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

Sicherheitsrichtlinie "Relationale Datenbanksysteme"

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 | ISMS300054 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Relationale Datenbanksysteme" | [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](#_Toc82463244)

[Dokumentenhistorie 3](#_Toc82463245)

[Inhaltsverzeichnis 4](#_Toc82463246)

[Allgemeine Festlegungen 6](#_Toc82463247)

[Ziel / Zweck 6](#_Toc82463248)

[Geltungsbereich 6](#_Toc82463249)

[Zuständigkeiten 6](#_Toc82463250)

[Genehmigungs- und Änderungsverfahren 7](#_Toc82463251)

[Aufbau des Dokuments 7](#_Toc82463252)

[Sicherheitsrichtlinie „Relationale Datenbanksysteme" 8](#_Toc82463253)

[Basismaßnahmen 8](#_Toc82463254)

[Installation des Datenbankmanagementsystems (APP.4.3.A2) 8](#_Toc82463255)

[Basishärtung des Datenbankmanagementsystems (APP.4.3.A3) 8](#_Toc82463256)

[Geregeltes Anlegen neuer Datenbanken (APP.4.3.A4) 8](#_Toc82463257)

[Benutzer- und Berechtigungskonzept (APP.4.3.A5) 8](#_Toc82463258)

[Passwortänderung (APP.4.3.A6) 8](#_Toc82463259)

[Zeitnahes Einspielen von Sicherheitsupdates (APP.4.3.A7) 9](#_Toc82463260)

[Datenbank-Protokollierung (APP.4.3.A8) 9](#_Toc82463261)

[Datensicherung eines Datenbanksystems (APP.4.3.A9) 9](#_Toc82463262)

[Standardmaßnahmen 9](#_Toc82463263)

[Auswahl geeigneter Datenbankmanagementsysteme (APP.4.3.A10) 10](#_Toc82463264)

[Ausreichende Dimensionierung der Hardware (APP.4.3.A11) 10](#_Toc82463265)

[Einheitlicher Konfigurationsstandard von Datenbankmanagementsystemen (APP.4.3.A12) 10](#_Toc82463266)

[Restriktive Handhabung von Datenbank-Links (APP.4.3.A13) 10](#_Toc82463267)

[Überprüfung der Datensicherung eines Datenbanksystems (APP.4.3.A14) 10](#_Toc82463268)

[Schulung der Datenbankadministratoren (APP.4.3.A15) 10](#_Toc82463269)

[Verschlüsselung der Datenbankanbindung (APP.4.3.A16) 11](#_Toc82463270)

[Datenübernahme oder Migration (APP.4.3.A17) 11](#_Toc82463271)

[Überwachung des Datenbankmanagementsystems (APP.4.3.A18) 11](#_Toc82463272)

[Schutz vor schädlichen Datenbank-Skripten (APP.4.3.A19) 11](#_Toc82463273)

[Regelmäßige Audits (APP.4.3.A20) 11](#_Toc82463274)

[Maßnahmen bei erhöhtem Schutzbedarf 12](#_Toc82463275)

[Einsatz von Datenbank Security Tools (APP.4.3.A21 - CIA) 12](#_Toc82463276)

[Notfallvorsorge (APP.4.3.A22 - A) 12](#_Toc82463277)

[Archivierung (APP.4.3.A23 - A) 12](#_Toc82463278)

[Datenverschlüsselung in der Datenbank (APP.4.3.A24 - CI) 13](#_Toc82463279)

[Sicherheitsüberprüfungen von Datenbanksystemen (APP.4.3.A25 - CIA) 13](#_Toc82463280)

# Allgemeine Festlegungen

## Ziel / Zweck

Datenbanksysteme sind ein häufig genutztes Hilfsmittel, um IT-gestützt große Mengen von Informationen zu organisieren, zu erzeugen, zu verändern und zu verwalten. Ein Datenbanksystem besteht aus dem so genannten Datenbankmanagementsystem und einer oder mehreren Datenbanken. Die Datenbank selbst, ist eine Zusammenstellung von Informationen samt ihrer Beschreibung (Metadaten), die dauerhaft im Datenbanksystem abgelegt werden. Da Datenbanksysteme eine zentrale Bedeutung in der <Institution> IT-Infrastruktur einnehmen, ergeben sich an sie wesentliche Sicherheitsanforderungen.

