder telefonisch dem Empfänger übermittelt werden. **Speicherung:** Die Speicherung der projektbezogenen und vertraulichen Daten erfolgt ausschließlich in den dafür eingerichteten Projektordnern, die über eine Zugriffsregelung für berechtigte Mitarbeiter verfügen. **Löschen/Entsorgung:** Nicht mehr benötigte Daten sind mittels geeigneter Shredder-Software (>7 Passes) zu löschen. Die Entsorgung von Schriftstücken erfolgt durch einen Papiershredder.

Geheim	Informationen, deren Kenntnis durch Unbefugte oder deren missbräuchliche Weitergabe und Verwendung das Erreichen von Unternehmenszielen nachhaltig gefährden kann und die daher einem äußerst restriktiven Verteiler und strikten Kontrollen unterliegen müssen. *Beispiele: Besondere Arten personenbezogener Daten (z.B. Gesundheitsdaten), Cycle-Pläne, Vorstandsvorlagen, Pläne zur Unternehmensstrategie, Designbilder von neuen Prototypen*	**Kennzeichnung:** "Geheim"-Kennzeichnung auf jeder Seite des Dokumentes. **Vervielfältigung und Weitergabe:** Die Einsicht der Daten/Informationen ist nur für einen äußerst begrenzten Bereich (z. B. namentliche Liste) berechtigter Mitarbeiter und berechtigter Dritter innerhalb des Aufgaben- oder Anwendungsbereichs nach vorheriger Genehmigung des Informationseigentümers bestimmt. Dabei sind die Daten, soweit technisch möglich, nach aktuellem Stand der Technik zu verschlüsseln. Sofern dies technisch nicht möglich ist, sind vergleichbare Schutzmaßnahmen einzusetzen. Zusätzlich sind weitere technische oder organisatorische Schutzmaßnahmen fallbezogen einzusetzen (z. B. Weitergabe- oder Druckverbot, Wasserzeichen). Es sind geeignete Sprachmedien zu nutzen, um ein Mithören zu verhindern (z. B. verschlüsselte Videokonferenz). Geheime Daten werden grundsätzlich durch verschlüsselte Hardware-Medien wie z. B. Disketten CD's, Tapes verschlüsselt weitergegeben. Die Weitergabe erfolgt durch: - persönliche Übergabe (hand-shake) mit Dokumentation - Direkt-Kuriere (im neutralen Umschlag als Wertpostbrief, darin ein verschlossener Umschlag mit Vermerk „geheim"). Es dürfen keine Original-Datenträger weitergegeben werden, sondern Kopien der Originale. Ein Ausdruck oder papiergebundener Transport der Daten ist zu vermeiden, falls dennoch erforderlich müssen die Seiten unmittelbar nach Verwendung vernichtet werden (Shredder etc.).

		Speicherung: Die Speicherung der projektbezogenen und geheimen Daten erfolgt ausschließlich in den dafür eingerichteten Projektordnern, die über eine Zugriffsregelung für berechtigte Mitarbeiter verfügen. Für die Speicherung geheimer Daten ist eine technische Lösung zur Verschlüsselung der Speicherbereiche zu implementieren. **Löschen/Entsorgung:** ▪ Nur nach Rücksprache mit dem Auftraggeber ▪ Erstellen einer Protokollierung (wer, wann, was, wo, womit) ▪ Protokollierung durch die Auftraggeber Fachabteilung schriftlich bestätigen lassen Grundsätzlich werden Datenträger mit geheimen Daten physisch vernichtet.

6. Benutzerregistrierung und Zugriffsberechtigung

Die Benutzerregistrierung, sowie die Vergabe und Verwaltung der Benutzerrechte im Unternehmensnetzwerk erfolgt durch die Sörensen IT-Abteilung, mittels Beauftragung der Geschäftsführung. Hierzu wird seitens der IT-Abteilung der schriftliche Nachweis geführt, wer wann welche Benutzerkennung erhalten hat.

Darüber hinaus sind die Zugriffsberechtigungen der einzelnen Mitarbeiter gemäß ihren Zuständigkeiten auf die jeweiligen Laufwerke/ Projektordner festzulegen und freizugeben. Die jeweiligen Zugriffsberechtigen sind zu protokollieren und einmal jährlich auf ihre Aktualität zu überprüfen. Die Überprüfung und ihr Ergebnis ist zu dokumentieren.

Lokale Administrator-Rechte sollten nur in beschränktem Umfang erteilt werden. Die jeweiligen Anwender sind spezifisch zu belehren und auf die Gefahren hinzuweisen. Die lokalen Administrator-Rechte sind zu dokumentieren und ebenfalls regelmäßig zu überprüfen.

