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

Sicherheitsrichtlinie "Software-Entwicklung"

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 | ISMS300006 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Software-Entwicklung" | [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](#_Toc78815421)

[Dokumentenhistorie 3](#_Toc78815422)

[Inhaltsverzeichnis 4](#_Toc78815423)

[Allgemeine Festlegungen 5](#_Toc78815424)

[Ziel / Zweck 5](#_Toc78815425)

[Geltungsbereich 5](#_Toc78815426)

[Zuständigkeiten 6](#_Toc78815427)

[Genehmigungs- und Änderungsverfahren 6](#_Toc78815428)

[Aufbau des Dokuments 6](#_Toc78815429)

[Sicherheitsrichtlinie "Software-Entwicklung" 7](#_Toc78815430)

[Basismaßnahmen 7](#_Toc78815431)

[Definition von Rollen und Verantwortlichkeiten (CON.8.A1) 7](#_Toc78815432)

[Auswahl eines Vorgehensmodells (CON.8.A2) 7](#_Toc78815433)

[Auswahl einer Entwicklungsumgebung (CON.8.A3) 7](#_Toc78815434)

[Einhaltung einer sicheren Vorgehensweise (CON.8.A4) 7](#_Toc78815435)

[Sicheres Systemdesign (CON.8.A5) 7](#_Toc78815436)

[Verwendung von Bibliotheken aus vertrauenswürdigen Quellen (CON.8.A6) 8](#_Toc78815437)

[Anwendung von Testverfahren (CON.8.A7) 8](#_Toc78815438)

[Bereitstellung von Patches, Updates und Änderungen (CON.8.A8) 8](#_Toc78815439)

[Berücksichtigung von Compliance-Anforderungen (CON.8.A9) 8](#_Toc78815440)

[Versionsverwaltung des Quellcodes (CON.8.A10) 9](#_Toc78815441)

[Standardmaßnahmen 9](#_Toc78815442)

[Ausführliche Dokumentation (CON.8.A12) 9](#_Toc78815443)

[Beschaffung von Werkzeugen (CON.8.A13) 9](#_Toc78815444)

[Schulung des Projektteams zur Informationssicherheit (CON.8.A14) 9](#_Toc78815445)

[Sicherer Einsatz der Test- und Entwicklungsumgebungen (CON.8.A15) 10](#_Toc78815446)

[Geeignete Steuerung der Software-Entwicklung (CON.8.A16) 10](#_Toc78815447)

[Maßnahmen bei erhöhtem Schutzbedarf 10](#_Toc78815448)

[Auswahl vertrauenswürdiger Entwicklungswerkzeuge (CON.8.A17 - CIA) 10](#_Toc78815449)

[Regelmäßige Sicherheitsaudits für die Entwicklungsumgebung (CON.8.A18 - CIA) 11](#_Toc78815450)

[Regelmäßige Integritätsprüfung der Entwicklungsumgebung (CON.8.A19 - I) 11](#_Toc78815451)

# Allgemeine Festlegungen

## Ziel / Zweck

Die <Institution> steht häufig vor Herausforderungen, die nicht mehr vollumfänglich mit Standardsoftware behandelt werden können. Daher ist es in diesen Fällen notwendig, eine existierende Software- oder Web-Lösung entweder anzupassen oder individuell entwickeln zu lassen. Beispiele hierfür sind hochspezifische Software-Lösungen wie Content-Management-Systeme oder Identity-Management-Systeme oder Altsysteme oder Customer-Relationship-Management-System.

Hierbei kann die Software durch die <Institution> selbst oder von einem Dritten komplett neu entwickelt werden. Ebenso kann es erforderlich sein, eine Basis-Lösung an die Anforderungen der <Institution> anzupassen und durch zusätzliche individuelle Funktionen zu erweitern.

