Leitfaden
Physische Sicherheit

1. Zutritt

Der Zutritt zu Ihren Büro- und Archivräumen darf nur berechtigten Personen möglich sein. Schlüssel dürfen nicht an Dritte weitergegeben werden und es ist zu dokumentieren, wer welchen Schlüssel hat. Besucher und Gäste sollten begleitet werden und sich nicht unbeobachtet in Räumlichkeiten bewegen können.

☞ **Checkliste**:

- □ Schlüsselplan erstellen / aktualisieren
- □ Zutrittstüren und Fenster durch einen Fachspezialisten prüfen lassen. Weitere Informationen und ein Verzeichnis von Spezialisten finden Sie unter http://www.sicher-ses.ch/.

2. Clean Desk-Richtlinien

Clean-Desk-Richtlinien legen fest, wie der Arbeitsplatz auszusehen hat, wenn die Arbeitnehmerinnen und Arbeitnehmer das Büro (Arbeitsplatz) verlassen. Es soll sichergestellt werden, dass sensitive Daten sicher verwahrt werden, wenn der Arbeitsplatz nicht besetzt ist. Es wird empfohlen, Clean-Desk-Richtlinien schriftlich festzulegen mit mindestens folgenden Punkten:

- Alle Dokumente mit sensitiven Informationen müssen abschliessbar verwahrt werden (Schlüssel nicht stecken lassen!). Solche Dokumente dürfen also nicht offen abgelegt, an der Wand, auf dem Whiteboard, auf dem Flipchart, im Papierkorb, in Unterschriftenmappen, in Post- oder Kurierfächern, im Drucker, im Multifunktionsgerät oder im Altpapier hinterlassen werden.
- Speichermedien, wie z.B. USB-Sticks, Speicherkarten, Harddisks, und mobile Geräte, wie z.B. Smartphones und Tablets sowie Diktiergeräte sind wegzuschliessen.
- Jeglicher Papiermüll, der sensitive Informationen enthält, muss im dafür bereitgestellten Aktenvernichter entsorgt werden.
- Es dürfen keinerlei Hinweise auf Passwörter oder Tresorcodes vorhanden sein, z.B. auf Zetteln unter dem Telefon, unter der Schreibunterlage oder in der obersten Schublade.
- Am Ende des Arbeitstages werden die Arbeitsplatz-Computer heruntergefahren. Bei kurzfristigem Verlassen des Arbeitsplatzes ist der Computer zu sperren.
- Bei Arbeitsschluss sind alle Fenster zu schliessen. Bei kurzfristigem Verlassen des Arbeitsplatzes sind einstiegsgefährdete Fenster (im Parterre) zu schliessen.
- Am Ende des Arbeitstages ist der Arbeitsplatz aufzuräumen; es sollen keine Papierstapel auf dem Pult liegen bleiben.

☞ **Checkliste**:

- □ Clean Desk-Richtlinien für Ihr Unternehmen festlegen, einführen und die Einhaltung regelmässig überprüfen

3. Post-it, Flip-Charts und Pinnwände

Nicht nur am eigenen Arbeitsplatz dürfen keine Passwörter oder sensitive Daten auf Post-it-Zetteln notiert werden, auch nicht an Pinnwänden oder Flip-Charts. Wer ein Flipchart benutzt, ist dafür verantwortlich, die beschriebenen Seiten danach zu entsorgen; sensitive Daten im Aktenvernichter entsorgen.

☞ **Checkliste:**

- □ Hinweis beim Flip-Chart anbringen, dass beschriebene Seiten jeweils umgehend entsorgt werden müssen.

4. USB-Stick, Datenträger und Notebooks

USB-Sticks sind nicht vor unberechtigtem Zugriff geschützt, daher ist besondere Vorsicht geboten. Falls sensitive Daten auf USB-Sticks oder anderen Datenträgern gespeichert werden, sollten die Daten verschlüsselt werden. Das kann mittels Software erfolgen, beispielsweise mit **VeraCrypt** oder mit dem auf modernen Windowssystemen integrierte **BitLocker**. Erhältlich sind auch Datenträger mit einer festintegrierten Verschlüsselung.

☞ **Checkliste:**

- □ Setzen Sie USB-Sticks / Datenträger mit Datenverschlüsselung ein.
- □ Wenden Sie sich an Ihren IT Partner, um die Daten auf Ihrer Notebook-Harddisk zu verschlüsseln.