Die Wiederverwendung von personenbezogenen Benutzerkennungen 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 Rückgabe der jeweiligen Benutzerkennung muss das Kennwort vom zuständigen Betreuer 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.

7. Benutzeranmeldung im Netzwerk

Die Benutzeranmeldung im Netzwerk erfolgt mittels einer Authentifizierung mit Namen und Passwort, die den Benutzer für die Anmeldung am PC und im Netzwerk autorisiert.

Für das Passwort ist eine sechsstellige Ziffernkombination vorgeschrieben, die keine trivialen Kombinationen (z.B. „123456“, „111111“ etc.) oder Aspekte aus dem persönlichen Umfeld (z.B.
Geburtsdatum) beinhaltet.

8. Passwörter

Grundsätzlich können Nutzer ihre Kennwörter nicht selbst ändern. Die Kennwörter dürfen Dritten nicht bekannt sein, Ausnahme ist der IT Administrator. Die nachstehende Komplexität- und Kennwortgültigkeit ist mittels technischer Maßnahme zu prüfen und durchzusetzen.

Jeder Nutzer hat ein Passwort, das die folgenden Mindestkriterien erfüllen:

- Es ist eine mindestens 6-stellige Kombination mit mindesten 2 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
- Passwörter dürfen nicht weitergegeben oder zugänglich aufbewahrt bzw. abgespeichert werden

Info: In der Praxis bewähren sich Passwörter, die sich aus Merksätzen oder auch Abkürzungen und Verfälschung von Merksätzen bilden.

Beispiel: Passwort: "Sicher-ist-besser!" oder Merksatz "Morgens stehe ich früh auf und putze meine Zähne." wird zu Passwort: "Ms1fa&pmZ.“

Wichtig: Die hier angegeben Beispiele sind nicht als eigene Passwörter zu verwenden!

9. Arbeitsplatz bei Abwesenheit

Der Arbeitsplatz ist vor einer Abwesenheit so zu verlassen, dass keine Dokumente mit mindestens interner Klassifikation einsehbar auf dem Arbeitsplatz verbleiben.

Der Nutzer muss sich in jedem Fall vom Computer abmelden. Der Nutzer hat einen Bildschirmschoner mit Passwortschutz zu verwenden.

Beim täglichen Dienstschluss muss sich der Nutzer abmelden und den Computer ausschalten / herunterfahren (Sicherheit gegen Zugriff von außen).

10. Mobile Computer

Beim Umgang mit mobilen Computern ist besondere Sorgfalt seitens des Nutzers erforderlich. Eine Verschlüsselung ist derzeit nicht vorgesehen.

Das Arbeiten in öffentlichen Bereichen, so dass das Einsehen der Informationen am Bildschirm Dritten möglich ist, ist nicht erlaubt. Es ist besondere Sorgfalt erforderlich, dass das Gerät nicht entwendet werden kann. Bei dem Transport und Nutzung des Laptops auf Dienstreisen muss das Gerät bei sich geführt werden. Eine Lagerung im Auto ist nicht gestattet. Bei einem Hotelaufenthalt ist das Gerät in Hotelsafe sicher zu verwahren. Besondere Sorgfalt ist darauf zur richten, dass das Gerät bei Nichtbenutzung gesperrt ist und nur mit Passwort entsperrt werden kann.

11. Antiviren-Schutz

Die Computer im Unternehmen sind mit Antiviren-Software auszustatten. Diese ist so zu konfigurieren, dass sie in einer täglichen Routine die Virenliste aktualisiert. Darüber hinaus sind die Systeme so zu konfigurieren, dass sie in vorgegebenen Zeitabständen einen kompletten Virensuchlauf durchführen.

Die Virenschutz Software ist so zu konfigurieren, dass sie automatisch Dateien auf mobilen Datenträgern oder Mail Attachments vor dem Öffnen überprüft.

Die Überprüfung der Funktionalität der Antiviren-Schutz-Software und dessen Aktualisierung wird durch die extern beauftragte IT-Firma in regelmäßigen Abständen durchgeführt und protokolliert. Die extern beauftragte IT-Firma prüft die ordnungsgemäße Funktion und berichtet darüber.

12. Systemaktualisierung

Die Systeme werden durch die Sörensen IT Abteilung aktualisiert. Die Überprüfung der Funktionalität der Aktualisierungsroutine wird durch die Sörensen IT-Abteilung in regelmäßigen Abständen durchgeführt und protokolliert.

13. Datensicherung

Datensicherungen müssen regelmäßig in einem festgelegten Turnus (täglich) durchgeführt werden. Die Speicherung erfolgt auf einem Datenträger, der an einem anderen Ort (andere Brandabschnitt) als die zu sichernde Server sicher verwahrt wird.