In beiden Fällen nimmt die Software-Entwicklung eine zentrale Rolle ein, indem aus den Anforderungen der <Institution> ein Programm-Code entwickelt bzw. angepasst wird. Hierbei ist es von essentieller Bedeutung, dass die Informationssicherheit und der Datenschutz sowie das Notfallmanagement über den gesamten Software-Entwicklungsprozess hinweg berücksichtigt wird, da nur auf diese Weise die Informationssicherheit der zu entwickelnden Software-Lösung gewährleistet werden kann. Denn es ist in der Regel viel aufwändiger und kostenintensiver, wenn Informationssicherheit erst in einer späten Phase der Software-Entwicklung betrachtet wird. Außerdem besteht die Gefahr, dass bereits fertig entwickelte Bestandteile der Software angepasst oder neu entwickelt werden müssen.

Die Sicherheitsrichtlinie beschäftigt sich mit allen relevanten Sicherheitsaspekten, die bei der Eigenentwicklung von Software zu beachten sind. Hierzu wird betrachtet, wie die <Institution> die Software-Entwicklung vorbereiten und durchführen kann. Es werden entsprechende Gefährdungen identifiziert und Anforderungen formuliert. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteine CON.8 "Software-Entwicklung" 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 Software-Entwicklung“ 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 "Software-Entwicklung"

## Basismaßnahmen

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

### Definition von Rollen und Verantwortlichkeiten (CON.8.A1)

Für den Software-Entwicklungsprozess ist ein Gesamtverantwortlicher zu benennen. Außerdem sind die Rollen und Verantwortlichkeiten für alle Aktivitäten im Rahmen der Software-Entwicklung festzulegen. Für jedes Entwicklungsprojekt ist ein Sicherheitsverantwortlicher zu benennen.

### Auswahl eines Vorgehensmodells (CON.8.A2)

Es ist ein geeignetes Vorgehensmodell zur Software-Entwicklung seitens des Projektteams festzulegen. Anhand des gewählten Vorgehensmodells ist ein Ablaufplan für die Software-Entwicklung zu erstellen. Die relevanten Sicherheitsanforderungen sind zu dokumentieren.

Die Entwickler und die Mitglieder des Projektteams sollten in der Methodik des gewählten Vorgehensmodells geschult sein.

### Auswahl einer Entwicklungsumgebung (CON.8.A3)

Es ist eine Liste der erforderlichen und optionalen Auswahlkriterien für eine Entwicklungsumgebung vom Verantwortlichen für die Software-Entwicklung zu erstellen. Anschließend ist die Entwicklungsumgebung anhand der zuvor definierten Kriterien auszuwählen.

### Einhaltung einer sicheren Vorgehensweise (CON.8.A4)

Das seitens des Projektteams ausgewählte Vorgehensmodell zur Software-Entwicklung, einschließlich der relevanten Sicherheitsanforderungen ist über den kompletten Zeitraum einzuhalten. Sofern ein Wechsel des Vorgehensmodells während des Projektes notwendig ist, sollten die Gründe dokumentiert und alle Beteiligten hierüber informiert werden. Der entwickelte oder geänderte Quellcode muss auf Fehler gesichtet und auf Kompatibilität mit aller genutzten Lizenzmodelle überprüft werden. Sofern externe Komponenten mit integriert werden, sind diese auf Schwachstellen und potentielle Konflikte zu überprüfen.

### Sicheres Systemdesign (CON.8.A5)

Folgende Grundregeln des sicheren Systemdesigns sind einzuhalten:

* Grundsätzlich sind alle Eingabedaten/Formulardaten vor der Weiterverarbeitung zu prüfen und zu validieren.
* Bei Client-Server-Anwendungen sind die Daten grundsätzlich auf dem Server zu validieren.
* Die Software ist so zu konfigurieren, dass ein sicherer Betrieb bereits im Standard der Software gewährleistet ist.
* Bei Fehlern oder Ausfall von Komponenten der Software oder des dadrunter liegenden IT-Systems dürfen keine vertraulichen Daten preisgegeben werden.
* Der Betrieb der Software muss mit möglichst geringen Benutzerprivilegien nach dem Need-to-Know-Prinzip möglich sein.

Das Software und Systemdesign muss für Dritte nachvollziehbar dokumentiert werden. Es muss überprüft werden, ob alle Sicherheitsanforderungen an das Software-, Kommunikations- und Systemdesign erfüllt wurden.

