ORGANISATION VON WERTEN (ASSETS)

1. Ordnungsgemäße Nutzung von Werten

Die Informationen, die sich auf den IT-Systemen befinden, müssen bestmöglich durch angemessene Maßnahmen geschützt werden. Dabei spielt die Identifizierung und Kennzeichnung von Assets eine bedeutende Rolle.

Die IT-Assets sollten ausschließlich für die betrieblich genehmigten Geschäftsprozesse genutzt werden. Es ist nicht gestattet, die IT-Assets unautorisiert zu ändern bzw. zu löschen. Zudem dürfen nur autorisierte und lizensierte Software bzw. Installationen auf den Systemen durchgeführt werden.

Daten von Kunden, Mitarbeitern, Geschäftspartnern und externen Dritten sind als besondere Assets einzustufen, welche eines zusätzlichen Schutzumfangs bedürfen. Dabei ist zu beachten, dass es nicht darauf ankommt, welchem Unternehmensbereich die Daten zugeordnet bzw. wo sie gespeichert oder verarbeitet werden.

2. Sicherheitsklassifizierung von Informationen

Die Sicherheitsklassifizierung von Informationen ist notwendig, damit bestimmt werden kann, welchen Schutzcharakter Informationen haben (z.B. vertraulich oder geheim).
Wenn Daten mit verschiedenen Sicherheitsklassifizierungsgraden betroffen sind, muss der höchste Sicherheitsklassifizierungsgrad für die verarbeitende Anwendung / das verarbeitende System gewählt werden.
Zur Gewährleistung der Informationssicherheit hinsichtlich der Vertraulichkeit, Verfügbarkeit und Integrität bietet es sich an, eine Klassifizierung festzulegen.
Im Rahmen dieser Klassifizierung bedeutet Vertraulichkeit, dass die Informationen nur für die berechtigten Personen zugänglich sind, Integrität, dass eine fehlerfreie Verarbeitung und der Schutz vor ungerechtfertigter Veränderung der Informationen sichergestellt werden und Verfügbarkeit, dass die Informationen zu einem bestimmten Zeitpunkt verfügbar sind.

3. Kategorisierung von Informationen

Um einschätzen zu können, welche Wertigkeiten bestimmte Informationen haben, sind die Daten in bestimmte Kategorien einzuteilen. Je nach Kategorie kann ein bestimmter Personenkreis festgelegt werden, welcher Zugriff auf die Daten erhält. Grundsätzlich ist das „need-to-now-Prinzip“

anzuwenden, demnach sind Informationen nur herauszugeben, wenn dies auch wirklich notwendig ist.

Klassifizierung	Bedeutung
Öffentlich	**Definition:** Diese Informationen sind der Öffentlichkeit bekannt und unterliegen keinen Restriktionen (z.B. Zeitungsbericht, Internetseite, Öffentliches Telefonbuch). Bevor Informationen veröffentlicht werden dürfen, bedarf dies der ausdrücklichen Zustimmung des Informationsverantwortlichen. **Kennzeichnung:** keine **Vervielfältigung und Weitergabe:** keine Einschränkungen **Speicherung:** keine Einschränkungen **Löschen/Entsorgung:** keine Einschränkungen
Intern	**Definition:** Diese Informationen sind nur für den unternehmensinternen Umlauf gedacht (z.B. dienstliche Kommunikationsdaten, Arbeitsanweisungen). Grundsätzlich kann eine Kenntnisnahme durch Unbefugte im Einzelfall zu Verletzungen der berechtigten Interessen führen (Schaden: gering). **Kennzeichnung:** Keine (oder als „Intern“) **Vervielfältigung und Weitergabe:** Weitergabe nur an berechtigte Personen innerhalb des Unternehmens bzw. an berechtigte Personen im Aufgaben- und Anwendungsbereich **Speicherung:** Schutz vor unberechtigter Einsichtnahme **Löschen/Entsorgung:** Nutzung der dafür vorgesehenen Löschungs- und Vernichtungsmaßnahmen
Vertraulich	**Definition:** Diese Informationen dürfen nur einem eingeschränkten Personenkreis mittgeteilt werden. Die Kenntnis durch Unbefugte oder deren missbräuchliche Verwendung kann sich negativ auf die unternehmerischen Ziele (z.B. Kunden- und Reputationsverlust, Schadensersatzansprüche) auswirken (Schaden: mittel). **Kennzeichnung:** „Vertraulich“ auf der ersten Seite des Dokuments in elektronischer und gedruckter Form **Vervielfältigung und Weitergabe:** Weitergabe nur an berechtigte Personen innerhalb des Unternehmens und an berechtigte Personen im Aufgaben- und Anwendungsbereich (begrenzter Personenkreis) Diese Daten bedürfen bei der Übermittlung eines hohen Schutzniveaus, d.h. dass nur geeignete Übertragungsmethoden gewählt werden dürfen z.B.

	verschlüsselte Verbindung beim E-Mail-Versand, kein Mithören von Telefonaten. **Speicherung:** Nur berechtigte Personen anhand der geschlossenen Benutzergruppen auf gesicherten Speicherorten und -medien **Löschen/ Entsorgung:** Nicht mehr benötigte Daten sind ordnungsgemäß zu löschen und zu entsorgen
Geheim	**Definitionen:** Diese Informationen unterliegen einem sehr hohen Schutzniveau und eine Kenntnisnahme von Unbefugte kann dazu führen, dass das Erreichen von unternehmensstrategischen Zielen nachhaltig gefährdet wird. Es ist dabei äußerst restriktiv an die unmittelbaren heranzuziehenden Personen herauszugeben und strikten Korntrollen zu unterziehen. Eine Verletzung kann dazu führen, dass das Unternehmen langfristig Schaden nimmt (z.B. Einbußen, massive Kundenverluste) (Schaden: hoch). **Kennzeichnung:** „Geheim“ auf jeder Seite des Dokuments in elektronischer und gedruckter Form **Vervielfältigung und Weitergabe:** Nur an einen äußerst begrenzten Personenkreis (z.B. namentliche Liste) mit Genehmigung des Informationsinhabers Die Dokumente sind auf dem aktuellen Stand der Technik zu verschlüsseln, sofern dies nicht vorgesehen ist, müssen andere technische und organisatorische Maßnahmen zum Schutz ergriffen werden (z.B. Wasserzeichen, Weitergabe- oder Druckverbot). **Speicherung:** Nur äußerst beschränkte Personen anhand der geschlossenen Benutzergruppen auf gesicherten Speicherorten und -medien **Löschen/ Entsorgung:** Nicht mehr benötigte Daten sind ordnungsgemäß zu löschen und zu entsorgen

Verantwortlich für die Kennzeichnung der Dokumente ist grundsätzlich der Ersteller. Wenn das Dokument nicht gekennzeichnet wurde, gilt es als internes Dokument, es sei denn, es ist offenkundig ein öffentliches Dokument (z.B. Pressemitteilung). Diese Regelungen gelten auch beim Umgang mit Daten auf IT-Systemen (z.B. Datenbanken, Festplatten).

Dokumente, die sich im Entwurfsstadium befinden, sind auch als Entwurf zu kennzeichnen (z.B. Entwurf, Versionsstand) bzw. die finalisierte Version ist als solche hervorzuheben.