STAR COOPERATION®

Your Partners in Excellence

Richtlinien

Informations-Sicherheits-Richtlinie für externen Dienstleister und Geschäftspartner

Geltungsbereich: Externe Dienstleister

Ersteller: Marcus Heer

Stand: 21.02.2018
Version: 2.0

Inhaltsverzeichnis

1 Präambel

Informationen – unabhängig ob digital oder in sonstiger Form wie Papier - gehören zu unseren wichtigsten Unternehmenswerten. Informationen über Projekte, Finanzen, Geschäftsprozesse, Kunden, Lieferanten, Partner und Mitarbeiter sind unerlässlich für unseren Geschäftserfolg. Deshalb sind der Schutz und die Sicherung dieser Informationen von entscheidender Bedeutung für unser Unternehmen und unsere Kundenbeziehungen.

Um diese Informationen zu schützen und Ihnen eine Hilfestellung beim Umgang mit diesen zu geben, haben wir die nachfolgende Richtlinie erstellt.

Diese Informations-Sicherheits-Richtlinie tritt am 13.06.2017 in Kraft.

Geltungsbereich

Diese Informations-Sicherheits-Richtlinie gilt für alle externen Personen (z.B. Dienstleister, Lieferanten, Kunden und an der Projektarbeit beteiligte Personen), die regelmäßig in unserem Unternehmen tätig sind oder Zugang zu unseren Unternehmenssystemen habe. Die externen Personen sind verpflichtet, sich an diese Richtlinie zu halten. Zur Sicherstellung der durchgängigen Informations-Sicherheit bedarf ein Abweichen von den Vorgaben dieser Richtlinie der schriftlichen Zustimmung des Informations-Sicherheits-Beauftragten (ISO).

Das Unternehmen wird entsprechende Vorkehrungen treffen, damit diese Richtlinie auch für die externen Personen verbindlichen Charakter hat. Ergänzenden Informationen zum Thema „IT-Sicherheit“ finden Sie auch in den IT Richtlinien der Firmengruppe.

Einhaltung von Rechtsvorschriften

Bei Umgang mit Informationen in unserem Unternehmen sind von den externen Personen die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie die Unternehmensregelungen einzuhalten. Sollten externe Personen unsicher sein, ob und inwieweit Rechtsvorschriften oder Unternehmensregelungen einzuhalten sind, haben sie sich an ihren unternehmensinternen Ansprechpartner zur Klärung zu wenden. Dieser muss ggf. Unklarheiten mit der IT-Abteilung oder dem Informations-Sicherheits-Beauftragten (ISO) abstimmen.

2 Welche Arten von Informationen gibt es?

Zur Gewährleistung des sicheren und sorgsamen Umgangs mit Informationen sind die folgenden 4 Kategorien für die Einstufung von Informationen hinsichtlich Vertraulichkeit festgelegt.

- Die Einstufung **geheim** bezeichnet die vertraulichsten aller Informationen. Die Weitergabe von geheimen Informationen muss auf einen sehr kleinen, namentlich bekannten Kreis von Personen beschränkt sein.

  - Geheime Informationen sind immer unter Verschluss zu halten
  - Papierunterlagen sind mit dem Wort „Geheim“ zu kennzeichnen. Dies kann durch einen Stempel oder ähnliche Kennzeichnungen erfolgen.
  - Für die Erstellung von geheimen Informationen ist eine spezielle Vorlage (mit Fußzeile „Geheim“) zu verwenden
  - Geheime Informationen dürfen NICHT per Email versendet werden
  - Das Speichern von geheimen Informationen darf nur auf verschlüsselten Datenträgern erfolgen. Wenden Sie sich hierzu an die „Anwenderbetreuung“.

  Beispielsweise sind vertraulich eingestufte Informationen:

    - Unterlagen, die der Jahresabschlusserstellung dienen
    - Strategische Entscheidungsgrundlagen
    - Dokumentationen zu gravierenden Störfällen
    - Passwörter
    - Unterlagen zu neuen Entwicklungen, die an externen Dienstleister übermittelt werden

- Die Einstufung **vertraulich** bezeichnet Informationen mit dem zweithöchsten Vertraulichkeitsniveau. Die Weitergabe von vertraulichen Informationen muss auf einen kleinen Personenkreis beschränkt sein.

