Aareal

Vertragsanlage

Informationssicherheitsvorgaben

Stand: Juli 2023

2423

Inhaltsverzeichnis

1. Zweck und Ziel der Informationssicherheitsanlage

In der Informationssicherheitsstrategie der Aareal Bank AG (die „**Bank**“) sind Ziele und Prinzipien für die Informationssicherheit verankert. Auch für den Auftragnehmer ergeben sich daraus Anforderungen, in welcher Form und Qualität die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Informationen, Daten und Systemen (insgesamt die „**Schutzziele**“) sicherzustellen ist.

Der Auftragnehmer erfüllt diese Anforderungen, indem er die in dieser „Vertragsanlage – Informationssicherheitsvorgaben“ (die „**Informationssicherheitsanlage**“) niedergelegten Anforderungen an die Informationssicherheit“ (insgesamt die „**Informationssicherheitsvorgaben**“) entsprechend der Schutzbedarfsvorgabe der Bank (siehe Ziffer 3.1) – wie beschrieben oder äquivalent – umsetzt. Dies schließt die Einhaltung sämtlicher auf die Informations- und Kommunikationstechnik (die „**IKT**“) anwendbarer Gesetze und Verordnungen ein; hierzu zählen ausdrücklich auch aufsichtliche Vorgaben (z.B. BAIT, CROE).

2. Geltungsbereich

Die Informationssicherheitsvorgaben gelten, sofern und soweit die Leistungen des Auftragnehmers den Betrieb, die individuelle Erstellung und/oder die individuelle programmiertechnische Anpassung von Software umfassen und/oder der Auftragnehmer zum Zwecke oder im Zusammenhang mit der Erbringung seiner Leistungen Daten der Bank (z.B. Geschäftsdaten, die der Auftragnehmer von der Bank erhalten oder bei seinen Leistungen für die Bank erzeugt hat) auf seinen Systemen speichert oder sonst verarbeitet. Im Übrigen – d.h. im Hinblick auf Themen, Prozesse oder Tätigkeiten des Auftragnehmers, die für die mit der Bank vertraglich vereinbarten Leistungen nicht relevant sind bzw. nicht genutzt werden – gelten die Informationssicherheitsvorgaben nicht.

Sofern und soweit der Auftragnehmer die vorbezeichneten Handlungen durch Subunternehmer ausführen lässt, hat er sicherzustellen, dass seine Subunternehmer die Informationssicherheitsvorgaben ebenfalls erfüllen, und dies laufend zu überwachen.

3. Allgemeines

Die Umsetzung der Informationssicherheitsvorgaben wird regelmäßig durch die Bank überprüft.

3.1 Schutzbedarf

Die Informationssicherheitsvorgaben richten sich am Schutzbedarf der jeweiligen Systeme aus. Deshalb werden im Weiteren manche Anforderungen in einer Matrix nach Schutzbedarf und Schutzziel aufgelöst. Wenn sich Aspekte überschneiden, ist die strengere Auslegung zu wählen.

Wenn und soweit die Informationssicherheitsvorgaben nach Schutzbedarf und Schutzzielen differenzieren, ist für die jeweiligen Schutzziele jeweils folgender Schutzbedarf maßgeblich:

	Niedrig	Mittel	Hoch	Sehr Hoch
Vertraulichkeit				
Integrität				
Verfügbarkeit				
Authentizität				

Erfolgt keine Differenzierung nach Schutzziel, gilt folgender Schutzbedarf als maßgeblich:

	Niedrig	Mittel	Hoch	Sehr Hoch
Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität				

Die Bank überprüft jährlich sowie anlassbezogen den Schutzbedarf. Etwaige Veränderungen teilt sie dem Auftragnehmer schriftlich oder in Textform mit; der Auftragnehmer hat seine Umsetzung der Informationssicherheitsvorgaben in diesem Fall entsprechend anzupassen.

3.2 Abweichungen, Soll/Ist-Abgleich

Der Auftragnehmer muss seine Umsetzung der Informationssicherheitsvorgaben anlassbezogen und regelmäßig, jedoch mindestens …

	Niedrig	Mittel	Hoch	Sehr Hoch
Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität	alle drei Jahre		jährlich	

… mit den Informationssicherheitsvorgaben abgleichen (der „**Soll/Ist-Abgleich**“) und die Ergebnisse an die Bank berichten.

Der Auftragnehmer muss die Bank ferner unverzüglich informieren, wenn ihm unabhängig von dem Soll/Ist-Abgleich bekannt wird (z.B. aufgrund oder infolge von Feststellungen durch Wirtschaftsprüfer, interne und externe Audits oder Sicherheitstests (z.B. Penetration Tests, Vulnerability Scans)), dass eine oder mehrere Informationssicherheitsvorgaben nicht oder nicht vollständig umgesetzt sind.

Werden eine oder mehrere Informationssicherheitsvorgaben nicht oder nicht vollständig umgesetzt, ist im Einzelfall zu entscheiden wie mit diesen Abweichungen umgegangen wird. Diese Entscheidung …

	Niedrig	Mittel	Hoch	Sehr Hoch
Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität	kann durch den Auftragnehmer ohne Abstimmung mit der Bank getroffen werden.	kann durch den Auftragnehmer ohne Abstimmung mit der Bank getroffen und muss der Bank mitgeteilt werden.	muss durch die Bank zuvor genehmigt werden.	