### Verwendung von Bibliotheken aus vertrauenswürdigen Quellen (CON.8.A6)

Sofern im Rahmen des Entwicklungs- und Implementierungsprozesses durch die Entwickler der <Institution> oder beauftragten Dienstleistern auf externe Bibliotheken zurückgegriffen wird, sind diese aus vertrauenswürdigen Quellen zu beziehen. Bevor die externe Bibliotheken verwendet werden, sind diese durch geeignete Methoden auf deren Integrität (bspw. die genutzte Lizenz, veröffentliche Sicherheitsprobleme und deren Zeitraum bis zur Behebung sowie die stetige Weiterentwicklung) zu prüfen.

### Anwendung von Testverfahren (CON.8.A7)

Vor der Freigabe neuer oder geänderter Softwareversionen sind angemessene Tests durchzuführen, bei denen die Funktionalität und Sicherheit der Software auf dem Zielsystem geprüft wird. Alle kritischen Grenzwerte für die Funktionalität und Sicherheit sind zu testen. Des Weiteren sind für die entwickelte Software Code Reviews und eine automatische statische Code-Analyse durchzuführen. Verwendete externe Bibliotheken sind ebenfalls in den Code Reviews zu integrieren.

Ein grundsätzlicher Aspekt des Testverfahrens ist die Überprüfung der Systemvoraussetzungen und deren Dimensionierung sowie Vereinbarkeit mit gesetzlichen und internen Vorgaben für die von der <Institution> oder deren Dienstleistern entwickelte Software.

### Bereitstellung von Patches, Updates und Änderungen (CON.8.A8)

Seitens den Entwicklern der <Institution> oder dem beauftragten Dienstleister muss sichergestellt sein, dass sicherheitskritische Patches und Updates zeitnah durch die Entwickler bereitgestellt und die Verantwortlichen für das Enrollment der Software diese einspielen. Die zeitnahe Bereitstellung und Aktualisierung von sicherheitskritische Patches und Updates gilt ebenfalls auch für verwendete externe Bibliotheken.

Für die Installations-, Update- oder Patchdateien sind vom Entwickler digitale Signaturen bereitzustellen.

### Berücksichtigung von Compliance-Anforderungen (CON.8.A9)

Alle Compliance-Anforderungen, die internen Sicherheitsvorgaben, die internen Datenschutzvorgaben, die internen Notfallmanagementvorgaben, die rechtlichen Anforderungen und die spezifischen Sicherheitsanforderungen sind bei der Software-Entwicklung zu ermitteln und zu berücksichtigen.

### Versionsverwaltung des Quellcodes (CON.8.A10)

Das Entwicklungsprojekt (der Quellcode des Projektes) ist über eine geeignete Versionsverwaltung zu verwalten. Die Verantwortlichen für das Versionsverwaltungslösung müssen regeln und festlegen:

* den Zugriff auf die Versionierungstools und
* wann Änderungen am Quellcode durch die Entwickler als eigene Version in der Versionsverwaltung gespeichert werden sollen.

Es ist sicherzustellen, dass durch die Versionsverwaltung alle Änderungen am Quellcode nachvollzogen und rückgängig gemacht werden können.

Die Versionsverwaltung muss in dem Konzept zur Datensicherung berücksichtigt werden und der Betrieb der Verwaltungslösung darf nicht ohne Datensicherung erfolgen.

## Standardmaßnahmen

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

### Ausführliche Dokumentation (CON.8.A12)

Es sollten ausreichende Projekt-, Funktions- und Schnittstellendokumentationen erstellt und aktuell gehalten werden, so dass die Dokumentation im Rahmen des Onboarding von Entwicklern, eines Sicherheitsaudit oder der Bewältigung von Notfallsituationen herangezogen werden kann. Benutzern (Mitarbeitenden und Kunden) und den verantwortlichen Administratoren sollten durch die Dokumentation geeignete Hilfen zur korrekten Nutzung bzw. Administration der Software zur Verfügung gestellt werden. Die Software-Entwicklung ist so zu dokumentieren, dass ein Fachexperte mithilfe der Dokumente den Programm-Code nachvollziehen und nach kurzer Zeit weiterentwickeln kann.

