|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Entwicklung und Einsatz von Individualsoftware"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300005 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc78733775)

[Dokumentenhistorie 3](#_Toc78733776)

[Inhaltsverzeichnis 4](#_Toc78733777)

[Allgemeine Festlegungen 5](#_Toc78733778)

[Ziel / Zweck 5](#_Toc78733779)

[Geltungsbereich 6](#_Toc78733780)

[Zuständigkeiten 6](#_Toc78733781)

[Genehmigungs- und Änderungsverfahren 6](#_Toc78733782)

[Aufbau des Dokuments 6](#_Toc78733783)

[Sicherheitsrichtlinie "Entwicklung und Einsatz von Individualsoftware" 8](#_Toc78733784)

[Basismaßnahmen 8](#_Toc78733785)

[Festlegung benötigter Sicherheitsfunktionen der Fachanwendung (CON.5.A1) 8](#_Toc78733786)

[Test und Freigabe von Fachanwendungen (CON.5.A2) 8](#_Toc78733787)

[Sichere Installation einer Fachanwendung (CON.5.A3) 8](#_Toc78733788)

[Heranführen von Nutzerinnen und Nutzern an die Anwendung (CON.5.A4) 9](#_Toc78733789)

[Sicherer Betrieb einer Fachanwendung (CON.5.A5) 9](#_Toc78733790)

[Standardmaßnahmen 9](#_Toc78733791)

[Umfassende Dokumentation der Anforderungen an die Anwendung (CON.5.A6) 9](#_Toc78733792)

[Erstellung eines Mandantenkonzeptes (CON.5.A7) 9](#_Toc78733793)

[Geeignete Steuerung der Anwendungsentwicklung (CON.5.A8) 10](#_Toc78733794)

[Außerbetriebnahme von Anwendungen (CON.5.A9) 10](#_Toc78733795)

[Notfallvorsorge für Anwendungen (CON.5.A10) 10](#_Toc78733796)

[Maßnahmen bei erhöhtem Schutzbedarf 10](#_Toc78733797)

[Geeignete und rechtskonforme Beschaffung (CON.5.A11 - CIA) 11](#_Toc78733798)

[Treuhänderische Hinterlegung (CON.5.A12 - CA) 11](#_Toc78733799)

[Entwicklung eines Redundanzkonzeptes für Anwendungen (CON.5.A13 - A) 11](#_Toc78733800)

[Mehrschichtige Netzwerkarchitektur (CON.5.bd.A1 - CIA) 11](#_Toc78733801)

[Anwendungssegmentierung (CON.5.bd.A2 - CIA) 12](#_Toc78733802)

# Allgemeine Festlegungen

## Ziel / Zweck

Die <Institution> steht vor der Herausforderung das Standardsoftware die benötigten Anforderungen für die Digitalisierung von Prozessen durch SaaS-Lösung und auch vereinzelt für die Office-IT nicht mehr hinreichend erfüllen können. Die mit diesen Herausforderungen verbundenen Aufgabenstellungen bedürfen somit Softwarelösungen, die auf die individuellen Bedürfnisse der <Institution> zugeschnitten sind, im Folgenden Individualsoftware genannt.

Hierzu können einerseits Basislösungen, die aus einer Grundmenge an typischen Funktionen bestehen, eingesetzt und individualisiert werden. Die Grundfunktionen werden hierbei für den individuellen Einsatzzweck der <Institution> angepasst und um individuell benötigte Funktionen erweitert. Gängige Beispiele hierfür sind IT-Anwendungen wie ERP- (Enterprise Resource Planning), CMS- (Content Management Systeme), DMS (Document Management System) oder IDM-Systeme (Identity Management). Individualsoftware kann auch vollständig neu von der <Institution> selbst oder von Dritten (externe Dienstleister) entwickelt werden.

Von essentieller Bedeutung ist es hierbei, dass bereits bei der Planung und Konzeptionierung der Individualsoftware auch die benötigten Sicherheitsfunktionen bedacht werden und die Informationssicherheit, der Datenschutz und das Notfallmanagement in dem gesamten Lebenszyklus der Individualsoftware berücksichtigt wird. Fehler in der Planung oder fehlende Sicherheitsfunktionen oder Abhängigkeiten bei der Wiederherstellung können im laufenden Betrieb nicht oder nur mit hohem zusätzlichem Aufwand ausgeglichen werden. Hieraus ableitend sind die vier folgenden Grundsätze bei der Entwicklung von Software oder Erweiterung von Funktionen zu beachten.

