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

Sicherheitsrichtlinie "Software-Tests und-Freigaben"

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 Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300013 | [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](#_Toc79384430)

[Dokumentenhistorie 3](#_Toc79384431)

[Inhaltsverzeichnis 4](#_Toc79384432)

[Allgemeine Festlegungen 5](#_Toc79384433)

[Ziel / Zweck 5](#_Toc79384434)

[Geltungsbereich 5](#_Toc79384435)

[Zuständigkeiten 6](#_Toc79384436)

[Genehmigungs- und Änderungsverfahren 6](#_Toc79384437)

[Aufbau des Dokuments 6](#_Toc79384438)

[Sicherheitsrichtlinie „Software-Tests und-Freigaben" 7](#_Toc79384439)

[Basismaßnahmen 7](#_Toc79384440)

[Planung der Software-Tests (OPS.1.1.6.A1) 7](#_Toc79384441)

[Durchführung von funktionalen Software-Tests (OPS.1.1.6.A2) 7](#_Toc79384442)

[Auswertung der Testergebnisse (OPS.1.1.6.A3) 7](#_Toc79384443)

[Freigabe der Software (OPS.1.1.6.A4) 7](#_Toc79384444)

[Durchführung nicht-funktionaler Software-Tests (OPS.1.1.6.A5) 7](#_Toc79384445)

[Standardmaßnahmen 8](#_Toc79384446)

[Geordnete Einweisung der Software-Tester (OPS.1.1.6.A6) 8](#_Toc79384447)

[Personalauswahl der Software-Tester (OPS.1.1.6.A7) 8](#_Toc79384448)

[Fort- und Weiterbildung der Software-Tester (OPS.1.1.6.A8) 8](#_Toc79384449)

[Beschaffung von Test-Software (OPS.1.1.6.A9) 8](#_Toc79384450)

[Erstellung eines Abnahmeplans (OPS.1.1.6.A10) 8](#_Toc79384451)

[Verwendung von anonymisierten oder pseudonymisierten Testdaten (OPS.1.1.6.A11) 9](#_Toc79384452)

[Durchführung von Regressionstests (OPS.1.1.6.A12) 9](#_Toc79384453)

[Trennung von Test- und Qualitätsmanagement-Umgebung von der Produktivumgebung (OPS.1.1.6.A13) 9](#_Toc79384454)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc79384455)

[Durchführung von Penetrationstests (OPS.1.1.6.A14 - CIA) 9](#_Toc79384456)

[Durchführung von Notfalltests (OPS.1.1.6.bd.A1 - CA) 10](#_Toc79384457)

# Allgemeine Festlegungen

## Ziel / Zweck

Der Einsatz von IT innerhalb der <Institution> setzt voraus, dass die Datenverarbeitung unabhängig ob IT oder OT soweit wie möglich fehlerfrei funktioniert, da die Einzelergebnisse in den meisten Fällen nicht mehr kontrolliert werden können. Dies bedeutet Software jeglicher Art muss schon vor Inbetriebnahme im Rahmen von Software-Tests überprüft werden. Durch die Softwareprüfung muss nachgewiesen werden, dass die Software die erforderlichen Funktionen zuverlässig bereitstellt und darüber hinaus keine unerwünschten Nebeneffekte (Benutzbarkeit, Zuverlässigkeit, Missachtung der GDPR, Missachtung der Informationssicherheitsanforderungen) aufweist. Mit der anschließenden Freigabe der Software durch die fachlich zuständigen Mitarbeiter in den Departments wird die grundsätzliche Erlaubnis erteilt, die Software produktiv zu nutzen. Gleichzeitig übernimmt dieses Department damit auch die Verantwortung für das IT-Verfahren bzw. Sub-Prozess, das durch die Software unterstützt wird.

Software kann an unterschiedlichen Stellen ihres Lebenszyklus getestet werden. So können Software-Tests bereits bei der Entwicklung, vor der Freigabe für den Produktivbetrieb oder im Zuge des Patch- und Änderungsmanagements notwendig werden. Die Software-Tests und -Freigaben sind sowohl für Individualsoftware als auch beim Einsatz von Standardsoftware durchzuführen.