Ziel dieser Sicherheitsrichtlinie ist es unter Beachtung der Vorgaben aus dem BSI Baustein APP.4.3 "Relationale Datenbanksysteme", Datenbanksysteme sicher betreiben zu können, sowie die Informationen, die in Datenbanken verarbeitet und gespeichert werden, angemessen zu schützen. Dazu werden Anforderungen in diesem Dokument definiert, mit denen sich die Datenbanksysteme in der Verantwortung der <Institution> sicher planen, umsetzen und betreiben lassen.

## 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

Die Sicherheitsrichtlinie „Relationale Datenbanksysteme“ 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 „Relationale Datenbanksysteme"

## Basismaßnahmen

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

### Installation des Datenbankmanagementsystems (APP.4.3.A2)

Die <Institution> stellt sicher, dass die Installationspakete des Datenbankmanagementsystems aus vertrauenswürdigen Quellen stammen. Insofern für das Datenbankmanagementsystem bereits Patches veröffentlicht wurden, werden diese vor der Inbetriebnahme des Datenbankmanagementsystems eingespielt.

### Basishärtung des Datenbankmanagementsystems (APP.4.3.A3)

Das Datenbankmanagementsystem der <Institution> wird durch zusätzliche Härtungsmaßnahmen geschützt. In diesem Zusammenhang wird eine Checkliste definiert, anhand der die durchzuführenden Maßnahmen zusammengestellt und abgearbeitet werden. Die Passwörter für das Datenbankmanagementsystem werden gemäß der technischen Richtlinie „Umgang mit Passwörtern“ angepasst. Darüber hinaus werden alle Passwörter ausschließlich mit den freigegebenen Verfahren verschlüsselt gespeichert. Grundlegende Härtungsmaßnahmen werden regelmäßig überprüft und im Bedarfsfall angepasst.

### Geregeltes Anlegen neuer Datenbanken (APP.4.3.A4)

Die <Institution> gewährleistet, dass neue Datenbanken anhand eines definierten Prozesses angelegt werden. Dieser Prozess sieht u.a. vor, dass beim Anlegen einer neuen Datenbank Grundinformationen nachvollziehbar dokumentiert werden.

### Benutzer- und Berechtigungskonzept (APP.4.3.A5)

Das allgemeine Benutzer und Berechtigungskonzepts der <Institution> wird um die für Datenbankmanagementsysteme notwendigen Berechtigungen für Rollen, Profile und Benutzergruppen erweitert.

Zum nachvollziehbaren Anlegen, Genehmigen, Einrichten, Modifizieren, Entziehen und Löschen von Datenbanknutzern sowie deren Berechtigungen werden durch die <Institution> entsprechende Prozesse etabliert. Diese stellen sicher, dass dem Benutzer nur so viele Berechtigungen eingeräumt werden, wie für die Aufgabenerfüllung notwendig (Need-to-know-Prinzip) sind. Es wird gewährleistet, dass jegliche Änderungen an Zugriffsberechtigungen angemessen dokumentiert werden. Die eingerichteten Benutzer sowie deren Zugriffsberechtigungen werden regelmäßig durch der <Institution> überprüft und im Bedarfsfall angepasst.

### Passwortänderung (APP.4.3.A6)

Die <Institution> gewährleistet, dass Benutzerpasswörter bei Verdacht eines Sicherheitsvorfalls unverzüglich angepasst werden. Insofern privilegierte Datenbankaccounts oder Dienstkonten von einem Sicherheitsvorfall betroffen sind, erfolgt der Passwortwechsel unter Absprache mit dem Anwendungsverantwortlichen.

### Zeitnahes Einspielen von Sicherheitsupdates (APP.4.3.A7)

Veröffentlichte Sicherheitsupdates für das Datenbankmanagementsystem und das Betriebssystem werden zeitnahe installiert. Die <Institution> stellt in vorangehenden Tests sicher, dass die Sicherheitsupdates kompatibel sind und keine Fehler verursachen. Vor der Implementierung eines Patches wird das Datenbankmanagementsystem im Rahmen einer Datensicherung gesichert.