**Security-By-Design:** Die Anwendung und seine Einzelkomponenten sind von Grund auf im Hinblick auf Sicherheit entwickelt. Vorsätzliche Angriffe und unberechtigte Handlungen werden explizit betrachtet, die Auswirkungen von Sicherheitsvorfällen werden durch das Anwendungsdesign minimiert.

**Minimal-Need-To-Know-Prinzip:** Jede Komponente und jeder Benutzer erhält nur die Rechte, die für die Ausführung einer Aktion notwendig sind. So werden z. B. Anwendungen, System und Netzwerk-Dienste nicht mit Administratorprivilegien, sondern nur mit den minimal nötigen Rechten betrieben.

**Defence-In-Depth Prinzip:** Sicherheitsrisiken werden nicht durch einzelne Schutzmaßnahmen angegangen, sondern durch die Implementierung gestaffelter, auf mehreren Ebenen ansetzender und sich ergänzender Sicherheitsmaßnahmen begrenzt.

**Redundanz-Prinzip:** Die Anwendung ist so ausgelegt, dass der Ausfall einzelner Komponenten die sicherheitsrelevanten Funktionen nicht beeinträchtigt. Das Anwendungsdesign verringert die Wahrscheinlichkeit und die Auswirkungen von Problemen, die durch das uneingeschränkte Anfordern von Ressourcen oder Netzwerkbandbreite entstehen.

Ziel dieser Sicherheitsrichtlinie ist es aufzuzeigen, welche grundlegenden Sicherheitsanforderungen bei der Planung, Beschaffung und Inbetriebnahme sowie im regulären Betrieb und bei der Außerbetriebnahme von Individualsoftware zu berücksichtigen sind. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben der BSI Bausteine CON.5 "Entwicklung und Einsatz von Individualsoftware" zurückgegriffen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Das Dokument "Sicherheitsrichtlinie Entwicklung und Einsatz von Individualsoftware“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie "Entwicklung und Einsatz von Individualsoftware"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Festlegung benötigter Sicherheitsfunktionen der Fachanwendung (CON.5.A1)

Für die Fachanwendung müssen die notwendigen Sicherheitsfunktionen bei der fachlichen Auswahl und der Integration in die IT-betrieblichen Infrastrukturen und Betriebsprozesse berücksichtigt werden.

Die Auswahl und Umsetzung geeigneter Sicherheitsfunktionen in der Fachanwendung erfolgt auf Grundlage der Informationen, die in der Anwendung verarbeitet werden, und gegebenenfalls einer zusätzlichen Risikoanalyse.

Die Sicherheitsfunktionen sind durch die Verantwortlichen für die Anwendung bzw. dem übergeordneten Prozess zu dokumentieren und mit dem <Informationssicherheitsbeauftragter> abzustimmen.

### Test und Freigabe von Fachanwendungen (CON.5.A2)

Innerhalb der <Institution> sind geeignete Vorgehensweisen für Test und Freigabe von Fachanwendungen mit unterschiedlichen betrieblichen und sicherheitstechnischen Anforderungen etabliert. Dabei wurden folgende Ebenen berücksichtigt:

* Die prozessuale Ebene vertreten durch den Verfahrensverantwortlichen
* Die Ebene des IT-Betriebes
* Die Ebene der Informationssicherheit
* Die Ebene des Datenschutzes
* Die Ebene des Notfallmanagements
* Die Ebene des Personalrechtes
* Je nach Art und Komplexität einer Anwendung weitere Funktionsträger

### Sichere Installation einer Fachanwendung (CON.5.A3)

Für jede Installation einer Fachanwendung werden Installationsanweisungen für das automatische Deployment erstellt. Diese beinhalten alle benötigten Anwendungsmodule (Bibliotheken), die Installationsreihenfolge und Konfiguration der Anwendungsmodule. Zusätzlich berücksichtigen die Installationsanweisungen die notwendigen Aspekte hinsichtlich der Installationsumgebung PaaS (bspw. AWS, GCP, Azure, O365) IaaS (bspw. AWS, GCP, Azure, 1und1). Ebenfalls wird in der Installationsanweisung berücksichtigt, ob die Anwendungskomponenten dem Prinzip der Mikrosegmentierung unterliegen und ob die Bereitstellung auf Basis von Containern, Hardwarevirtualisierung oder Serverless erfolgt.

Alle Fachanwendungen werden gemäß den Installationsanweisungen installiert. Bei Änderungen in der Anwendung und funktionalen Updates werden die Installationsanweisungen zeitnah mit angepasst.