3.3 Definitionen und Interpretation der Informationssicherheitsvorgaben

Die in dieser Informationssicherheitsanlage verwendeten Begriffe haben, soweit diese Informationssicherheitsanlage keine andere Definition enthält, stets die Bedeutung, die ihnen in dem Vertrag, dessen Anlage diese Informationssicherheitsanlage ist, (der „**Hauptvertrag**“) beigemessen wird.

Ferner gilt für die Interpretation der Informationssicherheitsvorgaben Folgendes:

(1) „**Muss“-Vorgaben**: Informationssicherheitsvorgaben die „muss“, „müssen“, „sind“, „darf nicht“, „dürfen nicht“ oder eine jeweilige Ableitung hiervon enthalten, sind in jedem Fall verpflichtend.

(2) „**Soll“-Vorgaben**: Informationssicherheitsvorgaben die „soll“, „sollten“, „soll nicht“, „sollen nicht“ oder eine jeweilige Ableitung hiervon enthalten, sind verpflichtend, wenn und soweit keine berechtigten Gründe für eine Abweichung bestehen. Wenn und soweit berechtigte Gründe für eine Abweichung bestehen, muss der Auftragnehmer diese Gründe und die Auswirkungen der Abweichung auf die Informationssicherheit schriftlich dokumentieren und der Bank zur Prüfung vorlegen, bevor er von der betreffenden Informationssicherheitsvorgaben abweicht. Die Dokumentation ist generell der Bank auf Verlangen vorzulegen.

(3) **„Kann“-Vorgaben**: Informationssicherheitsvorgaben die ein „kann“, „können“ oder einer Ableitung hiervon enthalten, sind nicht verpflichtend, sondern durch den Auftragnehmer freiwillig umzusetzen.

3.4 Regulatorik, Stand der Technik und Standards

Alle Vorgaben sind entsprechend den regulatorischen Vorgaben, dem Stand der Technik und anerkannten Industriestandards umzusetzen. Der Auftragnehmer weist die Bank auf veraltete, fehlende oder unzureichende Informationssicherheitsvorgaben anlassbezogen hin.

3.5 – einstweilen freibleibend –

3.6 Informations- und Kommunikationstechnologie (IKT)-Systeme

„**IKT-Systeme**“ im Sinne dieser Informationssicherheitsanlage (darin auch kurz „**Systeme**“ genannt) sind entsprechend EBA-Guideline EBA/GL/2019/04 IKT-Einrichtungen, die Teil eines Mechanismus oder eines verbindenden Netzwerks sind, dass den Betrieb eines Finanzinstitutes unterstützt (*ICT set-up as part of a mechanism or an interconnecting network that supports the operations of a financial institution*).

IKT-Systeme bzw. Komponenten von IKT-Systemen sind beispielweise Server, Netzwerke, Datenbanken, Business-Managed-Applications (BMA) oder IT-Managed-Applications (ITMA).

3.7 Informationssicherheitsrelevante Änderungen

Änderungen, die sich auf das Informationssicherheitsniveau oder die Risikoeinschätzung zur Informationssicherheit auswirken können, sind informationssicherheitsrelevant. Solche Änderungen können z.B. im Rahmen von Projekten, Software-Changes oder Vorfällen im IT-Betrieb entstehen.

4. Informationssicherheitsvorgaben an die Organisation

4.1 Zusammenarbeit

Der Auftragnehmer unterstützt die Bank beim Management der Informationssicherheit und stellt ihr die notwendigen Informationen zur Verfügung.

4.2 – einstweilen freibleibend –

4.3 Dokumentierte Bedienabläufe

Der Auftragnehmer muss eine Dokumentation von Systemen und Unternehmensprozessen erstellen, die

a.) alle wichtigen Bedienabläufe umfasst,

b.) den jeweiligen Benutzern zur Verfügung steht und

c.) …

	Niedrig	Mittel	Hoch	Sehr Hoch
Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität	mindestens einmal im Jahr		mindestens einmal im Jahr und anlassbezogen	

… geprüft und, soweit notwendig, aktualisiert und vervollständigt wird.

4.4 Trennung der Aufgaben

Der Auftragnehmer muss dafür Sorge tragen, dass miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche getrennt und die verschiedenen Rollen entsprechend gestaltet sind. Die Rollen zur Entwicklung, zum Test, zur Abnahme und zur Produktivsetzung von Neueinführungen oder Änderungen an bestehenden Systemen und Anwendungen müssen frei von Interessenskonflikten gestaltet und im jeweiligen Berechtigungskonzept dokumentiert werden.

Aufgaben, Verantwortlichkeitsbereiche und/oder Rollen stehen in Konflikt zueinander, wenn diese zur Risikomitigation organisatorisch/ prozessual getrennt sein müssen (z.B. Vier-Augen-Prinzip, *Segregation of Duties* (SoD)).

4.5 Schulung, Awareness und Training

Alle eingesetzten Mitarbeiter müssen regelmäßig zielgruppenspezifisch zu Security-Awareness-Themen trainiert werden. Der Auftragnehmer hat sicherzustellen, dass die eingesetzten Mitarbeiter die spezifischen Verfahren und Richtlinien mit Sicherheitsrelevanz in ihrem spezifischen Arbeitsbereich kennen.

4.6 Inventarisierung

Der Auftragnehmer muss sicherstellen, dass seine gesamten Systeme in Inventaren erfasst und gepflegt sind.

4.7 Trennung von Systemen

Bei der Erstellung von Quellcode oder der individuellen Anpassung einer Software, also der Änderung einer Software über die vorgesehenen Konfigurationseinstellungen hinaus, ...