Die <Institution> ernennt eine verantwortliche Rolle, die sich in regelmäßigen Abständen über identifizierte Sicherheitslücken und veröffentlichten Sicherheitsupdates informiert. Im Rahmen einer dokumentierten Überprüfung wird festgestellt, ob der interne Update-Zyklus für das Datenbankmanagementsystem an den des Herstellers angeglichen werden kann.

### Datenbank-Protokollierung (APP.4.3.A8)

Zum Zwecke einer übergreifenden Auswertung von Ereignissen muss die Zeit-Synchronisation der Datenbanksysteme mit den etablierten Zeitquellen der <Institution> erfolgen. Sicherheitsrelevante Ereignisse, die die Datenbanksysteme der <Institution> umfassen, werden mit einem eindeutigen Zeitstempel protokolliert.

Die Art und der Umfang der Protokollierung orientiert sich am Schutzbedarf der im Datenbanksystem verarbeiteten Information. Die <Institution> überprüft, ob die Protokollierung der Webanwendung und der Datenbank bereits ausreicht, um alle betriebs- und sicherheitsrelevanten Veränderungen zu erfassen oder ob weitere Maßnahmen notwendig sind und eingeleitet werden müssen. Die <Institution> gewährleistet über angemessene Maßnahmen, dass eine nachträgliche Veränderung der Protokolldateien nicht möglich ist. Durch die <Institution> wird sichergestellt, dass die Betriebsfähigkeit des Datenbanksystems auch bei einem hohen bis sehr hohen Protokollierungsvolumen sichergestellt ist.

### Datensicherung eines Datenbanksystems (APP.4.3.A9)

Das Datenbankmanagementsystem und die darunterliegenden Daten werden in regelmäßigen Systemsicherungen gespiegelt. Die <Institution> stellt durch die Verwendung von entsprechenden Dienstprogrammen sicher, dass Datenbankensysteme in jedem Fall gesichert werden, bevor eine Datenbank neu erzeugt wird.

Datenbanktransaktionen werden so gesichert, dass die Transaktionen jederzeit rekonstruierbar sind. Die <Institution> stellt sicher, dass die Datensicherung unter Berücksichtigung der vorliegenden Systemkapazitäten erfolgt und leitet im Bedarfsfall ein erweitertes Konzept, wie bspw. die inkrementelle Sicherung, ab. Anhand des Schutzbedarfs der Informationen werden entsprechende Wiederherstellungsparameter definiert.

## Standardmaßnahmen

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

### Auswahl geeigneter Datenbankmanagementsysteme (APP.4.3.A10)

Vor der Beschaffung, bzw. der Einführung eines Datenbankmanagementsystems sollten die Verantwortlichen der <Institution> alle funktionalen und nicht-funktionalen Anforderungen innerhalb eines Anforderungskataloges definieren. Alle für in Frage kommenden Datenbankmanagementsysteme werden anhand dieses Anforderungskataloges bewertet und die Ergebnisse dokumentiert.

### Ausreichende Dimensionierung der Hardware (APP.4.3.A11)

Die zu etablierenden Datenbankmanagementsysteme werden auf einer angemessen dimensionierten Hardware - unabhängig, ob virtuell oder Container oder physisch - installiert. Dabei berücksichtigt die <Institution> notwendige Reserven sowie zunehmende Anforderungen, die sich durch den zukünftigen Einsatz der Datenbankmanagementsysteme ergeben. Sollten sich im Betrieb dennoch Ressourcenengpässe aufzeigen, werden diese unverzüglich über angemessene Korrekturmaßnahmen behoben.

### Einheitlicher Konfigurationsstandard von Datenbankmanagementsystemen (APP.4.3.A12)

Die <Institution> definiert einen einheitlichen Konfigurationsstandard, anhand dessen alle Datenbankmanagementsysteme des gleichen Types konfiguriert und betrieben werden. Insofern bei der Installation und dem Betrieb von Datenbankmanagementsystemen Abweichungen notwendig sind, werden diese nachvollziehbar dokumentiert und vom <Informationssicherheitsbeauftragter> freigegeben. Der Konfigurationsstandard wird durch die <Institution> regelmäßig auf Angemessenheit überprüft und im Bedarfsfall angepasst.

