

# Anforderungs- katalog

## Trusted Application

Version: 2.0

Klassifizierung: öffentlich

**TÜV TRUST IT GmbH**  
Unternehmensgruppe TÜV AUSTRIA

Waltherstr. 49-51  
51069 Köln  
Tel. +49 (0)221 / 969789-0  
Fax +49 (0)221 / 969789-12  
[www.it-tuv.com](http://www.it-tuv.com)

**Ansprechpartner:**  
Manuel Münchhausen  
Tel. +49 (0)221 / 969789-71  
Fax +49 (0)221 / 969789-12  
Manuel.Muenchhausen@it-  
tuv.com

TÜV®

## 1 Geltungsbereich

Das vorliegende Dokument „Anforderungskatalog Trusted Application“ dient zur Darstellung der Basisanforderungen, die im Rahmen einer Überprüfung umgesetzt und eingehalten werden müssen.

Dieses Dokument basiert in seinen Grundlagen auf:

- ✓ ISO IEC 27001:2013 – „Informationssicherheitsmanagementsysteme – Anforderungen“
- ✓ ISO IEC 27033 „IT-Netzwerksicherheit“
- ✓ ISO IEC 27701 „Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz“
- ✓ relevante Anforderungen aus ITIL (IT Infrastructure Library)
- ✓ best practices des TÜV

Die Aspekte, die in diesem Anforderungskatalog beschrieben sind, wurden im Hinblick auf die Sicherheit von Online Applikationen ausgewählt, um ein adäquates Maß an Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität zu gewährleisten. Um sicherzustellen, dass das Vorgehen der Prüfung den Anforderungen an Online Applikationen gerecht wird, wurden die Prüfgrundlagen in drei Teile unterteilt:

- ✓ Allgemeine organisatorische Prüfung
- ✓ Technische Überprüfung der Applikation
- ✓ Überprüfung zur Beschaffung, Entwicklung und Wartung von Informationssystemen

Die Überprüfung stellt sicher, dass sowohl technische als auch organisatorische Aspekte bei der Prüfung und Zertifizierung berücksichtigt werden und somit für die Online Applikation das für den Nutzer erforderliche Maß an Sicherheit gewährleistet werden kann.

## 2 Anforderungen

### 2.1 Organisatorische Prüfung

Die organisatorischen Prüfungen der Prozesse und Verfahren und ihrer jeweiligen Umsetzung basieren auf ISO IEC 27001:2013. Hierzu werden Dokumentenprüfungen mit Interviews kombiniert, um ein möglichst umfassendes Bild zur Informationssicherheits-Organisation im Unternehmen zu erlangen. Die endgültige Prüfauswahl ist dabei je nach Schwerpunkt und Umfang der Prüfung zu treffen.

#### 2.1.1 Sicherheitsleitlinie (Security Policy)

Es muss eine Sicherheitsleitlinie vorhanden sein, als Richtungsvorgabe zur Unterstützung des Managements bei der Informationssicherheit, in Übereinstimmung mit Geschäftsanforderungen und geltenden Gesetzen und Regelungen.

#### 2.1.2 Organisation der Informationssicherheit

##### 2.1.2.1 Interne Organisation

Es müssen Regelungen zur Handhabung der Informationssicherheit innerhalb der Organisation vorhanden sein.

##### 2.1.2.2 Involvierte Externe/Dritte bei der Erstellung bzw. dem Betrieb der Applikation

Es sind Maßnahmen zur Aufrechterhaltung der Sicherheit von Informationen und der Sicherheit von informationsverarbeitenden Einrichtungen der Organisation, die von Externen benutzt oder verwaltet werden, die für diese zugänglich sind, oder die an Externe kommuniziert werden, zu treffen.

#### 2.1.3 Asset Management

##### 2.1.3.1 Verantwortung für Assets bezogen auf die Erstellung bzw. den Betrieb der Applikation

Es müssen Maßnahmen zum Erreichen und zur Erhaltung des angemessenen Schutzes von organisationseigenen Werten (Assets) umgesetzt sein.

## **2.1.4 Personalsicherheit**

### **2.1.4.1 Vor der Anstellung**

Es ist sicher zu stellen, dass Angestellte, Auftragnehmer und Dritte ihre Verantwortlichkeiten verstehen und für die vorgesehenen Aufgaben geeignet sind, um die Risiken durch Diebstahl, Betrug oder Missbrauch von Einrichtungen zu verringern.