	Niedrig	Mittel	Hoch	Sehr Hoch
Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität	kann	sollte	muss	

… der Auftragnehmer Entwicklungs-, Test- und Betriebsumgebungen voneinander getrennt betreiben, um das Risiko unbefugter Zugriffe auf oder Änderungen an Daten und Quellcode zu verringern.

4.8 Zutrittsregelung

Räumlichkeiten, in denen der Auftragnehmer seine Leistung erbringt und/oder in denen sich sonstige informationsverarbeitende Einrichtungen befinden, insbesondere sicherheitskritische Bereiche, müssen vor dem Zutritt Unbefugter geschützt werden. Besucher, Handwerker und andere externe Dritte dürfen sich nicht frei und unkontrolliert oder unbegleitet außerhalb der ihnen zugewiesenen Tätigkeiten im Gebäude bewegen.

Insbesondere müssen IKT-Infrastrukturen (z.B. Server- und Verteilräume, Rechenzentrum) und weitere besonders schützenswerte Unternehmensbereiche (z.B. Vorstand) mittels geeigneter physischer und logischer Maßnahmen vor unerlaubtem Zugriff/Zutritt geschützt werden.

Bei längerer Abwesenheit eines Mitarbeiters muss die entsprechende Zutrittsberechtigung vorübergehend gesperrt werden. Zutrittsstellen wie Anlieferungs- und Ladebereiche sowie andere Stellen, über die unbefugte Personen die Räumlichkeiten betreten könnten, müssen überwacht und, falls möglich, von informationsverarbeitenden Einrichtungen getrennt werden, um unbefugten Zutritt zu verhindern.

4.9 Benutzerzugangsverwaltung

4.9.1 Zugangs- und Zugriffsregelung

Zugangs- und Zugriffsberechtigungen für Netzwerke, Systeme, Anwendungen und Informationen sind nur zu erteilen, soweit und solange sie zur Erledigung der jeweiligen Aufgabenerfüllung notwendig sind (*Need-to-know-Prinzip*).

Benutzerkonten müssen nur diejenigen Zugriffsrechte erhalten, die für die Ausführung der Aufgaben zwingend erforderlich sind – nicht mehr und nicht weniger (*Least-Privilege-Prinzip*).

Alle Anwendungen mit Berechtigungsverwaltung müssen ein Berechtigungskonzept vorweisen. Dieses Berechtigungskonzept muss mindestens jährlich überprüft werden.

Es ist dazu eine Zugangs- und Zugriffssteuerungsrichtlinie unter Berücksichtigung folgender sicherheitsrelevanter und geschäftlicher Anforderungen zu erstellen:

- Die Vergabe von Berechtigungen darf ausschließlich über Berechtigungsanträge erfolgen und muss inklusive des Freigabe-Prozesses nachweisbar dokumentiert werden.

- Accounts und deren Berechtigungen müssen immer einer verantwortlichen Person zugeordnet sein.
- Vor der Vergabe von Benutzerberechtigungen muss der Berechtigte eindeutig identifiziert werden.
- Die Änderung, Deaktivierung oder Löschung von Berechtigungen muss den Prozessen in den entsprechenden Berechtigungskonzepten unterliegen und nachweisbar sein.
- Standardberechtigungen auf Basis bestimmter Benutzerattribute (z.B. Zugehörigkeit zu einer Organisationseinheit) können automatisch zugewiesen werden. Solche Regeln müssen im Berechtigungskonzept dokumentiert werden.
- Das Berechtigungskonzept muss Genehmigungsstufen festlegen, die mindestens folgende Anforderungen erfüllen:
    - Die Genehmigung Business-Kritischer (wie unter Ziffer 4.9.2 definiert) und (hoch-)privilegierter (wie unter Ziffer 4.9.3 definiert) Berechtigungen muss mindestens im 4-Augen-Prinzip erfolgen (d.h. es muss eine 2-stufige Genehmigung vorgesehen werden).
    - Selbstgenehmigungen in der Rolle als Führungskraft dürfen nicht erfolgen.
    - Die fachlich verantwortliche Person für die Berechtigung muss eingebunden werden.

4.9.2 Benutzerverwaltung

Für das Anlegen und Löschen bzw. Deaktivieren von Benutzern und deren Berechtigungen sowie die regelmäßige Rezertifizierung muss für alle Benutzerkonten ein formaler Prozess genutzt werden. Dies umfasst auch technische Benutzer.

Business-Kritische und (hoch-)privilegierte (wie unter Ziffer 4.9.3 definiert) Berechtigungen müssen mindestens zweimal jährlich und sonstige Berechtigungen mindestens einmal jährlich überprüft werden (Rezertifizierung). Eine Selbst-Rezertifizierung darf nicht zugelassen sein.

Als „**Business-Kritisch**“ gelten Berechtigungen, wenn sie Zugriff auf sensible Daten ermöglichen, die kundenspezifische oder geschäftsspezifische Relevanz für die Bank haben. Dies sind unter anderem persönliche Daten, wie Stamm- oder Transaktionsdaten oder Risikokennzahlen, die nicht öffentlich zugänglich sind. Es kann sich aber auch um Daten handeln, die eine hohe Integrität erfordern, (wie z. B. Risikowertberechnungen oder Customizing-Parameter kritischer Daten), eine hohe Verfügbarkeit verlangen (z.B. das schnelle Ausführen von Zahlungen) oder bei denen die Authentizität eine hohe Relevanz besitzt (z. B. Meldedaten, die eindeutig von der Bank kommen müssen).
Zudem sind diese Daten abgrenzbar von Daten und Berechtigungen für den technische Umgang von IT-Systemen.