5. Abschliessbare Büromöbel

Wesentlicher Bestandteil der Clean-Desk-Richtlinien sind abschliessbare Büromöbel. Mitarbeitende können sensible Dokumente an einem sicheren Platz lagern. Die Möbel sollten mindestens über eine 3-Punkt-Schliessung verfügen. Auch bei den Büromöbeln sollte ein Schlüsselplan erstellt werden. Hochsensible Dokumente, die auf jeden Fall einbruch- und feuersicher verwahrt werden sollten, sind in einem Tresor (intern oder extern, z.B.in einem Schliessfach einer Bank) aufzubewahren. Erhältlich und online leicht auffindbar sind Nachrüstschlösser für Büromöbel, die noch nicht abschliessbar sind. Externe Archive eignen sich, um Dokumente sicher zu lagern, wenn im Büro kein Platz für die Aufbewahrung vorhanden ist. Schweizweite, zertifizierte Archivdienstleistungen finden Sie unter: www.archivsuisse.ch.

☞ **Checkliste:**

- □ Schlüsselplan der Büromöbel erstellen / aktualisieren.
- □ Büromöbel mit Schlössern nachrüsten.
- □ Prüfen, welche Dokumente in einem Tresor oder Schliessfach aufbewahrt werden sollten.

6. Entsorgung von Dokumenten

Im Bereich der Datenvernichtung sollte ebenfalls auf die Datensicherheit geachtet werden. Akten und Dokumente können mit einem Aktenvernichter zerschnitten und verkleinert werden, sodass sensible Inhalte nicht mehr lesbar sind, und danach in verschiedenen Müllbehältern entsorgt werden. Eine andere Möglichkeit wäre die sichere Entsorgung von vertraulichen Dokumenten outzusourcen, beispielsweise durch die Abholung durch professionelle Aktenvernichter, wie z.B. Reisswolf. Auf diese Weise werden die Unterlagen in zertifizierten Prozessen zuverlässig vernichtet.

Leitsätze für die Unterteilung von Altpapier:

- Was man einem Besucher an einem Tag der offenen Tür nicht zeigen würde, das sollte auch nicht im offenen Altpapier entsorgt werden.
- Im Unternehmen ausgedruckte Dokumente dürfen nicht im normalen Altpapier landen.
- Alle Dokumente, die mit einer Adresse versehen sind, dürfen nicht im offenen Altpapier entsorgt werden.

Idealerweise sollte die Trennung in «vertraulich» und «unbedenklich» möglichst früh stattfinden – damit kann der Aufwand für das Aussortieren verringert werden.

☞ **Checkliste:**

- □ Hinweis beim Altpapier anbringen, welche Dokumente in den Aktenvernichter müssen.

7. Vertrauliche Unterlagen

Vertrauliche Unterlagen, die Kundendaten, Mitarbeitendendaten oder Entwicklungsdaten enthalten, müssen entsprechend gekennzeichnet werden. Über die Kennzeichnung soll einfach erkennbar sein, zu welcher Informationsklassifizierungsgruppe die Unterlagen gehören.
Klassifizierung von Informationen:

- **Öffentlich**: Daten sind für alle zugänglich, auch für Personen ausserhalb der Firma. Das Bekanntwerden der Informationen hat keine negativen Auswirkungen. Beispiele: Publikationen, Broschüren.
- **Intern**: Daten werden nur den eigenen Mitarbeitenden zugänglich gemacht. Das Bekanntwerden der Informationen kann einen geringen bis mittelgrossen Schaden verursachen. Beispiele: Preislisten, Prozessbeschreibungen, Organigramme.
- **Vertraulich**: Daten sind nur einer bestimmten Anzahl von Mitarbeitenden zugänglich. Das Bekanntwerden der Informationen kann einen grossen Schaden verursachen. Beispiele: Personaldaten, Kundenlisten, Kalkulationen.
- **Streng vertraulich**: Daten sind lediglich einer streng definierten Personengruppe zugänglich. Die Weitergabe dieser Daten kann für das Unternehmen existenzgefährdend sein. Beispiele: Entwicklungsdaten, Unternehmensstrategie.

Richtlinien zur Klassifizierung von Informationen nach **ISO/IEC 270001** finden Sie unter:
https://www.sec4you.com/klassifizierung-iso-27001/

☞ Checkliste:

- □ Festlegen, welche Klassifizierungen in Ihrem Unternehmen verwendet werden sollen.
- □ Word-/Excel-Vorlagen erstellen, in denen der Vertraulichkeitsstatus angegeben werden muss.

8. Vertrauliche (Telefon-)Gespräche

Es liegt in der Verantwortung des Arbeitsgebers die Privatsphäre der Mitarbeitenden und Kunden zu schützen. Stellen Sie sicher, dass vertrauliche Gespräche in einem **geschützten Raum** geführt werden können, ohne dass Informationen nach aussen gelangen.

Online sind Telefonboxen mit Glastür zu finden, die in einem Büro aufgestellt werden können.