### **2.1.4.2 Während der Anstellung**

Es ist zu gewährleisten, dass Angestellte, Auftragnehmer und Dritte die Informationssicherheitsbedrohungen und -bedenken sowie ihre Verantwortlichkeiten und Pflichten kennen und die organisationseigene Sicherheitsleitlinie bei ihrer normalen Arbeit befolgen, um das Risiko von menschlichen Fehlern zu reduzieren.

### **2.1.4.3 Beendigung der Anstellung**

Es ist zu gewährleisten, dass Administratoren, Nutzer und Dritte die Organisation ordnungsgemäß verlassen oder Berechtigungen entsprechend den jeweiligen Erfordernissen wechseln.

## **2.1.5 Physische und umgebungsbezogene Sicherheit**

### **2.1.5.1 Sicherheitsbereiche**

Es sind Maßnahmen zum Schutz vor unerlaubtem Zutritt zu und Beschädigung und Störung von Organisationsinfrastruktur und der Organisation gehörenden Informationen zu treffen.

### **2.1.5.2 Sicherheit von Betriebsmitteln**

Es sind Maßnahmen zur Verhinderung des Verlusts, der Beschädigung, des Diebstahls oder der Kompromittierung von organisationseigenen Werten (Assets) und Unterbrechung der Aktivitäten einer Organisation zu treffen.

## **2.1.6 Betriebs- und Kommunikationsmanagement**

### **2.1.6.1 Verfahren und Verantwortlichkeiten**

Es sind Maßnahmen zur Sicherstellung des korrekten und sicheren Betriebs der informationsverarbeitenden Einrichtungen zu treffen.

### **2.1.6.2 Management der Dienstleistungserbringung von Dritten**

Es sind Maßnahmen zur Umsetzung und Aufrechterhaltung eines angemessenen Grads an Informationssicherheit und Dienstleistungserbringung zu treffen, in Übereinstimmung mit den Liefervereinbarungen mit Dritten.

### **2.1.6.3 Systemplanung und Abnahme**

Es sind Maßnahmen zur Minimierung der Risiken von Systemfehlern und Systemausfällen zu treffen.

### **2.1.6.4 Schutz vor Schadsoftware und mobilem Programmcode**

Es sind Maßnahmen zum Schutz der Integrität von Software und Informationen zu treffen.

### **2.1.6.5 Datensicherung / Backup**

Es sind Maßnahmen zur Erhaltung der Integrität und der Verfügbarkeit von Informationen und informationsverarbeitenden Einrichtungen zu treffen.

### **2.1.6.6 Handhabung von Speicher- und Aufzeichnungsmedien**

Es sind Maßnahmen zu treffen, um die unerlaubte Veröffentlichung, Veränderung, Entnahme oder Zerstörung von Informationen als organisationseigenen Werten (Assets) und daraus folgende Störungen des Geschäftsbetriebs zu verhindern.

### **2.1.6.7 Austausch von Informationen**

Es sind Maßnahmen zum Erhalt der Sicherheit von Informationen und Software, die innerhalb einer Organisation oder mit Externen ausgetauscht werden, zu treffen.

### **2.1.6.8 Überwachung / Monitoring beim Betrieb der Applikation**

Es sind Maßnahmen zur Aufdeckung nicht genehmigter informationsverarbeitender Aktivitäten zu treffen.

## **2.1.7 Zugangskontrolle**

### **2.1.7.1 Geschäftsanforderungen für Zugangskontrolle**

Es sind Maßnahmen zur Kontrolle von Zutritt und Zugang zu Informationen und des Zugriffs auf Informationen zu treffen.

#### **2.1.7.2 Benutzerverwaltung**

Es sind Maßnahmen zu treffen, um befugten Benutzern den Zugang zu Informationssystemen zu sichern und unbefugten Zugang zu Informationssystemen zu verhindern.

#### **2.1.7.3 Benutzerverantwortung**

Es sind Maßnahmen zur Verhinderung von unbefugtem Benutzerzugriff, Kompromittierung und Diebstahl von Informationen und informationsverarbeitenden Einrichtungen zu treffen.

#### **2.1.7.4 Mobile Computing und Telearbeit**

Es sind Maßnahmen zu treffen, um die Informationssicherheit bei der Benutzung von Einrichtungen für mobile Computing und Telearbeit zu wahren.

