

# Office365 Implementation im Unternehmen

## IT-Sicherheit

- Verfügbarkeit
  - Backup
  - Wiederherstellbarkeit
- Nutzerverwaltung
- Rechteverwaltung
- Verschlüsselung

## Datenschutz

- Zutrittskontrolle
  - AVV mit Microsoft / Standort in Europa
  - Unternehmensgeräte
  - BYOD
- Zugangskontrolle
  - Nutzerverwaltung
    - intern
    - extern
- Zugriffskontrolle
  - Berechtigungskonzept
    - intern
    - extern
  - können Nutzer eigenen Account auf anderen Geräten ohne IT anlegen?
- Eingabekontrolle
  - Nachvollziehbarkeit
- Weitergabekontrolle
  - Nachvollziehbarkeit
- Verfügbarkeitskontrolle
  - Backupsystem
  - Verschlüsselung
  - Gerätemanagement
- Trennungsgebot
  - keine private Verwendung
- Risikomanagement
  - Risikobewertung
  - Datenschutzvorfall
  - Auskunftersuchen
  - Berichtigung von Daten
  - Sperrung von Daten
  - Löschungskonzept
- Datenminimierung

## rechtliche Situation

- interne Benutzervorgaben
- Betriebsvereinbarung
- Informationspflicht gegenüber den Betroffenen
- Zusammenarbeit mit Dritten
  - wem gehören die Daten und Informationen?
- gesetzliche Aufbewahrungsfristen

## Verhalten Mitarbeiter

- Kommunikationstraining für Online Kommunikation
- Etikette leben
- Vorbildfunktion von GF

# Office365 Implementation im Unternehmen

## 1. IT-Sicherheit

### 1.1. Verfügbarkeit

#### 1.1.1. Backup

#### 1.1.2. Wiederherstellbarkeit

### 1.2. Nutzerverwaltung

### 1.3. Rechteverwaltung

### 1.4. Verschlüsselung

## 2. Datenschutz

### 2.1. Zutrittskontrolle

#### 2.1.1. AVV mit Microsoft / Standort in Europa

#### 2.1.2. Unternehmensgeräte

#### 2.1.3. BYOD

### 2.2. Zugangskontrolle

#### 2.2.1. Nutzerverwaltung

##### 2.2.1.1. intern

##### 2.2.1.2. extern

### 2.3. Zugriffskontrolle

#### 2.3.1. Berechtigungskonzept

##### 2.3.1.1. intern

##### 2.3.1.2. extern

#### 2.3.2. können Nutzer eigenen Account auf anderen Geräten ohne IT anlegen?

### 2.4. Eingabekontrolle

2.4.1. Nachvollziehbarkeit

2.5. Weitergabekontrolle

2.5.1. Nachvollziehbarkeit

2.6. Verfügbarkeitskontrolle

2.6.1. Backupsystem

2.6.2. Verschlüsselung

2.6.3. Gerätemanagement

2.7. Trennungsgebot

2.7.1. keine private Verwendung

2.8. Risikomanagement

2.8.1. Risikobewertung

2.8.2. Datenschutzvorfall

2.8.3. Auskunftersuchen

2.8.4. Berichtigung von Daten

2.8.5. Sperrung von Daten

2.8.6. Lösungskonzept

2.9. Datenminimierung

### **3. rechtliche Situation**

3.1. interne Benutzervorgaben

3.2. Betriebsvereinbarung

3.3. Informationspflicht gegenüber den Betroffenen

3.4. Zusammenarbeit mit Dritten

3.4.1. wem gehören die Daten und Informationen?

3.5. gesetzliche Aufbewahrungsfristen

### **4. Verhalten Mitarbeiter**

4.1. Kommunikationstraining für Online Kommunikation

4.2. Etikette leben

4.3. Vorbildfunktion von GF