**Arbeitsanweisung**

# Richtlinie für Informationssicherheit an Lieferanten_A.15

## Inhaltsverzeichnis

# 1. Zweck

## 1.1 Ausgangssituation

Die Unternehmensgruppe Welser Profile betreibt ein Informationssicherheits-managementsystem (ISMS). Dies verpflichtet die Unternehmensgruppe Welser Profile dazu Richtlinien, Verfahrensanweisungen und Arbeitsanweisungen zu definieren und zu dokumentieren welche in der DIN EN ISO 27001 im Anhang A.15 „Lieferanten-beziehungen“ beschrieben sind.

## 1.2 Ziel des Dokuments

Die vorliegende Richtlinie definiert Anforderungen an den Umgang mit Informationen und informationsverarbeitenden Einrichtungen.

# 2. Begriffe und Abkürzungen

| | |
|---|---|
| ***ISMS*** | Informationssicherheitsmanagementsystem |
| ***UB-IT*** | Unternehmensbereich Informationstechnologie |
| ***UWP*** | Unternehmensgruppe Welser Profile |

# 3. Geltungsbereich

Diese AA gilt für die Produktionsstandorte inkl. VNL der Unternehmensgruppe Welser Profile.

# 4. Zuständigkeiten

Die Zuständigkeiten sind im Kapitel 5 geregelt.

# 5. Beschreibung

## 5.1 Informationsklassifizierung

Alle Informationen der UWP, welche mit Externen ausgetauscht werden, sind bzgl. ihrer Vertraulichkeit klassifiziert. Dabei gilt folgende Einteilung:

| Vertraulichkeitsklasse | Beschreibung |
|---|---|
| Öffentlich | Die unberechtigte Offenlegung ist nicht möglich da für die Öffentlichkeit bestimmt. Kein Schaden möglich. |
| Intern | Die unberechtigte Offenlegung kann bis zu kleineren Schäden und Unannehmlichkeiten für die UWP führen |
| Vertraulich | Nur für einen bestimmten Personenkreis bestimmt. Es kann ein mittlerer Schaden bei Veröffentlichung entstehen. |
| Geheim | Nur für einen engen Personenkreis bestimmt. Es kann ein hoher Schaden entstehen, wenn diese Information öffentlich gemacht wird. |

Die Klassifizierung eines vertraulichen bzw. geheimen Dokumentes muss für den Verwender klar ersichtlich sein. Sollte eine Information nicht klassifiziert sein, ist sie so lange als UGW „interne“ Information zu behandelt, bis eine Klassifizierung durch den Informationseigentümer erfolgt ist.

Beim Zusammenführen von Informationen unterschiedlicher Vertraulichkeitsstufen gilt für die neue Information die höchste Stufe der Quellinformation.

Bei der Kennzeichnung von Informationen sind folgende Anforderungen sicherzustellen:

- Die Klassifizierung wird in der Regel durch eine Kennzeichnung in der Fußzeile vorgenommen.
- Emails mit vertraulichen und geheimen Inhalten müssen in der ersten Zeile gekennzeichnet werden. Weder Klassifikation noch Inhalte von Internen, Vertraulichen oder geheimen Informationen sollen in dem E-Mail-Titel inkludiert werden.

## 5.2 Anforderungen an den Umgang mit Informationen

Alle Informationen sind sorgsam und im Einklang mit dem Auftrag zu behandeln.

Externe müssen sicherstellen, dass sie im Umgang mit Informationen stets nach den, in dieser Richtlinie definierten, Minimalanforderungen handeln.

Sämtliche Informationen bleiben auch nach der Übertragung an Externe im Eigentum der UWP.