Im Rahmen der Benutzerverwaltung müssen die gleichen Kontrollinstanzen wie beim erstmaligen Anlegen von Benutzern und deren Berechtigungen einbezogen werden (z.B. der fachliche Verantwortliche).

Bei geplanter längerer Abwesenheit von Benutzern müssen in den Applikationen und Services mit hohem oder sehr hohem Schutzbedarf die betreffenden Benutzerkonten gesperrt werden. Dies gilt entsprechend, wenn eine ungeplante Abwesenheit länger andauert.

In allen anderen Fällen müssen Benutzerkonten, die nicht mehr benötigt werden, gesperrt und die Berechtigungen entzogen werden.

4.9.3 (Hoch-)Privilegierte Benutzer (High Privileged Users, HPUs)

Hochprivilegierte Benutzer (High Privileged Users, HPUs), sind zu identifizieren und gesondert zu überwachen, um sicherzustellen, dass sie ihren täglichen Tätigkeiten ohne Abweichungen vom vorgesehenen Rahmen nachgehen und keine unerlaubten Aktivitäten stattfinden.

Als „**Hochprivilegierte Benutzer**“ bzw. „**HPUs**“ zu verstehen und entsprechend (z.B. hinsichtlich des Monitorings oder der Risikominderung durch technische/organisatorische Maßnahmen) zu behandeln sind Benutzer, die in Bankprozessen, in aufsichtsrechtlichen, Rechnungswesen-, Risiko- oder steuerungsrelevanten Systemen und auf deren Infrastrukturkomponenten eine oder mehrere der folgenden Berechtigungen haben oder verwalten können:

- Anlegen und Löschen von Benutzerkonten;
- Konfiguration von Soft- oder Hardware-Komponenten (inkl. Schnittstellen);
- Löschen von Protokolldateien;
- Verwaltung von systemübergreifenden Sicherheitsmechanismen (z.B. Ein-/Ausschalten);
- Verwaltung von Back-ups und Wiederherstellung von Systemen;
- Konfiguration von Kommunikationswegen

Der Auftragnehmer muss sicherstellen, dass nur ausreichend qualifizierte Mitarbeiter über Benutzerberechtigungen verfügen, die zur Einstufung als HPU führen, und mit solchen Benutzerberechtigungen für die Bank tätig sind.

Wenn es technische User gibt (insbesondere mit hart codierten HPU-Anmeldedaten), die solche Rechte besitzen, sind auch diese entsprechend zu überwachen.

„**Notfallaccounts**“ oder „**Notfallidentifikationen**“ sind Identifikationen für Benutzerkonten mit Kritischen Berechtigungen (HPU) zur Verwendung für Aktivitäten im Notfall, die nicht mit administrativen Benutzerkonten durchgeführt werden können. Die Hinterlegung von Passwörtern (s. Kap. 4.9.10) ist für diese Accounts gesondert zu regeln.

4.9.4 Hilfsprogramme mit privilegierten Rechten

Hilfsprogramme, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen wie die unter Ziffer 4.9.3 Genannten zu umgehen, müssen ausschließlich für zugelassene Benutzer zur Verfügung stehen. Die Möglichkeiten zum Einsatz solcher Software sind zu beschränken und zu überwachen.

4.9.5 Fernwartungszugänge

Wenn und soweit zum Zweck der Wartung oder Störungsbeseitigung ein Zugang von außen – d.h. in der Regel über das Internet – zu IT-Komponenten im lokalen Netz eingerichtet wird, muss ergänzend zu den Zugangsregelungen für Benutzer und Berechtigungen Folgendes umgesetzt werden:

(1) Die Initiative zum Aufbau einer Support- oder Fernwartungssession muss immer vom Auftragnehmer ausgehen (4-Augen-Prinzip).

(2) Jede Fernwartungsverbindung muss verschlüsselt werden.

(3) Der Fernwartende muss sicher authentifiziert werden, bevor er Zugriff auf das System erhält. Eine starke Multi-Faktor-Authentifizierung sollte genutzt werden.

(4) Der Zugang muss so eingerichtet werden, dass der Fernwartende keinerlei Zugriff auf Rechner außerhalb des Tätigkeitsbereichs erhält.

(5) Die zur Etablierung des Fernwartungszugangs an den zentralen Sicherheits-Gateways vorzunehmenden Modifikationen sind so gering wie möglich zu halten.

(6) Die Durchführung einer Fernwartung muss protokolliert werden.

(7) Nach Beendigung der Aufgaben muss die Fernwartungssession wieder abgebaut werden.

4.9.6 Kennwortregelung

Folgende technische Mindeststandards gelten für Kennwörter (Passwörter):

(1) Kennwortgültigkeit: Dauer kann unbegrenzt sein, wenn das Kennwort mindestens 2 Faktoren aus den Kategorien Wissen, Haben und Sein/Biometrie umfasst; anderenfalls muss das Kennwort regelmäßig geändert werden.

(2) Kennwortlänge: Muss mindestens 16 Zeichen betragen; umfasst das Kennwort mindestens 2 Faktoren aus den Kategorien Wissen, Haben und Sein/Biometrie, kann auf mindestens 8 Zeichen reduziert werden.

(3) Kennwortkomplexität: Muss mindestens drei aus diesen vier Möglichkeiten enthalten: Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern.

(4) Kennwort-Historie: Darf nicht mit den 10 zuletzt verwendeten Kennwörtern übereinstimmen.

(5) Kennwörter dürfen nicht in Klartext angezeigt und übermittelt werden (das Anzeigen von Klartext auf Wunsch des Nutzers, durch eine absichtliche Aktion, kann jedoch erfolgen).