### **2.1.8 Umgang mit Informationssicherheits-Vorfällen**

#### **2.1.8.1 Umgang mit Vorfällen**

Es sind Maßnahmen zu treffen, um die Anwendung eines einheitlichen und effektiven Ansatzes für den Umgang mit IS-Vorfällen zu gewährleisten.

### **2.1.9 Sicherstellung des Betriebs (ITSCM)**

#### **2.1.9.1 Sicherstellung des Geschäftsbetriebs**

Es sind Maßnahmen zum Schutz vor Unterbrechungen von Geschäftsaktivitäten zu treffen und um kritische Geschäftsprozesse vor den Auswirkungen größerer Störungen von Informationssystemen oder vor Katastrophen zu schützen und ihre rechtzeitige Wiederaufnahme sicherzustellen.

### **2.1.10 Einhaltung von Vorgaben (Compliance)**

#### **2.1.10.1 Einhaltung allgemeiner rechtlicher Vorgaben**

Es sind Maßnahmen zur Vermeidung von Verstößen gegen Gesetze, amtliche oder vertragliche Verpflichtungen und gegen jegliche

Sicherheitsanforderungen zu treffen. Vorgaben aus anwendungsspezifischen Regelungen sind eingeschlossen.

#### **2.1.10.2 Einhaltung von Sicherheitsregelungen und -standards, und technischen Vorgaben**

Es sind Maßnahmen zu treffen, um sicherzustellen, dass Systeme die organisationsweiten Sicherheitsregelungen und –standards einhalten.

#### **2.1.10.3 Datenschutz und Geheimhaltung personenbezogener Informationen**

Es sind Maßnahmen zu treffen, um die Verarbeitung personenbezogener Informationen angemessen zu schützen. Die Vorgaben aus dem jeweils anzuwendenden Recht und aus anwendungsspezifischen Regelungen sind zu beachten.

## **2.2 Datenschutzmanagement**

### **2.2.1 Organisation des Datenschutzes**

Es sollte ein hinreichend qualifizierter Beauftragter für den Datenschutz vorhanden sein, um eine lückenlose Überwachung und Umsetzung von Anforderungen sicherzustellen. Vorhandene Revisionsprozesse sollten berücksichtigt werden.

### **2.2.2 Organisatorische Einbindung des Datenschutzbeauftragten**

Der Beauftragte für den Datenschutz sollte wirksam und effektiv in die Betriebsprozesse eingebunden sein. Qualifikation und ausreichende Ressourcen sind bei gleichzeitiger Vermeidung von Interessenkonflikten zu gewährleisten.

### **2.2.3 Schulung / Training / Awareness**

Mitarbeiter sind regelmäßigen Basisschulungen zu unterziehen und auf einen ausreichenden Kenntnisstand zu prüfen. Das Schulungsangebot sollte regelmäßig auf seine inhaltliche Tauglichkeit und Effizienz überprüft werden.

### **2.2.4 Richtlinien/Policies**

Es sollte eine übergeordnete Richtlinie zum Datenschutz existieren, die hinreichend

kommuniziert wird und allen Mitarbeitern jederzeit zur Verfügung steht. Die Inhalte der Richtlinie sind in Arbeitsanweisungen zu berücksichtigen.

### **2.2.5 Change Management**

Änderungen an Anforderungen der Informationssicherheit und des Datenschutzes sollten über wirksame Prozesse identifiziert, analysiert und bewertet werden. Eine Umsetzung erforderlicher Änderungen sollte per Kopplung an Change- und Incident Management für die vorhandenen und neu entstehenden Prozesse berücksichtigt werden.

### **2.2.6 Handhabung von personenbezogenen Informationen**

Zu personenbezogenen Informationen, die durch das Unternehmen erhoben, verarbeitet oder genutzt werden müssen Angaben darüber dokumentiert werden, woher diese Informationen stammen, zu welchem Zweck sie erhoben und an wen sie weitergegeben wurden.

### **2.2.7 Betroffenenrechte**

Es sind Verfahren zu treffen, um Betroffenen Auskunft über die zu Ihnen gespeicherten personenbezogenen Informationen zu erteilen. Stellen sich Informationen als unrichtig heraus, so sind sie zu korrigieren. Auf Anfrage Betroffener sind Informationen zu löschen bzw. zu sperren, sofern eine Löschung aus z.B. regulatorischen Gründen nicht möglich ist.

### **2.2.8 Dokumentationsanforderungen**

#### **2.2.8.1 Allgemeine Dokumentation**

Für den Datenschutz relevante Prozesse müssen etabliert und hinreichend dokumentiert sein. BCM und Risikomanagement sind zu berücksichtigen.