### Beschaffung von Werkzeugen (CON.8.A13)

Werkzeuge für die Software-Entwicklung sollten nach standardisierten und dokumentierten Beschaffungsprozessen den Entwicklern der <Institution> bzw. des externen Dienstleisters bereitgestellt werden.

### Schulung des Projektteams zur Informationssicherheit (CON.8.A14)

Die Entwickler und die übrigen Mitglieder des Projektteams sollten zu generellen Datenschutz-, Informationssicherheits- und Notfallmanagementaspekten sowie zu den jeweils speziell für sie relevanten Aspekten geschult sein.

### Sicherer Einsatz der Test- und Entwicklungsumgebungen (CON.8.A15)

Die Test- und Entwicklungsumgebungen sollten getrennt von der Produktionsumgebung betrieben werden. Alle Informationen und Tool, die für den Produktivbetrieb nicht relevant sind oder ein erhöhtes Missbrauchsrisiko darstellen, sollten möglichst entfernt werden, bevor die Programmpakete in die Produktionsumgebung überführt werden. Testdaten sind unter Berücksichtigung des Datenschutzes sorgfältig auszuwählen und zu schützen.

Verteilte und remote Arbeitsplätze der Software-Entwicklung dürfen nur über eine kryptographisch abgesicherte Verbindung miteinander kommunizieren. Der Zugriff auf die Entwicklungsdaten ist entsprechend dem etablierten Berechtigungskonzept der <Institution> unter Berücksichtigung des Need-to-Know-Prinzip zu etablieren und zu kontrollieren. Erkannte potentielle Missbräuche des Zugriffes sind als Sicherheitsvorfall zu bewerten und der Information Security Officer ist umgehend zu involvieren.

### Geeignete Steuerung der Software-Entwicklung (CON.8.A16)

Ein geeignetes Steuerungs- und Projektmanagementmodell auf Basis des ausgewählten Vorgehensmodells sollte für die Software-Entwicklung verwendet werden und in die Konzepte zur Software-Entwicklung integriert werden. Dabei sollten insbesondere die benötigten Qualifikationen bei den Mitarbeitenden und die Abdeckung aller relevanten Phasen während des Lebenszyklus der Software berücksichtigt werden. Außerdem sollte ein geeignetes Entwicklungsmodell und Risikomanagement sowie geeignete Qualitätsziele festgelegt werden. Werden Teile der Software-Entwicklung von einem oder mehreren Dienstleistern durchgeführt, sollten diese geeignet in die internen Steuerungs- und Sicherheitsprozesse der <Institution> eingebunden werden.

## 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).

### Auswahl vertrauenswürdiger Entwicklungswerkzeuge (CON.8.A17 - CIA)

Zur Entwicklung der Software sollten nur Werkzeuge bzw. Infrastrukturen mit nachgewiesenen Sicherheitseigenschaften verwendet werden. Es sollte sichergestellt sein, dass die Werkzeuge und Infrastrukturen nicht manipuliert werden können bzw. durch den Betreiber der Infrastruktur entsprechende Mechanismen zur Erkennung von Manipulationen etabliert wurden. An die Hersteller von Entwicklungshardware oder Software sollten hinreichende Anforderungen zur Sicherheit ihrer Werkzeuge gestellt werden.

### Regelmäßige Sicherheitsaudits für die Entwicklungsumgebung (CON.8.A18 - CIA)

Es sollten regelmäßige Sicherheitsaudits der Software-Entwicklungsumgebung und der Software-Testumgebung durchgeführt werden.

### Regelmäßige Integritätsprüfung der Entwicklungsumgebung (CON.8.A19 - I)

Die Integrität der Entwicklungsumgebung sollte regelmäßig mit kryptographischen Mechanismen entsprechend dem Stand der Technik geprüft werden. Die Prüfsummendateien und das Prüfprogramm selbst sollten ausreichend vor Manipulationen geschützt sein. Wichtige Hinweise auf einen Integritätsverlust sollten nicht in einer Fülle irrelevanter Warnmeldungen (false positives) untergehen.