(6) Nach mehrmaliger (5-10) fehlerhafter Kennworteingabe muss der Benutzer gesperrt werden. Eine automatische Entsperrung kann nach einem beschränkten Zeitraum (z.B. 15 Minuten) erfolgen.

(7) Die Änderung von Initial-Kennwörtern muss erzwungen werden.

(8) Wenn technisch möglich, sollte für HPUs eine regelmäßige Rotation der Passwörter durchgeführt werden.

Die folgenden zusätzlichen Mindeststandards müssen zumindest organisatorisch (nicht zwingend technisch) umgesetzt werden:

(1) Kennwörter dürfen nicht Benutzernamen oder -kennungen oder Teilen davon entsprechen oder diese beinhalten.

(2) Kennwörter dürfen nicht im Duden oder Fremdwortlexikon zu finden sein.

(3) Kennwörter dürfen nicht in Skripten fest einprogrammiert werden.

(4) Kennwörter dürfen nur im Kenn-/Passwortmanager in Klarschrift hinterlegt werden, ansonsten ist ein Kenn-/Passworthash zu verwenden (Ausnahmen für das Business Continuity Management sind individuell zu klären.).

Sind Teile der Regeln technisch nicht umsetzbar, z.B. weil die Software die Regeln nicht darstellen kann, muss die Abweichung an die Bank gemeldet und/oder zusätzliche Sicherungsmaßnahmen getroffen werden. Das Vorgehen im Zusammenhang mit solchen Abweichungen ist…

	Niedrig	Mittel	Hoch	Sehr Hoch
Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität	zu erarbeiten.		mit Zustimmung der Bank zu erarbeiten.	

Dies muss dokumentiert und im Rahmen des Soll/Ist-Abgleichs vermerkt werden.

4.9.7 Erstellung von Kennwörtern

Bei der Erstellung eines Kennworts sind die technischen Kennwortregeln (siehe Ziffer 4.9.6) anzuwenden. Bei der Softwareinstallation automatisch vergebene Kennwörter sind unverzüglich durch eigene Kennwörter zu ersetzen.

Initiale Kennwörter müssen einmalig und zufallsgeneriert sein.

Durch Dritte erstellte Kennwörter müssen umgehend durch ein eigenes Kennwort ersetzt werden.

Neuerstellte, zurückgesetzte oder Default-Kennworte sind nach der ersten Verwendung zu ändern. Dies ist systemseitig zu erzwingen.

4.9.8 Rücksetzung von Kennwörtern

Soweit technisch und organisatorisch möglich, muss für die Kennwortrücksetzung ein automatisiertes Verfahren eingesetzt werden.

Rückgesetzte Kennwörter müssen umgehend durch ein eigenes Kennwort ersetzt werden.

4.9.9 Übermittlung von Kennwörtern

Ein initial vergebenes Kennwort muss dem Benutzer so mitgeteilt werden, dass eine Kenntnisnahme durch unbefugte Dritte vermieden wird.

4.9.10 Hinterlegung von Kennwörtern

Kennwörter, die zu BCM- und Sicherungszwecken und damit zur Aufrechterhaltung des Betriebes notwendig sind, können physisch hinterlegt werden. Diese Kennwörter müssen

- vor unbefugtem Zugriff geschützt und sicher verwahrt und
- nach Benutzung geändert

werden. Solche Kennwörter können im Übrigen auch in einem geeigneten Kenn-/Passwortmanager in den Systemen des Auftragnehmers gespeichert werden. Das Kennwort zu diesen Dateien darf nur den jeweiligen Notfallbenutzern (Nutzer von Notfallaccounts) bekannt seien.

4.10 Change-Management

Änderungen an IKT-Systemen bzw. Anwendungen oder den zugrundeliegenden Architekturen und Technologien sind vom Auftragnehmer zu erfassen und nachvollziehbar (dokumentiert) zu steuern.

Sicherheitskritische Änderungen dürfen nicht ohne die Zustimmung der Bank umgesetzt werden, sofern diese das Sicherheitsniveau der Daten der Bank negativ beeinflussen können.

Aus zeitkritischen Störungen kann der Bedarf für Notfalländerungen (*Emergency Changes*) erwachsen. In diesen Fällen muss die Änderung im Nachgang mit der Bank abgestimmt werden.

4.11 Aufrechterhaltung der Informationssicherheit im BCM

Im Not-/Krisen- oder Katastrophenfall muss der situative höchstmögliche Schutz durch den Auftragnehmer erreicht werden. Dabei sind die Schutzbedarfe für die jeweiligen Schutzziele zu beachten.

Während einer für das Business-Continuity-Management („**BCM**“) relevanten Störung sind die Schutzziele so gut wie möglich sicherzustellen. Es ist wahrscheinlich, dass während einer BCM-relevanten Störung das Schutzniveau entsprechend dieser Informationssicherheitsvorgaben nicht eingehalten werden kann. Deshalb muss im Rahmen des BCM festgelegt werden, welches Schutzniveau akzeptabel ist. Dieses Niveau muss der Bank mitgeteilt werden, soweit es die für die Bank erbrachten Leistung bzw. die Daten der Bank betrifft. Es sind Prozesse, Verfahren und Maßnahmen zu dokumentieren, wie die jeweiligen Schutzniveaus erreicht bzw. aufrechterhalten werden. Die BCM-Dokumentation muss regelmäßig überprüft und, soweit erforderlich, aktualisiert werden.