  - Vertrauliche Informationen sind immer unter Verschluss zu halten
  - Papierunterlagen sind mit dem Wort „Vertraulich“ zu kennzeichnen. Dies kann durch einen Stempel oder ähnliche Kennzeichnungen erfolgen.
  - Für die Erstellung von vertraulichen Informationen ist eine spezielle Vorlage (mit Fußzeile „Vertraulich“) zu verwenden.
  - Vertrauliche Informationen dürfen NUR VERSCHLÜSSELT per Email versendet werden. Wenden Sie sich hierzu an die „Anwenderbetreuung“.
  - Das Speichern von vertraulichen Informationen erfolgt in Dateiverzeichnissen mit eingeschränktem Benutzerzugriff.

  Beispielsweise sind vertraulich eingestufte Informationen:

    - Kalkulationen
    - Personalunterlagen
    - Entgelt-Unterlagen
    - Bewerberunterlagen
    - Betriebswirtschaftliche Daten, Reports
    - Vertragsunterlagen
    - Entwicklungsdaten
    - Projektdaten

Intern ist die gebräuchlichste Einstufung von Informationen. Die Weitergabe von internen Informationen ist normalerweise auf größere Personengruppen beschränkt. Der Versand von Emails ist unverschlüsselt möglich. Alle erstellten Dokumente gelten grundsätzlich zunächst als „Intern“ und sind in der Fußzeile der erstellten Dokumente zu kennzeichnen.

Beispielsweise sind intern eingestufte Informationen:

- Telefonverzeichnis der Mitarbeiter
- Organigramme
- Aufgaben-beschreibungen
- Kundendatenbanken
- Besprechungs-protokolle

Als **öffentlich** eingestufte Informationen sind nicht vertraulich und für den allgemeinen Gebrauch innerhalb und außerhalb von Star bestimmt.

Beispielsweise sind öffentlich eingestufte Informationen:

- Marketingunterlagen Vertriebspräsentationen,
- Angebote
- Referenzlisten.

Die Verantwortung für die richtige Klassifizierung und dem Umgang mit den Informationen trägt der Informationseigner.

3 Richtiger Umgang mit schützenswerten Informationen auf Reisen

Auf den mobilen Endgeräten, die in Ihrem Eigentum stehen oder die Ihnen vom Unternehmen zur Verfügung gestellt werden (z.B. Laptops, Handys, Smartphones, Tablets, USB-Sticks,...), sind ggf. unternehmenseigene Daten gespeichert. Verlust oder Diebstahl können schädliche Auswirkungen für das Unternehmen haben.

- Nehmen Sie grundsätzlich nur die Unterlagen, die Sie tatsächlich benötigen, mit auf Dienstreisen.
- Bei Reisen in Drittländer (bspw. China, USA, Russland) kann nicht ausgeschlossen werden, dass Behörden bei Einreise Zugriff auf Daten von Endgeräten nehmen. Daher müssen bei Reisen in solche Länder immer von IT-Services, bereit gestellte Notebooks ohne lokale Datenverfügbarkeit genutzt werden. Zugriff auf die Daten (E-Mails, Dateien) ist über die Cloud möglich. Das Notebook ist nach Rückkehr unverzüglich ohne Zugriff auf das Firmennetzwerk bei IT-Services abzugeben.
  Bei Smartphones/Tablets ist der E-Mail-Account vor Reiseantritt auf dem Endgerät zu löschen.
- Speichern Sie nur die Daten lokal verschlüsselt ab, die Sie unterwegs benötigen.
- Benachrichtigen Sie bei Verlust oder Diebstahl mobiler Endgeräte Ihren Vorgesetzten und informieren Sie die „Anwenderbetreuung“ per E-Mail.
- Führen Sie keine mobilen Endgeräte ohne Passwortschutz mit sich.
- Geben Sie mobile Endgeräte bei Reisen nicht mit Ihrem Koffer auf.

- Lassen Sie mitgeführte Unterlagen und mobile Endgeräte nie unbeaufsichtigt (z.B. im Auto) liegen. Auch Temperaturschwankungen können nicht nur die Festplatte, sondern auch andere Speichermedien sowie das LCD-Display beschädigen.

4 Richtiges Verhalten in der Öffentlichkeit

Viele Geschäftsgeheimnisse werden durch Gedankenlosigkeit vor allem in Gesprächen mit Kollegen oder durch Telefongespräche in öffentlichem oder privatem Umfeld (z.B. Flugzeug, Biergarten, Restaurant) preisgegeben.