### Restriktive Handhabung von Datenbank-Links (APP.4.3.A13)

Durch angemessene Maßnahmen gewährleistet die <Institution>, dass ausschließlich Verantwortliche dazu berichtigt sind, Datenbank-Links anzulegen. Die Verantwortlichen werden dabei verpflichtet, bevorzugt Private Datenbank-Links statt Public Datenbank-Links zu verwenden. Alle angelegten Datenbank-Links werden dokumentiert und regelmäßig auf ihre Notwendigkeit überprüft. Ferner wird sichergestellt, dass Datenbank-Links im Rahmen von Datensicherungen berücksichtigt werden.

### Überprüfung der Datensicherung eines Datenbanksystems (APP.4.3.A14)

Durch regelmäßige Integritätsüberprüfungen stellt die <Institution> fest, ob die vorgenommenen Datensicherungen vollständig und korrekt erfolgten. Die verantwortlichen Mitarbeitenden üben außerdem regelmäßig, wie Datenbanken im Rahmen von Notfallsituation (BCM) zeitnahe wiederhergestellt werden.

### Schulung der Datenbankadministratoren (APP.4.3.A15)

Die Administration der Datenbankmanagementsysteme erfolgt ausschließlich über ausreichend qualifizierte Mitarbeitende. Die <Institution> sollte zu diesem Zweck einen Schulungsplan in Zusammenarbeit den verantwortlichen Administratoren definieren um sicherzustellen, dass Datenbankverantwortliche angemessen hinsichtlich der Informationssicherheit, der Performance sowie dem Funktionsumfang neuer Versionen des Datenbankmanagementsystems geschult werden.

### Verschlüsselung der Datenbankanbindung (APP.4.3.A16)

Datenbankmanagementsysteme werden so konfiguriert, dass diese ausschließlich verschlüsselte Datenbankkommunikationsverbindungen zulassen. Die dazu eingesetzten kryptografischen Verfahren und Protokolle müssen den internen Vorgaben der <Institution> entsprechen. Sofern die kryptografischen Verfahren und Protokolle derzeit noch nicht freigegeben sind, sind diese zu beantragen und durch den <Informationssicherheitsbeauftragter> der <Institution> freizugeben.

### Datenübernahme oder Migration (APP.4.3.A17)

Bei initialen und regelmäßigen Datenübernahme in eine Datenbank wird vorab definiert, wie diese Migration erfolgt. Die <Institution> stellt durch angemessene Tests und Überprüfungen sicher, dass die Daten nach der Migration vollständig und unverändert übertragen wurden.

### Überwachung des Datenbankmanagementsystems (APP.4.3.A18)

Die Betriebsverantwortlichen für die Datenbanksysteme definieren Parameter, Ereignisse sowie Betriebszustände des Datenbankmanagementsystems, die für den Betrieb als kritisch zu betrachten sind und überwachen diese mithilfe eines Monitoring-Systems. Für kritische Parameter und Ereignissen werden außerdem Schwellwerte festgelegt, deren Überschreitung einen Alarm auslöst und das Durchführen angemessener Korrekturmaßnahmen zur Folge hat. Insofern auch anwendungsspezifische Parameter, Ereignisse und Schwellenwerte in das Monitoring-System miteinfließen, gewährleistet die <Institution>, dass diese mit den entsprechenden Service-Verantwortlichen abgestimmt werden.

### Schutz vor schädlichen Datenbank-Skripten (APP.4.3.A19)

Für die Entwicklung von Datenbank-Skripten definiert die <Institution> verpflichtende Qualitätskriterien. Darüber hinaus werden Datenbank-Skripte vor der Überführung in die Produktivumgebung aus gesonderten Testsystemen einem Funktionstest unterzogen. Die Ergebnisse dieser Überprüfung werden angemessen dokumentiert.