### Heranführen von Nutzerinnen und Nutzern an die Anwendung (CON.5.A4)

Alle Nutzer und Administratoren werden zur korrekten Nutzung und Administration der Anwendung geschult. Die Schulungen berücksichtigen auch die Sicherheitsfunktionen der einzelnen Fachanwendungen. Den Mitarbeitenden werden Richtlinien und Arbeitsanweisungen zur Nutzung und Administration der Anwendung, Schulungen und Einweisungen, Handbücher und Online-Hilfen sowie eine Benutzerunterstützung durch Schlüsselanwender angeboten.

### Sicherer Betrieb einer Fachanwendung (CON.5.A5)

Alle Berechtigungen zur Nutzung und Administration werden korrekt und nach dem „Need-to-know-Prinzip“ vergeben und regelmäßig auf ihre Korrektheit hin überprüft. Nicht mehr benötigte Berechtigungen werden den Mitarbeitenden entzogen und der Entzug dokumentiert.

Es wird sichergestellt, dass die Protokolldaten regelmäßig ausgewertet und gesetzlich vorgegebene Speicherfristen eingehalten werden.

Sicherheitskritische Patches und Updates werden auf Grundlage der vertraglichen Vereinbarungen durch den Hersteller bzw. die <Institution> bereitgestellt. Diese werden zeitnah eingespielt. Alle Patches und Updates werden zuvor getestet und freigegeben.

Es finden regelmäßige Datensicherungen und Rücksicherungsübungen statt.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Umfassende Dokumentation der Anforderungen an die Anwendung (CON.5.A6)

Alle relevanten Anforderungen an die Anwendung werden dokumentiert. Die Dokumentation wird bei Änderungen an der Anwendung sowie funktionalen Updates aktualisiert.

### Erstellung eines Mandantenkonzeptes (CON.5.A7)

Seitens der <Institution> ist für alle für Dritte bereitgestellten Lösungen ein Mandantenkonzept zu erstellen und deren Implementierung sicherzustellen, so dass die Daten und Zugänge verschiedener Kunden sauber getrennt betrieben werden. Insofern durch einen Dienstleister eine Lösung für die <Institution> bereitgestellt wird, ist durch den Dienstleister ein entsprechendes Mandantenkonzept zu erstellen und der <Institution> zu übergeben. Die benötigten Mechanismen zur Mandantentrennung bei den Dienstleistern werden bei der Infrastrukturumsetzung mit berücksichtigt.

### Geeignete Steuerung der Anwendungsentwicklung (CON.5.A8)

Für die Anwendungsentwicklung werden geeignete Modelle für die Steuerung und zum Projektmanagement verwendet. Dieses sollte die folgenden Aspekte berücksichtigen:

* Das für die Entwicklung vorgesehene Personal verfügt über die notwendige Qualifizierung.
* Für die Steuerung der Erstellung und Pflege der Anwendungen wird ein Gesamtprozess eingeführt, der alle Phasen des Lebenszyklus (Application Lifecycle Management (ALM)) abdeckt.
* Zur geordneten Durchführung des Anwendungsprojektes werden die benötigten Voraussetzungen geschaffen. Die Rollen im beschriebenen Gesamtprozess besetzt. Die Auswahl eines Vorgehensmodells für die Entwicklung der Anwendung vorgenommen, welches für die <Institution> sowie die Art und Größe des Softwareprojektes am besten geeignet ist. Mögliche Vorgehensmodelle können sein, das evolutionäre Vorgehen, das iterative Vorgehensmodelle, die inkrementelle Entwicklung oder die rekursive System-Entwicklung.
* Die Risiken bei der Softwareentwicklung sind zu bewerten und zu behandeln. Hierbei sind spezifische Sicherheitsrisiken zu berücksichtigen, die üblicherweise durch Einsatz von Sicherheitsfunktionen reduziert werden.
* Es müssen die Qualitätsaspekte des Entwicklungsprozesses ausreichend berücksichtigt werden, die auch für die Gesamtsicherheit wichtig sind.

### Außerbetriebnahme von Anwendungen (CON.5.A9)

Jede Außerbetriebnahme von Anwendungen wird geplant und folgt den Vorgaben der Sicherheitsrichtlinie „Löschen und Vernichten von Informationen“.

Es wird für alle Daten der Fachanwendung geklärt, welche Daten migriert, aufgehoben oder gelöscht werden. Vertraglich oder gesetzlich nicht mehr benötigte vertrauliche Daten werden sicher gelöscht. Die Außerbetriebnahme wird nachvollziehbar dokumentiert.

### Notfallvorsorge für Anwendungen (CON.5.A10)

Insofern die Lösung Bestandteil eines geschäftskritischen Prozesses ist, werden die Fachanwendungen in die Planung zur Notfallvorsorge der <Institution> aufgenommen.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Geeignete und rechtskonforme Beschaffung (CON.5.A11 - CIA)

Bei der Beschaffung von Fachanwendungen werden die bestehenden rechtlichen und organisatorischen Vorgaben umgesetzt. Werden Dienstleister einbezogen, werden in den Verträgen die relevanten Sicherheitsaspekte berücksichtigt.