#### **2.2.8.2 Dokumentation der technisch-organisatorischen Maßnahmen**

Die getroffenen technisch-organisatorischen Maßnahmen sind angemessen zu dokumentieren.

### **2.2.8.3 Verarbeitungsverzeichnis**

Für Verfahren, in denen personenbezogene Daten verarbeitet werden, sind Verarbeitungsverzeichnisse durch den Datenschutzbeauftragten zu führen.

### **2.2.9 Technisch-Organisatorische Maßnahmen**

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen werden geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

#### **2.2.9.1 Pseudonymisierung und Verschlüsselung personenbezogener Daten**

Pseudonymisierung und Verschlüsselung werden, sofern keine Ausschlussgründe vorliegen, im produktiven Betrieb wie auch im Bereich von Test und Entwicklung eingesetzt, unter Berücksichtigung des Stands der Technik. Die Verfahren sind nachvollziehbar dokumentiert.

#### **2.2.9.2 Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit**

Zugang, Zutritt und Zugriff sind angemessen zu schützen. Die Weitergabe von Daten und die Datenveränderung dürfen nur unter geregelten Bedingungen und im Rahmen definierter Berechtigungen erfolgen. Der Zugang zu IT-Systemen ist angemessen zu schützen. Es sind Authentisierungsmaßnahmen festzulegen.

#### **2.2.9.3 Wiederherstellbarkeit der Verfügbarkeit**

Es sollten Konzepte für Notfälle, Wiederanlaufverfahren und Ausweichmöglichkeiten im Falle eines Störfalls existieren, dokumentiert und erprobt sein.

#### **2.2.9.4 Weitergabekontrolle**

Übermittlungs- und Übertragungswege sowie die jeweiligen Verantwortlichkeiten und Befugnisse sind hinreichend zu bestimmen. Dies umfasst die Art der Übermittlung und getroffene Schutzmaßnahmen.

#### **2.2.9.5 Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen**

Die getroffenen Maßnahmen sind regelmäßig hinsichtlich ihrer Wirksamkeit zu überprüfen, um unter Berücksichtigung der Entwicklung des Stands der Technik einen andauernden Schutz personenbezogener Daten zu gewährleisten.

#### **2.2.10 Auftragsverarbeitung**

Bei Einsatz von Dienstleistern zur Verarbeitung personenbezogener Daten sind die vertraglich festgelegten Weisungs- und Kontrollbefugnisse und Pflichten vertraglich gemäß den gesetzlichen Vorgaben zu fixieren und durch entsprechende Prozesse umzusetzen. Der Auftraggeber hat sich vor Auftragserteilung und sodann regelmäßig von der Einhaltung der vereinbarten Maßnahmen zu überzeugen.

### **2.3 Technische Prüfung**

Die technischen Analysen bzgl. der Infrastruktur sollen sicherstellen, dass sowohl der Aufbau als auch der Betrieb dieser sensiblen IT-Infrastruktur den sicherheitstechnischen Anforderungen auf einem hinreichenden Niveau genügt. Die Anforderungen, die an dieser Stelle spezifiziert sind, wurden aus internationalen Standards wie ISO 18028, aus Anforderungen des PCIDSS V2.0, der OSSTMM, der OWASP und den Best Practices der Sicherheitsindustrie und der TÜV TRUST IT abgeleitet. Die endgültige Prüfauswahl ist je nach Schwerpunkt und Umfang der Prüfung zu treffen.

#### **2.3.1 Anforderungen an Netzwerke**

Es müssen dokumentierte Konzepte, Richtlinien und Verfahrensanweisungen für das Netzwerkmanagement vorhanden sein

(Zugriffskontrolle, Zugänge, Segmentierung, Routing, Logging, etc.).

#### **2.3.2 Anforderungen an Firewall Systeme**

Die Übergänge zu nicht vertrauenswürdigen Netzen sind durch Firewalls abzusichern. Ein Firewall-Management muss etabliert sein.

#### **2.3.3 Systemhärtung**

Es sind technische Maßnahmen zu treffen, um mittels Härtung die Stabilität und Sicherheit von IT-Systemen zu gewährleisten und zu verbessern. Die Konfiguration ist zu dokumentieren. Regelmäßige Audits sind einzuplanen.