### Regelmäßige Audits (APP.4.3.A20)

Alle Komponenten des Datenbanksystems werden in regelmäßigen Audits dahingehend überprüft, ob die festgelegten Sicherheitsmaßnahmen umgesetzt und korrekt konfiguriert sind. Im Rahmen des Audits wird insbesondere überprüft, ob der dokumentierte Stand dem Ist-Zustand entspricht, ob die Konfiguration des Datenbanksystems den Standardkonfigurationen entsprechen, ob alle Datenbankskripte notwendig sind und diese die Qualitätskriterien der <Institution> erfüllen. Das Audit sieht ebenso vor, dass Protokolldateien des Datenbanksystems und des dazugehörigen Betriebssystems auf Auffälligkeiten untersucht werden.

Die <Institution> dokumentiert die Auditergebnisse nachvollziehbar und gleicht diese mit dem Soll-Zustand ab. Etwaige Mängel, die sich bei diesem Abgleich identifizieren lassen, werden im Anschluss nachverfolgt.

## 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).

### Einsatz von Datenbank Security Tools (APP.4.3.A21 - CIA)

Es werden Informationssicherheitsprodukte für Datenbanken eingesetzt. Die eingesetzten Produkte stellen folgende Funktionen bereit:

* Erstellung einer Übersicht über alle Datenbanksysteme,
* Erweiterte Konfigurationsmöglichkeiten und Rechtemanagement der Datenbank,
* Erkennung und Unterbindung von möglichen Angriffen (z. B. Brute Force Angriffe auf ein Benutzerkonto, SQL-Injection) und
* Auditfunktionen (z. B. Überprüfung von Konfigurationsvorgaben).

### Notfallvorsorge (APP.4.3.A22 - A)

Die <Institution> erstellt für das Datenbankmanagementsystem ein Notfallplan, welcher festlegt, wie der Notfallbetrieb realisiert werden kann, welche Ressourcen dafür notwendig sind und wie die Wiederherstellung des Regelbetriebes aus dem Notfallbetrieb heraus erfolgt. Um zeitnahe Eskalationen in Notfallsituationen zu ermöglichen, definiert die <Institution> notwendige Meldewege, Reaktionswege, Ressourcen und Reaktionszeiten, die im Notfallbetrieb zu berücksichtigen sind. Die von der Datenbank abhängigen IT-Systeme werden anhand von Wiederanlaufplänen ermittelt und in der Notfallvorsorge berücksichtigt.

### Archivierung (APP.4.3.A23 - A)

Zur Archivierung von Daten aus einem Datenbanksystem hinaus, etabliert die <Institution> ein Archivierungskonzept, welches sicherstellt, dass Datenbestände zu einem späteren Zeitpunkt vollständig und konsistent zur Verfügung gestellt werden können.

Innerhalb des Archivierungskonzepts werden die Archivierungsintervalle, die Vorhaltefristen der archivierten Daten sowie die zu verwendende Technik zur Datenbankarchivierung festgelegt. Im Rahmen von dokumentierten Wiederherstellungstest wird regelmäßig überprüft, ob archivierte Daten ordnungsgemäß wiederhergestellt werden können.

### Datenverschlüsselung in der Datenbank (APP.4.3.A24 - CI)

Daten innerhalb der Datenbanken werden verschlüsselt, wobei die <Institution> die folgenden Faktoren berücksichtigt:

* Einflüsse auf die Datenbank-Performance,
* Notwendige Prozesse und Verfahren zur Schlüsselverwaltung, -Aufbewahrung und –Sicherung,
* Einfluss auf Backup-Recovery-Konzepte,
* Funktionale Auswirkung auf die Datenbank wie bspw. Sortiermöglichkeiten.

### Sicherheitsüberprüfungen von Datenbanksystemen (APP.4.3.A25 - CIA)

Die <Institution> stellt sicher, dass Datenbanksysteme regelmäßigen Sicherheitsüberprüfungen unterzogen werden. Im Rahmen dieser Sicherheitsüberprüfungen werden insbesondere die system- und herstellerspezifischen Aspekte der Datenbank-Infrastruktur sowie das Datenbankmanagementsystem berücksichtigt.