In der <Institution> sollten definierte Prozesse und festgelegte Ansprechpartner existieren. Diese Verantwortlichen müssen die Berücksichtigung der jeweiligen Rahmenbedingungen sicherstellen.

### Treuhänderische Hinterlegung (CON.5.A12 - CA)

Für geschäftskritische Anwendungen wird geprüft, ob eine Absicherung gegen Ausfall des Herstellers nötig ist. Dabei wird die treuhänderische Hinterlegung von nicht zum Lieferumfang der Anwendung gehörenden Materialien bei einer Escrow-Agentur erwogen. In diesem Fall werden die Pflichten der Escrow-Agentur bei der Lagerung und Herausgabe vertraglich geregelt.

### Entwicklung eines Redundanzkonzeptes für Anwendungen (CON.5.A13 - A)

Für Anwendungen mit einem hohen oder sehr hohen Schutzbedarf an die Verfügbarkeit wird ein Redundanzkonzept erstellt. Dieses beinhaltet folgende Aspekte:

* Planung eines eingeschränkten IT-Betriebs sowie der Wiederherstellung im Notfall (Notfallvorsorgekonzeption),
* Redundanz auf Anwendungsebene mittels Loadbalancing oder Anwendungsclustern/Cloud-Services,
* Möglichkeiten zum Schwenken der Anwendungen auf andere Systeme.

Das Redundanzkonzept beinhaltet zusätzlich die für den Anwendungsbetrieb benötigten Gebäude und Räume, Systeme und Kommunikationsverbindungen und bei vorhanden sein zusätzlich bzw. ergänzend die relevanten Cloud-Dienstleister. Das Redundanzkonzept ist mit dem Notfallkonzept abgestimmt. Alle Maßnahmen werden regelmäßig getestet und geübt.

### Mehrschichtige Netzwerkarchitektur (CON.5.bd.A1 - CIA)

Die Netzwerkarchitektur verfolgt einen mehrschichtigen (Multi-Tier) Ansatz. Idealerweise erfolgt dies mindestens mittels einer Tier-3-Architektur. Um den zukünftigen Anforderungen besser begegnen zu können, sollte die Netzarchitektur den Domain-Driven-Design Ansatz für Software unterstützen. Insofern eine Tier-3-Architektur implementiert wird, werden mindestens die folgenden Sicherheitszonen berücksichtigt:

* Webschicht: Diese Schicht grenzt an öffentliche Netze (z. B. Internet) und stellt die exponierte Schicht mit direkten Zugriffen durch Benutzer dar.
* Anwendungsschicht: Die Anwendungsschicht grenzt zum einen an die Webschicht und zum anderen an die Datenschicht an. Der Netzverkehr zu den angrenzenden Netzen (Sicherheitszonen) ist durch Sicherheitskomponenten zu filtern, sodass kein direkter Zugriff zwischen den angrenzenden Netzen möglich ist.
* Datenschicht: Die Datenschicht ist die vertrauenswürdigste Zone der mehrschichtigen Architektur. Sicherheitskomponenten zwischen den angrenzenden Netzen sollten den Datenverkehr separieren und nach dem „Need-to-know-Prinzip“ reglementieren. In dieser Schicht sollten die Hintergrundsysteme der Webanwendung wie z. B. Datenbanken und Verzeichnisdienste aufgestellt sein.

### Anwendungssegmentierung (CON.5.bd.A2 - CIA)

Die Segmentierung von Anwendungen ist wichtiger denn je, da dynamische Multi-Cloud-Umgebungen oder schnelllebige DevSecOps-Bereitstellungsmodelle für die <Institution> zur Norm werden. Insbesondere da sich die heterogenen Umgebungen ständig weiterentwickeln und somit sich eine Absicherung immer anspruchsvoller gestaltet.

Durch eine granulare Transparenz und Kontrolle mittels der anwendungsorientierten Mikrosegmentierung soll es ermöglicht werden, neue oder aktualisierte Anwendungen zum Zeitpunkt der Bereitstellung ohne zusätzliche Komplexität oder Verzögerung proaktiv zu sichern. Die gewählte Anwendungssegmentierung soll sicherstellen, dass das <Informationssicherheitsmanagementteam> jede abnormale Anwendungsaktivität im Rahmen der Sicherheitsüberwachung schnell erkennt und schnell auf neue Sicherheitsrisiken reagieren kann, bevor diese durch Unberechtigte ausgenutzt werden.