Diese Sicherheitsrichtlinie beschreibt den Test- und Freigabeprozess für individuell entwickelte oder angepasste Software sowie für Standardsoftware. Der Test- und Freigabeprozess zeichnet sich dadurch aus, dass dieser je nach Ergebnis mehrmals durchlaufen werden kann. Bei der Erstellung dieser Sicherheitsrichtlinie wurden die Vorgaben des BSI Bausteines OPS.1.1.6 "Software-Tests und -Freigaben" beachtet.

## 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-Tests und-Freigaben“ 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-Tests und-Freigaben"

## Basismaßnahmen

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

### Planung der Software-Tests (OPS.1.1.6.A1)

Vor der Durchführung der Software-Tests sind die Rahmenbedingungen entsprechend der Schutzbedarfe (Verfügbarkeit, Vertraulichkeit und Integrität), Departments, technischen Möglichkeiten und Test-Umgebungen festzulegen. Die Software-Tests müssen auf den Angaben eines Pflichtenhefts bzw. den Inhalten der Stories für die Sprints basieren.

Bei der Auswahl der Testfälle (Test-Use-Cases) hinsichtlich UI, Betrieb, Datenschutz, Informationssicherheit und Notfallmanagement ist darauf zu achten, dass diese möglichst repräsentativ für die zu testenden Funktionen der Software sind.

### Durchführung von funktionalen Software-Tests (OPS.1.1.6.A2)

Um die ordnungsgemäße und vollständige Funktion der Software zu überprüfen, sind funktionale Software-Tests durchzuführen. Idealerweise werden die funktionalen Software-Tests auch auf die UI und den hinterlegten Workflows ausgeweitet. Die funktionalen Software-Tests sind so durchzuführen, dass der Produktivbetrieb nicht beeinflusst wird.

### Auswertung der Testergebnisse (OPS.1.1.6.A3)

Die Ergebnisse der Software-Tests müssen ausgewertet werden. Es sollte ein Soll-Ist-Vergleich mit definierten Vorgaben (bspw. aus den Pflichten/Lastenheft bzw. den Inhalten der Stories für die Sprints) durchgeführt werden. Die Ergebnisse der Auswertung sind geeignet zu dokumentieren. Falls benötigt sind Optimierungsmaßnahmen und deren Umsetzungszeitraum mit in der Auswertung aufzuführen.

### Freigabe der Software (OPS.1.1.6.A4)

Es ist zu prüfen, ob die Ergebnisse der Software-Tests mit den vorher festgelegten Erwartungen übereinstimmen. Ebenfalls ist zu verifizieren, ob die Einhaltung rechtlicher oder organisatorischer Vorgaben sichergestellt ist.

Sobald die Software-Tests erfolgreich durchgeführt wurden, ist die Software durch die Verantwortlichen, den Information Security Officer und bei Bedarf durch den Data Protection Commissioner freigegeben. Die Freigabe wird in Form einer Freigabeerklärung im Rahmen der etablierten Prozesse festgehalten.

### Durchführung nicht-funktionaler Software-Tests (OPS.1.1.6.A5)

Zusätzlich zu den funktionalen Software-Tests werden nicht-funktionale Tests durchgeführt. Die sicherheitsspezifischen Software-Tests werden insbesondere bei Anwendungen mit sicherheitskritischen Funktionen durchgeführt. Die durchgeführten Testfälle als auch die Testergebnisse sind geeignet zu dokumentieren.

## Standardmaßnahmen

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

### Geordnete Einweisung der Software-Tester (OPS.1.1.6.A6)

Ein Software-Tester muss über die durchzuführenden Testarten und die zu testenden Bereiche einer Software informiert werden. Darüber hinaus sollte der Software-Tester über die Anwendungsfälle und mögliche weitere Anforderungen der Software informiert werden.

### Personalauswahl der Software-Tester (OPS.1.1.6.A7)

Bei der Auswahl der Software-Tester sollten gesonderte Auswahlkriterien berücksichtigt werden. Die Personen müssen die erforderliche berufliche Qualifikation besitzen. Es sollten außerdem ausreichende Kenntnisse der zu testenden Programmiersprache, der Entwicklungsumgebung und der einzusetzenden Testmethoden vorhanden sein. Darüber hinaus sollte eine entsprechende Rollentrennung erfolgen, sodass Quellcode nicht ausschließlich von Testern überprüft wird, die an der Erstellung des Quellcodes beteiligt waren.