4.12 Lifecycle-Sicherheitsanforderungen an IKT-Systeme

Bei der Einführung neuer IKT-Systeme, sowie bei der Veränderung von IKT-Systemen sind die Informationssicherheitsvorgaben zu berücksichtigen.

Dies beinhaltet, dass die Informationssicherheitsvorgaben bereits in die Anforderungen für ein neues System (Pflichtenheft) oder in einen Change (siehe Ziffer 4.10) einfließen müssen.

4.13 Besonderheiten bei Übertragungen in Netzwerken

Informationen, die durch öffentliche Netzwerke übertragen werden, müssen gemäß Ziffer 5.5 verschlüsselt werden. Dies muss durch entsprechende Übertragungswege sichergestellt werden, die durch die IKT-Betreiber zur Verfügung gestellt werden. Endanwenderkommunikation wie E-Mail fällt nicht unter diese Regeln, muss aber ebenfalls sicher geregelt werden.

Darüber hinaus muss sichergestellt werden,

- welche Informationen übertragen werden dürfen und wer dies freigeben darf,
- dass die Kommunikationspartner vor Übertragung von Information eindeutig identifiziert werden, und,
- dass geeignete Übertragungsverfahren gewählt werden, die die Integrität der Information schützen.

Wenn Dienste/Services des Auftragnehmers an Finanztransaktionen beteiligt sind, sind besondere folgende Sicherheitsmaßnahmen zu erfüllen:

- Benutzerauthentifizierungsinformationen sind gültig und verifiziert;
- Transaktionsdaten sind an einem nicht öffentlich zugänglichen Speicherort zu sichern.

4.14 Application Development und Deployment

Für die Entwicklung von Software und Systemen muss eine interne Richtlinie bestehen. Bei der Erstellung und Anpassung von Programmen müssen Sicherheitsaspekte zum Schutz von Informationen gemäß dem *Security-by-Design-Prinzip* mit einbezogen werden.

Änderungen an Systemen müssen im Rahmen des Change-Prozesses bearbeitet, gesteuert und dokumentiert werden (siehe Ziffer 4.10).

Um sicherzustellen, dass Änderungen an den technischen Plattformen der wesentlichen Anwendungen den Betrieb und die Informationssicherheit nicht beeinträchtigen, sind auch die Anwendungen in solchen Fällen risikobasiert zu testen.

Standardsoftware sollte, soweit möglich, ohne Änderungen in der vom Hersteller bereitgestellten Form verwendet werden. Sollten Änderungen an Standardsoftware unvermeidbar sein, sollten die Konsequenzen, wie z.B. Wartbarkeit, Update neuer Versionen, Kompatibilität zu anderer Software und Auswirkung auf Kontrollmechanismen, berücksichtigt werden.

Für interne Entwicklungsprozesse/-projekte sind Verfahren zu nutzen die in der Analyse, Entwicklung und Pflege von Systemen die Informationssicherheitsvorgaben berücksichtigen.

Der Zugang zur Entwicklungsumgebung und insbesondere zum Quellcode von Programmen muss nach dem *Need-to-Know-Prinzip* eingeschränkt werden. Die Dokumentation über sensible Systeminformationen, Konfigurationen oder Quellcode (ggf. in Repositories) muss gegen unbefugten Zugriff und Verlust geschützt werden.

4.14.1 Ausgegliederte Entwicklung

Wird durch den Auftragnehmer (oder Subunternehmer des Auftragsnehmers) im Auftrag der Bank Software erstellt oder angepasst, sind die Best Practices aus dem Bereich der sicheren Anwendungsentwicklung zu berücksichtigen. Als Richtwert gelten z.B. die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik.

4.14.2 Abnahmetest und Systemsicherheit

Vor dem Einsatz muss neue und geänderte Soft- und Hardware getestet werden.

Die Tests während der Entwicklung von Systemen müssen immer auch die Prüfung der relevanten Informationssicherheitsvorgaben umfassen. Der Umfang der Prüfungen sollte der Bedeutung und der Beschaffenheit des Systems entsprechen. Dabei sollte auch die Art der Änderung berücksichtigt werden.

4.15 Testdaten

Daten der Bank dürfen nicht ohne vorherige Zustimmung der Bank in Schrift- oder Textform zu Testzwecken genutzt werden.

4.16 Informationssicherheitsvorfälle, Incident-Management

Begriff	Definition entsprechend ISO27000
Informationssicherheit (en: information security)	Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Anmerkung zum Begriff: Zusätzlich können auch andere Eigenschaften wie Authentizität, Zurechenbarkeit, Nicht-Abstreitbarkeit und Verlässlichkeit einbezogen werden.
Informationssicherheitsereignis (en: information security event) ISE	Erkanntes Auftreten eines Zustands eines Systems, Dienstes oder Netzwerks, der eine mögliche Verletzung der Informationssicherheitspolitik oder die Unwirksamkeit von Maßnahmen oder eine vorher nicht bekannte Situation, die sicherheitsrelevant sein kann, anzeigt.

Informationssicherheitsvorfall (en: information security incident) ISI	Einzelnes ungewolltes oder unerwartetes Informationssicherheitsereignis oder eine Reihe solcher Ereignisse, die eine erhebliche Wahrscheinlichkeit besitzen, Geschäftstätigkeiten zu gefährden und die Informationssicherheit zu bedrohen.

Ein Informationssicherheitsvorfall könnte beispielsweise sein:

- Unbefugter **Zutritt** zum Rechenzentrum oder anderen sicherheitskritischen Räumen;
- unbefugter **Zugang** zum System durch die Benutzung eines Accounts durch einen unberechtigten Dritten (z.B. das Kennwort wurde ermittelt); oder
- unbefugter **Zugriff** auf Dateien, indem diese abgefangen oder anscheinend manipuliert wurden, z.B. wenn ein Benutzerkonto dazu missbraucht wurde oder sensible Daten/ der Datentransfer nicht verschlüsselt wurden.