### 5.2.1 Speicherung, Übertragung und Vernichtung von Informationen

Die Speicherung und Übermittlung von Informationen muss entsprechend der nach folgenden Tabelle erfolgen:

| Information | klassifiziert als | | | |
|---|---|---|---|---|
| Aktion | öffentlich | intern | vertraulich | geheim |
| Speicherung (lokal, zentral, mobil) | unverschlüsselt | unverschlüsselt | unverschlüsselt *) | verschlüsselt |
| Versand (E-Mail, Filetransfer) | unverschlüsselt | unverschlüsselt | verschlüsselt | verschlüsselt (NUR durch den Informationseigen-tümer) |
| Druck | erlaubt | erlaubt | nur auf definierten Druckern **) | nur auf definierten Druckern **) |
| Fax | erlaubt | erlaubt | verboten | verboten |
| Veröffentlichen im Internet | erlaubt | verboten | verboten | verboten |
| Veröffentlichen im Intranet | erlaubt | erlaubt | erlaubt *) | verboten |

*) nur in geschützten Arbeitsräumen

**) definierte Drucker sind jene Geräte, die entweder in nicht allgemein zugänglichen Räumen (z.B. in den Räumen der Geschäftsleitung) stehen oder sich im direkten Sichtfeld des ausdruckenden Mitarbeiters befinden.

Bei der Speicherung von Informationen ist folgendes sicherzustellen:

- Information die auf Servern gespeichert werden, dürfen nur in die dafür vorgesehenen Laufwerke und Ordner abgelegt werden, um die Korrektheit der Zugriffsberechtigung zu gewährleisten.
- Für die Verschlüsselung sind nur Algorithmen aus dem Pkt. 5.3.6 zu verwenden.

Die Vernichtung von Informationen muss nach folgender Tabelle erfolgen:

| Klasse | Papier | Digitale Speichermedium |
|---|---|---|
| Öffentlich | Keine besonderen Vorkehrungen | |
| Intern | Shredder oder Reißwolf Container | mechanisch zerstören oder sicheres Löschen |
| Vertraulich | Schredder | |
| Geheim | | |

## 5.3 Anforderungen an den Umgang mit informationsverarbeitenden Einrichtungen

Alle informationsverarbeitenden Einrichtungen sind sorgsam zu behandeln.

Externe müssen sicherstellen, dass sie im Umgang mit informationsverarbeitenden Einrichtungen stets nach den, in dieser Richtlinie definierten, Minimalanforderungen handeln.

### 5.3.1 Teleworking und VPN

Bei der Verwendung von Teleworking und Remote Zugängen ist stets folgendes sicherzustellen:

- Der Externe muss sicherstellen, dass die externe Umgebung ausreichend geschützt ist, um unberechtigten Personen die Einsichtnahme zu verwehren.
- Der Externe muss sicherstellen, dass Aktivitäten unternommen werden um Shoulder Surfing präventiv entgegenzuwirken.

### 5.3.2 Umgang mit Benutzeraccounts

Externe müssen sicherstellen, dass keine Aktivitäten unternommen werden, die zu einem Missbrauch der digitalen Identität führen kann. Dazu zählen u.a.

- Weitergabe von Benutzerkonten und Passwörter
- Weitergabe von Zutrittskarten

### 5.3.3 Passwörter

Externe müssen sicherstellen, dass stets sichere Passwörter verwendet werden.

**Folgende Anforderungen sind bei der Wahl von Passwörtern stets zu befolgen:**

- Mindestlänge von 10 Zeichen
- Mindestens Zeichen aus drei der folgenden Gruppen: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen
- Keine Verwendung von persönlichen Informationen (Kontoname, Name, Geburtsdatum, Personalnummer, Durchwahlnummer)
- Keine Tastaturmuster (asdf, 1234) sowie Wörter aus Wörterbüchern

**Folgende Anforderungen sind beim Umgang mit Passwörtern stets zu befolgen:**

- Passwörter müssen geheim gehalten und nur vom zugehörigen Benutzer verwendet werden.
- Passwörter dürfen niemals an Unberechtigte offengelegt werden
- Bei Offenlegung oder dem Verdacht einer Offenlegung des Passwortes muss umgehend das Passwort erneuert und der Einkäufer der UGW informiert werden.
- Passwörter müssen mindestens alle 90 Tage geändert werden
- Das neue Passwort muss sich vom alten Passwort in mindestens 3 Zeichen unterscheiden
- Bei der Passwortwahl dürfen die letzten 5 Passwörter nicht verwendet werden
- Passwörter dürfen niemals notiert werden.
- Nach maximal 10 erfolglosen Anmeldeversuchen müssen Benutzerkonten gesperrt werden.
- Nach maximal 10 Minuten Inaktivität (= keine Benutzerinteraktion) muss der Bildschirm gesperrt und darf nur durch neuerliche Eingabe des Passwortes durch den Benutzer wieder aktiviert werden