### Fort- und Weiterbildung der Software-Tester (OPS.1.1.6.A8)

Alle Software-Tester der <Institution> bzw. von der <Institution> beauftragte Tester des Dienstleisters sind ausreichend auf Basis eines abgestimmten Schulungsplanes zu schulen bzw. geschult. Zusätzlich sollten Verfahren etabliert werden, mit denen die Software-Tester für ihr relevantes Aufgabenspektrum über Neuerungen informiert werden.

### Beschaffung von Test-Software (OPS.1.1.6.A9)

Die Beschaffung von Test-Software sollte anhand eines Anforderungskatalogs erfolgen. Die Test-Software wird ebenfalls dem Test- und Freigabeprozess unterzogen. Es ist zu überprüfen, ob die Hilfestellungs- und Supportleistungen des Softwareherstellers ausreichend sind und den internen Vorgaben (SLA, OLA, Vertraulichkeit, Integrität) und Erwartungen entsprechen.

### Erstellung eines Abnahmeplans (OPS.1.1.6.A10)

In einem Abnahmeplan sollten die durchzuführenden Testarten, Testfälle und die erwarteten Ergebnisse dokumentiert sein. Außerdem sollte der Abnahmeplan die Freigabekriterien beinhalten. Es muss eine Vorgehensweise für die Situation festgelegt werden, wenn eine Freigabe abgelehnt wird.

### Verwendung von anonymisierten oder pseudonymisierten Testdaten (OPS.1.1.6.A11)

Für die Software-Tests sollten nur anonymisierte oder pseudonymisierte Testdaten verwendet werden. Wenn ein Personenbezug von den Testdaten abgeleitet werden könnte, sind der Data Protection Commissioner hinzuziehen.

### Durchführung von Regressionstests (OPS.1.1.6.A12)

Wenn Software-Tests nach einer Änderung der Software durchgeführt werden sollen, sind Regressionstests mit zu inkludiert werden. Regressionstests sollten vollständig durchgeführt werden. Werden Testfälle ausgelassen, sollte dies begründet und dokumentiert werden. Die durchgeführten Testfälle und die Testergebnisse sollten geeignet dokumentiert werden.

### Trennung von Test- und Qualitätsmanagement-Umgebung von der Produktivumgebung (OPS.1.1.6.A13)

Die Software wird nur in einer hierfür vorgesehenen Umgebung getestet. Die Test- und Qualitätsmanagement-Umgebungen sind von der Produktivumgebung getrennt. Die in der Test- und Qualitätsmanagement-Umgebung verwendeten Architekturen und Mechanismen sollten dokumentiert werden. Die Test- und Qualitätsmanagement-Umgebung sollte der Produktivumgebung in ihrer Funktion entsprechen. Es sollte dokumentiert sein, wie mit der Test- und Qualitätsmanagement-Umgebung nach Abschluss des Software-Tests zu verfahren ist.

## 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).

### Durchführung von Penetrationstests (OPS.1.1.6.A14 - CIA)

Für Anwendungen beziehungsweise IT-Systeme mit erhöhtem Schutzbedarf sind Penetrationstests als Testmethode durchzuführen. Es sollte ein Penetrationstest-Konzept erstellt werden. Im Penetrationstest-Konzept sollten neben den zu verwendenden Testmethoden auch die Erfolgskriterien dokumentiert werden. Sofern Seitens der <Institution> kein eigenes Penetrationstest-Konzept für Web-Anwendungen erstellt wird, sollte auf den Testing Guide der OWASP in Version 4 zurückgegriffen werden (siehe <https://www.owasp.org/images/1/19/OTGv4.pdf>).

Der Penetrationstest sollte nach den Rahmenbedingungen des Penetrationstest-Konzepts erfolgen. Die durch den Penetrationstest aufgefundenen Sicherheitslücken sind zu klassifizieren, zu dokumentieren und entsprechend der Klassifizierung in einem Behandlungsplan zu integrieren.

### Durchführung von Notfalltests (OPS.1.1.6.bd.A1 - CA)

Für Anwendungen beziehungsweise IT-Systeme mit erhöhtem Schutzbedarf sind Notfalltests durchzuführen. Hierfür sollte ein Notfall-Konzept erstellt bzw. die bestehenden Notfallkonzepte ergänzt werden.

Der Notfalltest sollten nach den Rahmenbedingungen des erarbeiteten Konzepts erfolgen. Die aufgefundenen Lücken zu klassifizieren, zu dokumentieren und entsprechend der Klassifizierung in einem Behandlungsplan zu integrieren.