Neben der regelmäßigen kurzfristigen Datensicherung muss in längeren Abständen (mindestens einmal im Quartal) eine Datensicherung durchgeführt werden, die an einem anderen Ort als dem Gebäude des Büroraums sicher verwahrt wird.

In größeren Abständen ist ein Wiederherstellungstest (Recovery) durchzuführen. Die Durchführung und das Ergebnis sind zu dokumentieren.

Nach jeder Sicherung ist durch Überprüfung zu gewährleisten, dass die Datensicherung korrekt ausgeführt wurde, und dass die Wiederherstellung der Daten einwandfrei funktioniert.

Die Überprüfung der Funktionalität des BackUp-Systems wird durch die extern beauftragte IT-Firma in regelmäßigen Abständen durchgeführt und protokolliert.

14. Netzwerk

Das Netzwerk ist so zu konfigurieren, dass nur identifizierte Geräte Zugriff zum Netzwerk haben. Wifi-Netzwerke dürfen nur verschlüsselt betrieben werden. Verwendete Schlüssel sind nach den geltenden Passwortkriterien (siehe Punkt 8) anzulegen.

15. Mobile Datenträger

Mobile Datenträger dürfen grundsätzlich nicht eingesetzt werden. Ist ein Einsatz zwingend aus betrieblichen Gründen erforderlich, so ist hierzu die Genehmigung der Geschäftsleitung erforderlich. Die USB-Anschlüsse und CD-Laufwerke aller Rechner bis auf die der Geschäftsleitung sind gesperrt. Die Freischaltung des erforderlichen USB-Anschlusses wird durch die Sörensen IT-Abteilung vorgenommen und überwacht. Nach Nutzung wird der USB-Anschluss wieder gesperrt. Nach der Übergabe sind die Daten vom mobilen Datenträger zu löschen.

Mobile Datenträger werden auch für die Datensicherung verwendet. Diese Datenträger müssen an einem sicheren Ort verschlossen verwahrt werden.

Die Daten auf den mobilen Datenträgern sind nicht verschlüsselt abgespeichert.

Vor der Entsorgung der Datenträger müssen diese unbrauchbar gemacht werden, in dem sie physikalisch zerstört, zerbrochen etc. werden.

Der Transport dieser Medien per Post, Kurier etc. ist untersagt.

16. Mobile Kommunikationsgeräte

Mobile Kommunikationsgeräte (Handys, Smartphones u.Ä.), die an Mitarbeiter ausgegeben werden, werden in einer zentralen Liste erfasst. Die Nutzer sind schriftlich über die besonderen Gefahren und Sicherheitsmaßnahmen im Umgang mit den Geräten, insbesondere bei der Speicherung von Daten und der Installation von Software auf den Geräten, sowie den erlaubten Umfang der Nutzung zu belehren. Die Belehrung ist zu dokumentieren.

Soweit Daten oder Informationen auf mobilen IT-Geräten oder mobilen Systemen gespeichert werden sollen, ist der Zugang zu den Geräten grundsätzlich mit einem 4-stelligen Pin zu schützen.

17. Umgang mit Mail-Attachments / Websites

Mail Attachments mit ausführbarem Inhalt (z.B. MS Office Dateien, exe/zip Dateien etc.) dürfen nur geöffnet werden, wenn sie von vertrauenswürdigen Personen stammen. Es ist darauf zu achten, dass der Virenschutz in jedem Fall aktiv ist.

Bei Webseiten mit ausführbaren Inhalten ist darauf zu achten, dass sie vertrauenswürdig sind. Darüber hinaus ist darauf zu achten, dass der Virenschutz aktiv ist und die Einstellungen im Browser so restriktiv wie möglich gehalten werden.

18. Elektronischer Austausch von Informationen per Mail, FTP etc.

Informationen, die mindestens die Klassifikation vertraulich haben, dürfen nur verschlüsselt per Email oder FTP ausgetauscht werden. Hierfür ist der E-Mail-Dienst auf den internen Server verlagert. Der sichere E-Mail Austausch wird mit einem Verschlüsselungsprotokoll gewährleistet.

Mindestanforderung ist der Austausch per verschlüsselten Zip-File (Mindestlänge des Kennwortes 10 Zeichen, Bildungsvorschrift siehe Abschnitt „Passwörter"). Das Passwort hierzu darf nicht per Mail ausgetauscht werden, sondern muss persönlich, telefonisch oder per SMS übermittelt werden.

19. Physische Sicherheit

Die Sicherheitszone der Sörensen Hydraulik GmbH sind die Büroräume am Firmensitz in Hamburg (21031 Hamburg, Osterrade 3) und am Standort in Ulfborg (DK-6990 Ulfborg, Industriearealet 54). Die Büroräume sind beim Verlassen abzuschließen und die Schlüssel sicher zu verwahren.