#### **2.3.4 Schutz von gespeicherten Informationen**

Es sind technische Maßnahmen zu treffen, um die in Systemen oder Applikationen zu speichernden Informationen hinsichtlich ihrer Schutzbedarfe zu definieren und die abgespeicherten Daten zu schützen.

#### **2.3.5 Benutzerverwaltung**

Systemweit dürfen nur sichere User Logins Verwendung finden und User müssen über eine eindeutige Kennung verfügen. Bei sensiblen Systemen muss der Zugriff auf ein Minimum an berechtigten Personen limitiert sein. Änderungen an den Berechtigungen müssen geloggt werden.

#### **2.3.6 Entwicklung und Betrieb sicherer Applikationen**

Es ist eine Analyse des Quellcodes von Eigenentwicklungen durchzuführen, um eventuelle Sicherheitslücken zu identifizieren und insbesondere allgemeine Programmierfehler zu vermeiden.

#### **2.3.7 Anforderungen an die Administration von Infrastrukturen.**

Es sind Maßnahmen zum Management der erweiterten und privilegierten Rechte von Administratoren zu ergreifen.

### **2.3.8 Anforderungen an Systemüberwachung (Monitoring)**

Es sind Maßnahmen zu treffen, um Logging-Mechanismen und die Verfolgung von Benutzeraktivitäten nachvollziehbar zu ermöglichen.

## **2.4 Überprüfung zur Beschaffung, Entwicklung und Wartung**

Folgende Themengebiete sind für die Prüfung nach „Trusted Application“ zu berücksichtigen und stellen spezifische Anforderungen an Beschaffung, Entwicklung und Wartung von Informationssystemen dar. Die endgültige Prüfauswahl ist je nach Schwerpunkt und Umfang der Prüfung zu treffen.

### **2.4.1 Analyse und Spezifikation der Sicherheitsanforderungen**

Es sollten Maßnahmen ergriffen werden, um die Anforderungen an Sicherheitsmaßnahmen für neue Informationssysteme oder Erweiterungen bestehender Informationssysteme zu spezifizieren. Wirtschaftliche Faktoren sind zu berücksichtigen.

### **2.4.2 Validierung der Eingabedaten**

Daten, die in Anwendungen eingegeben werden, sollten validiert werden, um sicherzustellen, dass diese Eingaben korrekt und passend sind.

### **2.4.3 Validierung der Ausgabedaten**

Die Datenausgabe einer Anwendung sollte validiert werden, um sicherzustellen, dass die Verarbeitung der gespeicherten Informationen korrekt und den Umständen angemessen erfolgt ist.

### **2.4.4 Maßnahmen für Software in Produktionssystemen**

Es sind Maßnahmen zur Kontrolle der Installation von Software in Produktionssystemen zu treffen. Das Risiko von Störungen an Produktionssystemen ist auf ein Mindestmaß zu reduzieren.

### **2.4.5 Schutz von Systemtestdateien**

Es sind Verfahren zur sorgfältigen Auswahl, zur angemessenen Handhabung, zum Schutz und zur Kontrolle von Systemtestdaten einzusetzen.

### **2.4.6 Zugriffskontrolle zu Programm-Quellcode**

Es sind strenge Kontrollen des Zugriffs auf Programm-Quellcode und zugehörige Elemente durchzuführen, um die Einführung nicht genehmigter Funktionen zu verhindern und unabsichtliche Änderungen zu vermeiden.

### **2.4.7 Änderungskontroll-Verfahren**

Die Einführung neuer Systeme und größere Änderungen an bestehenden Systemen sollten einen formalen Prozess der Dokumentation, der Spezifizierung, des Testens, der Qualitätskontrolle und der Implementierung umfassen. Eine Bewertung der entstehenden Risiken, der Auswirkungen und der erforderlichen Maßnahmen ist einzuschließen. Änderungen sind im Rahmen von Änderungskontrollverfahren zu berücksichtigen.

### **2.4.8 Ausgelagerte Softwareentwicklung**

Ausgelagerte Softwareentwicklung sollte in Vereinbarungen hinreichend spezifiziert sein. Kontroll- und Auditverfahren, Qualitätsanforderungen und Anforderungsmanagement sind zu berücksichtigen.

### **2.4.9 Maßnahmen in Bezug auf technische Schwachstellen**

Ein Management technischer Schwachstellen sollte implementiert werden, das auf effektive, systematische und wiederholbare Weise, mit Maßnahmen zur Bestätigung seiner Wirksamkeit, arbeitet. Incident- und Problemmanagement sind zu berücksichtigen.