Der Auftragnehmer muss Informationssicherheitsvorfälle sofort und unmittelbar entsprechend der Betriebsdokumentation an den/die seitens der Bank benannten Kontaktdaten melden.

Für Informationssicherheitsvorfälle, die in Zusammenhang mit den an die Bank zu erbringenden Leistungen stehen, erfolgen die Mitteilungen gegenüber externen Dritten (z.B. Behörden) ausschließlich durch oder in Abstimmung mit dem Chief Information Security Officer der Bank oder dessen benanntem Vertreter. Gesetzliche Meldepflichten des Auftragnehmers bleiben hiervon unberührt.

Es sind Verantwortlichkeiten und Verfahren festzulegen, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen. Erkenntnisse aus der Lösung und der Analyse der Informationssicherheitsvorfälle müssen zur Erstellung risikominimierender Maßnahmen genutzt werden, um das Sicherheitsniveau nachhaltig zu verbessern, indem den jeweiligen Szenarien vorgebeugt wird.

Es sind Prozess zur Ermittlung, Sicherung und gerichtsfesten Aufbewahrung von Beweismaterial anzuwenden.

Alle internen und externen Mitarbeiter sind auf ihre Verantwortung hinzuweisen, Informationssicherheitsereignisse so schnell wie möglich zu melden.

4.17 Security Tests

Das Testen und Prüfen auf Informationssicherheit von Informationssicherheits-Assets im Geltungsbereich des ISMS (Informationsverbund) ist eine zentrale Maßnahme, um die Wirksamkeit der Schutzmaßnahmen festzustellen und noch nicht identifizierte Schwachstellen zu finden. Der Auftragnehmer muss die für die Leistungen an die Bank relevanten Systeme regelmäßig und risikobasiert Sicherheitstests unterziehen, z.B. Penetrationstests oder Schwachstellen-Scans.

Testergebnisse, die für die Bank relevant sind (z.B. es sind Systeme oder Infrastruktur betroffen, auf denen Daten der Bank verarbeitet werden), müssen regelmäßig und zeitnah an die Bank gemeldet werden. Die Schließung der gefundenen Schwachstellen muss ebenfalls an die Bank berichtet werden.

Sollten im Rahmen von Sicherheitstests Kritische Schwachstellen gefunden werden, müssen diese unverzüglich der Bank schriftlich mitgeteilt werden. Als „**Kritisch**“ gilt eine Schwachstelle mit einem Common-Vulnerability-Scoring-System (CVSS) -Score von 9,0 oder höher oder eine Schwachstelle, die von einer qualifizierten Instanz (z.B. BSI, NIST) als kritisch eingestuft wurde.

5. Technische Informationssicherheitsvorgaben

5.1 Systemhärtung

5.1.1 Least Functionality

Systeme sind nach dem *Least-Functionality-Prinzip* einzurichten. Das heißt, es müssen ausschließlich Komponenten installiert/aktiv sein, die zwingend notwendig sind. Dies umfasst die beabsichtigte Anwendung und ihre Komponenten, Komponenten, die zur Integration in die lokale Infrastruktur notwendig sind, und Komponenten, die für die Wartung notwendig sind. Alle Services der Softwarekomponenten, die nicht zur Erbringung des Dienstes, zur Integration in die Infrastruktur oder zur Wartung benötigt werden, sind zu deinstallieren. Falls eine Deinstallation nicht möglich ist, sind diese Dienste zu deaktivieren.

Eingesetzte Software muss

- offiziell eine vom Entwickler freigegebene, stabile und sichere Versionen (*Stable Release*) sein;
- für das Betriebssystem-Release vorgesehen sein; und
- sicher konfiguriert werden (Herstellerstandardkonfigurationen sind als unsicher anzusehen).

5.1.2 Netzwerkhärtung

Das Netzwerk muss gruppenweise (nach Benutzer, Diensten, Services etc.) voneinander getrennt (segmentiert) betrieben werden. Es müssen ausschließlich benötigte Ports offen sein. Alle anderen Ports sind zu schließen. Zudem muss die Konfiguration regelmäßig geprüft und, soweit erforderlich, aktualisiert werden.

5.1.3 Schutz vor Schadsoftware

Zum Schutz vor Schadsoftware sind angemessene Erkennungs-, Vorbeugungs- und Wiederherstellungsmaßnahmen umzusetzen. Hierzu gehört insbesondere der Einsatz vor Virenschutz auf Clients und Servern.

5.1.4 Patch Management

Bei jeder Entscheidung zur Aktualisierung von IT-spezifischen Lösungen sind die geschäftlichen Anforderungen für die Änderung und die Sicherheit der jeweiligen Version aus Sicht der betroffenen Informationen zu berücksichtigen.

Anpassungen an der Sicherheitsarchitektur sind in regelmäßigen Zeitabständen vorzunehmen, um dem aktuellen Stand der Technik zu entsprechen. Dies umfasst insbesondere System- und Sicherheitsupdates (siehe untenstehende Auflistung) sowie einen angemessenen Schutz durch ein Antivirenprogramm mit täglich aktualisierten Signaturen.

Bei der Planung muss eine Rollback-Strategie berücksichtigt werden. Frühere Versionen der Systeme sind als Fallback-Version aufzubewahren.