### 5.3.4 Aufgeräumter Schreibtisch

Folgende Grundsätze sind stets zu befolgen:

- Beim Verlassen des Schreibtischs ist dafür zu sorgen, dass der Bildschirm des PC oder Laptops gesperrt ist.
- Auf dem Schreibtisch dürfen keine internen, vertraulichen oder geheime Dokumente verbleiben, wenn der Schreibtisch verlassen wird.
- Vertrauliche und geheime Dokumente sind stets versperrt aufzubewahren.

### 5.3.5 Nutzung privater Gerätschaften

Die Nutzung von privaten oder firmenfremden Gerätschaften zur Ausübung der Geschäftstätigkeit ist untersagt.

Die Nutzung und das Anstecken von privater IT-Ausrüstung (u.a. mobile Datenträger) an informationsverarbeitenden Einrichtungen/Gerätschaften oder das IT-Netzwerk ist untersagt.

### 5.3.6 Kryptographie

Folgende Algorithmen sind zulässig:

| Zulässige Algorithmen | Schlüssellänge |
|---|---|
| AES | 256 |
| RSA | 2048 |

Kryptographische Schlüssel sind geheim zu halten. E-Mails bzw. E-Mail Inhalte, welche lt. Pkt. 5.2 zu verschlüsseln sind, müssen entweder mit Hilfe von Outlook Zertifikaten verschlüsselt werden oder deren Inhalte in einem verschlüsselten ZIP Archiv gepackt sein.

### 5.3.7 Sicherheit der Endgeräte

**Technische Sicherheitsmaßnahmen**

Folgende technische Anforderungen sind sicherzustellen:

- Das Endgerät muss mit einem Betriebssystem ausgestattet sein, das von dem Hersteller aktuell unterstützt wird
- Das Endgerät muss mit aktuellen Updates versorgt und aktuell gehalten werden.
- Auf dem Endgerät muss eine Virenschutzsoftware installiert werden.
- Mobile Endgeräte muss mit einem zulässigen Verschlüsselungsverfahren vollverschlüsselt werden
- Das Endgerät muss eine Firewall aktiviert haben.
- Das Endgerät muss mit einem Passwort unter Einhaltung der Anforderungen aus Pkt. 5.3.3 geschützt werden.

**Organisatorische Sicherheitsmaßnahmen**

Folgender zulässige Gebrauch ist sicherzustellen:

- Das Endgerät ist stets sicher zu platzieren und vor Einsichtnahme Unberechtigter zu schützen.
- Das Endgerät darf nicht an unberechtigte Personen weitergegeben werden.
- Bei der Erstellung, Bearbeitung, Übermittlung und Löschung von Informationen ist stets die Regeln entsprechend der Informationsklassifizierung lt. Pkt. 5.1 zu befolgen.

### 5.3.8 Datensicherung

Externe müssen sicherstellen, dass Informationen adäquat gesichert werden.

Externe müssen die Datensicherung regelmäßig prüfen, indem Stichproben wieder-hergestellt werden.

### 5.3.9 Meldung von Sicherheitsvorfällen

Externe sind verpflichtet Sicherheitsvorfälle sofort zu melden.

Die Meldung erfolgt schriftlich an die Mailadresse 2000@welser.com oder telefonisch an die (+437443) 800-2000.

Externe sind verpflichtet bei der Analyse und Behebung von Sicherheitsvorfällen zu unterstützen.

### 5.4 Aufzeichnungen

| Bezeichnung | Dokumentation/ Speicherort | Zuständig | Aufbewahrung |
|---|---|---|---|
| Sicherheitsvorfälle | ITSM-Tool | IT Service Desk | 3 Jahre |

## 6. Änderungsdienst

Der Änderungsdienst dieser AA unterliegt der IT und ist nach Bedarf durchzuführen.

## 7. Umsetzungsverantwortliche

siehe Liste PMS-Umsetzungsverantwortliche

## 8. Mitgeltende Unterlagen

- DIN EN ISO 27001 Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen
- Liste der PMS-Umsetzungsverantwortlichen