# SecureIT GmbH

## Audit report on ISO 27001 and GDPR for Kook8 GmbH

### 1. Allgemeine Informationen

* Company: SecureIT GmbH
* Audit date: December 15, 2024
* Audit manager: Max Mustermann
* Audit team: Lisa Müller, Hans Meier, Sabine Klein
* Audit objective: Evaluation of conformity with ISO 27001 and GDPR
* Locations: Head office Berlin, branch office Munich

### 2. Summary of the Results

#### 2.1 Overview of the audited areas

* Information security management system (ISMS)
* Data processing and data protection
* Access controls
* Backup and recovery procedures
* IT asset management

#### 2.2 Festgestellte Konformität

* ISO 27001: 92% of the requirements fulfilled
* GDPR: 87% of the requirements fulfilled

#### 2.3 Positive Beobachtungen

* Robust access controls implemented.
* Regular employee training on data protection guidelines.
* Comprehensive and up-to-date documentation of the ISMS.

#### 3. Identifizierte Risiken

|  |  |  |  |
| --- | --- | --- | --- |
| Risk-ID | Description | Assessment | Relevant standard |
| R-001 | Lack of encryption of sensitive data on mobile devices | High | ISO 27001 Section A.10 |
| R-002 | Incomplete data protection impact assessments | Medium | DSGVO Art. 35 |
| R-003 | Outdated software in critical systems | High | ISO 27001 Section A.12 |

#### 4. Maßnahmenempfehlungen

|  |  |  |  |
| --- | --- | --- | --- |
| Risk-ID | Recommended measure | Priority | Responsible |
| R-001 | Implementation of encryption solutions on all devices | High | IT-Department |
| R-002 | Implementation of complete data protection impact assessments | Medium | Data Protection Officer |
| R-003 | Updating the software and monitoring versioning | High | IT Security Officer |

#### 5. Summary

Overall, the audit shows good compliance with the requirements of ISO 27001 and the GDPR. However, critical and medium risks were identified that need to be addressed to ensure compliance. It is recommended that the measures listed above be implemented within the next three months.

#### 6. Attachments

* Audit checklist
* Risk assessment scheme
* Training protocols