- Seien Sie sich immer bewusst, worüber Sie wo kommunizieren. Achten Sie bei allen Gesprächen auf Vertraulichkeit.
- Geben Sie Informationen in Telefongesprächen nur an persönlich bekannte Geschäftspartner preis.
- Prüfen Sie im Zweifelsfall durch einen Rückruf die Identität des Anrufers.
- Achten Sie unterwegs darauf, dass niemand einsehen kann, woran Sie arbeiten (z.B. Laptop, Dokumente, etc.).
- Geben Sie keine vertraulichen und geheimen Unternehmensinformationen in privaten Gesprächen preis.
- Führen Sie keine vertraulichen Gespräche in der Öffentlichkeit (z.B. in Flugzeugen, in Hotels, Restaurants).
- Übermitteln Sie keine vertraulichen und geheimen Informationen über Dritte.
- Lassen Sie mobile Geräte nie unbeaufsichtigt.
- Geben Sie keine geheimen Informationen am Telefon preis!

5 Richtiges Verhalten im Internet und Emailnutzung

- Speichern sie die Zugangsdaten zu den Unternehmenssystemen nicht in Ihrem Browser.
- Geben Sie keine Informationen in sozialen Netzwerken (XING, Facebook oder ähnliche) preis, die Sie im Rahmen Ihrer Tätigkeit in unserem Unternehmen zur Kenntnis bekommen haben.
- Persönliche Profile dürfen keine Zusätze wie „arbeitet zurzeit für Kunde XXXX“ oder ähnliches enthalten.
- Besuchen Sie nur vertrauenswürdige Internetseiten.
- Klicken Sie nicht auf Links, die in SPAM-Mails oder „Kettenbriefen“ enthalten sind.
- Sofern Ihnen eine E-Mail-Account zur Verfügung gestellt wird, darf dieser ausschließt für die geschäftliche Kommunikation der Star verwendet werden. Eine private Nutzung ist ausdrücklich verboten.

- Beantworten Sie keine Emails, die persönliche Kennwörter oder PINs anfordern.
- Falls Sie am Absender der Email zweifeln – nicht antworten!

6 Richtiges Verhalten in unseren Geschäftsräumen

- Externe Personen müssen Besucherausweise tragen und am Empfang registriert werden.
- Besucherausweise müssen vor dem Verlassen des Gebäudes am Empfang abgegeben werden.
- Die standortbezogenen Sicherheitshinweise müssen eingehalten werden (z.B. Fotografierverbot, Schutzausrüstung usw.).
- Fremdgeräte dürfen nicht an das Unternehmensnetzwerk angeschlossen werden.

7 Sichere Aufbewahrung von Informationen

- Halten Sie vertrauliche oder geheime Unterlagen immer unter Verschluss.
- Sperren Sie Ihren Computer vor dem Verlassen des Arbeitsplatzes (Tasten "Strg+ALT+Entf" drücken und dann auf "Computer sperren" klicken).
- Beenden Sie die Verbindung zu den Unternehmenssystemen, sobald Sie Ihre Tätigkeit in den Unternehmenssystemen abgeschlossen haben.
- Lassen Sie keine Unterlagen (insbesondere Aufzeichnungen auf Flip-Charts oder Whiteboards etc.) in Besprechungszimmern liegen.
- Lassen Sie nie vertrauliche oder geheime Arbeitsunterlagen unbeaufsichtigt auf Ihrem Schreibtisch liegen.
- Lassen Sie nie mobile Geräte unbeaufsichtigt auf Ihrem Schreibtisch liegen. Notebooks müssen mit Kensington-Schlössern abgesichert werden.

8 Richtiger Umgang mit Speichermedien

Auf elektronischen Speicher- und Kommunikationsmedien (z.B. USB-Sticks, CDs, DVDs, etc.) sind oft vertrauliche oder geheime Unternehmensinformationen gespeichert. Um diese Informationen zu schützen, ist ein sicherer Umgang mit diesen Medien zwingend notwendig.

- Unternehmensdaten dürfen nur verschlüsselt auf mobilen Speichermedien gespeichert werden.
- Verstauen Sie bei Flugreisen Ihre mobilen Endgeräte im Handgepäck.
- Verwahren Sie Laptops, Handys, Schlüssel etc. sicher auf, auch außerhalb der Arbeitszeiten.
- Lassen Sie mitgeführte Unterlagen und Geräte nie sichtbar und unbeaufsichtigt (z.B. im Auto, Bahnhöfen, Flughäfen, Restaurants) liegen.

- Lassen Sie nie mobile Endgeräte unbeaufsichtigt auf Ihrem Schreibtisch liegen.

Sie sind als Nutzer von elektronischen Speicher- und Kommunikationsmedien für ein ordnungsgemäßes Vernichten verantwortlich. Unternehmenseigene Informationen gehören nicht in den Papierkorb, sondern müssen speziell entsorgt werden.

Für die STAR Unternehmensgruppe

Oliver Messer
Aktualisiert Februar 2018