In den Büroräumen herrscht kein Publikumsverkehr. Etwaige Besucher werden ausschließlich im Beratungsraum empfangen. Die Besucherregelung ist unter Punkt 23 aufgeführt.

Im Büroraum herrscht Film- und Fotografierverbot.

Die Eingangsbereiche zu den Büroräumen sind verschlossen. Zugang ist nur nach Anmeldung am Empfang möglich.

Im Falle eines Einbruchs muss umgehend die örtliche Polizeidienststelle informiert werden.

20. Schulung zur Informationssicherheit

In regelmäßigen Abständen (mindestens einmal jährlich) führt die Geschäftsführung der Sörensen Hydraulik GmbH Informations- und Schulungstermine zur Informationssicherheit und den Regelungen dieser Richtlinie durch. Die Teilnahme an den Schulungsterminen wird von den Mitarbeitern mit einem Teilnahmenachweis schriftlich bestätigt.

21. Meldung von Vorkommnissen und kontinuierlichen Verbesserungen

Jeder Mitarbeiter ist verpflichtet besondere Vorkommnisse wie einen Verdacht auf Schadsoftware oder einen Hackerangriff unverzüglich der Geschäftsführung zu melden.

Darüber hinaus ist jeder Mitarbeiter im Sinne einer kontinuierlichen Verbesserung aufgefordert und verpflichtet, Vorschläge zur Verbesserung der IT Sicherheit gegenüber der Geschäftsführung vorzubringen.

Die Geschäftsführung ist verpflichtet, besondere Vorkommnisse, die mittelbar oder unmittelbar Auswirkungen auf Daten von Geschäftspartnern haben, wie z.B. Einbruch, Diebstahl, Feuer oder Hacking-Angriffe, unverzüglich dem Geschäftspartner zu melden. Darüber hinaus ist die Geschäftsführung verpflichtet, Änderungen mit Bezug auf zertifizierte Sicherheitsbereiche (bauliche Veränderungen, Standortwechsel, Änderungen der Verantwortlichkeit, der Rahmenbedingungen etc.) unverzüglich dem zertifizierenden Geschäftspartner mitzuteilen.

22. Anwendung der Arbeitsanweisung bei Mitarbeitern und Partnerfirmen

Die Arbeitsanweisung ist für Mitarbeiter und Partnerfirmen der Sörensen Hydraulik GmbH verbindlich, sobald sie mit mindestens als vertraulich klassifizierten Daten zu tun haben.

Für die Umsetzung der Arbeitsanweisung bei den betroffenen Mitarbeitern und Partnerfirmen ist die Geschäftsführung der Sörensen Hydraulik GmbH verantwortlich. Dies überprüft die Geschäftsführung in regelmäßigen Abständen (mindestens einmal jährlich), legt ggf. umzusetzende Maßnahmen fest und hält die Umsetzung dieser nach. Die Vor-Ort Termine werden schriftlich protokolliert.

23. Besucherregelung

Die Besucherregelung schreibt den Umgang mit den Besuchern der Sörensen Hydraulik GmbH vor. Besucher sind beim Eintritt in die Firmenräumlichkeiten in einem Besucherbuch mit Datum, Name, Vorname und Firma einzutragen. Darüber hinaus sind alle Besucher zum Datenschutz/Fotografier-Verbot aktenkundig zu belehren und auf Geheimhaltung zu verpflichten. Die Besucher bestätigen per Unterschrift, dass sie die Richtlinien verstanden haben und sich zur Umsetzung verpflichten.

Mitarbeiter externer Firmen (z.B. Reinigungskräfte, Monteure und Handwerker) sind wie Besucher zu behandeln. Externe Mitarbeiter dürfen nur unter Aufsicht arbeiten. Clear Screen und Clean Desk sind strikt einzuhalten.

24. Film- und Fotografierverbot

In den Räumlichkeiten der Sörensen Hydraulik GmbH besteht generelles Film- und Fotografierverbot. Entsprechende Hinweisschilder sind an den Zugängen zu den internen Bereichen angebracht. Mitarbeiter und Besucher sind diesbezüglich zu belehren und zur Einhaltung der Festlegungen zu verpflichten.

Die Anfertigung von Aufzeichnungen (Film, Foto, Audio usw.) bedarf grundsätzlich immer der Genehmigung durch die Geschäftsleitung. Die Verwendung von privatem oder fremdem Equipment ist dafür nicht gestattet. Aufzeichnungen, die für firmeninterne Zwecke notwendig sind und durch die Geschäftsleitung autorisiert wurden, sind ausschließlich mit firmeneigenem Equipment anzufertigen. Die Behandlung der aufgezeichneten Daten erfolgt dann gemäß der jeweiligen Datenklassifikation.