Für die eingesetzten Systeme muss mindestens monatlich und anlassbezogen eine Prüfung auf verfügbare Updates bzw. Release-Changes (Minor und Major) erfolgen.

Patches sind …

	Niedrig	Mittel	Hoch	Sehr Hoch
Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität	spätestens nach 3 Monaten		spätestens nach 3 Monaten im Fall von BIOS/Firmware und Treibern sowie im Übrigen spätestens nach 1 Monat, sofern die Risikobewertung jeweils keine kürzere Frist gebietet,	

… zu testen und einzuspielen.

Wenn eine angemessene Überprüfung der Patches nicht möglich ist, z.B. aus Kostengründen oder aufgrund fehlender Ressourcen, können Patches zurückgestellt werden, um zuvor die damit verbundenen Risiken auf Grundlage der von anderen Benutzern berichteten Erfahrungen abzuschätzen.

Tests und Upgrades von Minor- und Major Releases sind im Rahmen des Change-Managements zu entscheiden und zu planen. Das Vorgehen muss innerhalb von …

	Niedrig	Mittel	Hoch	Sehr Hoch
Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität	beliebiger Zeit festgelegt werden.	3 Monaten festgelegt werden.	1 Monat festgelegt werden.	

Vor der Umsetzung muss der Patch/die Aktualisierung/der Hot- oder Bugfix getestet werden.

Zu den Patch-relevanten Systemen gehören mindestens:

- BIOS/ Firmware;
- Betriebssysteme;
- Treiber anderer betriebssystemzugehöriger Komponenten;
- Middleware;
- Betriebs- und Wartungssoftware;
- Anwendungssoftware;
- Mobilgeräte.

Abweichende Zielfristen gelten für Security Patches zur Behebung von Kritischen Schwachstellen innerhalb der Systeme. In diesen Fällen richten sich die Zeiträume nach dem Schweregrad der zu behebenden Schwachstelle und sind durch den Auftragnehmer nach Rücksprache mit der Bank festzulegen.

5.2 Datensicherung und -Wiederherstellung, Datentransport

Neben der Verfügbarkeit und der Authentizität gelten die Integrität und Vertraulichkeit von Informationen als gleichermaßen wichtig aus Sicht der Bank. Daher ist der Zugriff auf die Datensicherungen und Datenträger vor Unbefugten logisch und physisch zu schützen. Sicherungskopien sind so aufzubewahren, dass die Datenträger längerfristig aufbewahrt werden können. Die Sicherungsmedien sind so aufzubewahren, dass sie problemlos wieder aufgefunden werden können.

Es sind mindestens folgende Qualitäten und Frequenzen einzuhalten:

	Niedrig	Mittel	Hoch	Sehr Hoch
Integrität	monatliche Sicherung	wöchentliche Sicherung	tägliche Sicherung	
Verfügbarkeit	monatliche Sicherung	wöchentliche Sicherung	entsprechend der eigenen BCM-Festlegung, aber mind. tägliche Sicherung	

Das Rückeinspielen der vorliegenden Backup-Kopien muss jährlich geprüft werden. Die Funktionalität der Backup-Kopien muss stichprobenweise …

	Niedrig	Mittel	Hoch	Sehr Hoch
Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität	jährlich	halbjährlich	quartalsweise	

… geprüft werden. Reale Fälle einer Rückeinspielung im Betrieb können auf die Testfälle angerechnet werden.

Backup-Medien sind vor unbefugten Dritten logisch und physisch zu schützen.

Sofern Backup-Medien zwischen Rechenzentren außerhalb des gesicherten Geländes des Auftragnehmers transportiert werden, sind die Datenträger für den physischen Transport zu verschlüsseln und mit geeigneten physischen Maßnahmen abzusichern.

5.3 Protokollierung

Ereignisprotokolle die Benutzertätigkeiten, Ausnahmen, Störungen und Informationssicherheitsvorfälle aufzeichnen, müssen durch den Auftragnehmer erzeugt, aufbewahrt und regelmäßig überprüft werden.

Ereignisprotokolle enthalten unter Umständen sensible Informationen und müssen daher vor unbefugter Einsicht und Manipulation geschützt werden. Die Systemadministratoren sollen keine Befugnis haben, die Protokolle zu löschen. Die Deaktivierung der Protokollierungsfunktion muss ausschließlich nach dem 4-Augen-Prinzip geschehen und schriftlich dokumentiert sein (Grund, Zeitraum, Beteiligte).

Die Aufbewahrung der Protokolle richtet sich nach den geschäftsrelevanten Anforderungen, darf aber die gesetzlichen Regelungen oder regulatorische Vorgaben nicht verletzen.

Zur Verhinderung einer Manipulation der Protokolldateien können diese in ein dafür geeignetes SIEM (*Security Information and Event Management*) übertragen werden.

5.4 Zeitsynchronisation

Die Uhren aller informationsverarbeitenden Systeme sind mit einer Referenzzeitquelle zu synchronisieren.

5.5 Kryptografie

Kryptografische Systeme sind mindestens einzusetzen, wenn Daten über das öffentliche Netz (Internet) oder in ein als nicht ausreichend sicher geltendes Netzwerk übertragen werden. Dabei ist zu beachten, dass kryptografische Systeme jederzeit dem aktuellen Stand der Technik entsprechen müssen. Details sind mit der Bank abzusprechen.

Sensible und personenbezogene Daten sind angemessen zu schützen und, sofern technisch möglich, verschlüsselt zu speichern.

Der Auftragnehmer muss schriftlich dokumentieren, welche kryptographischen Verfahren zulässig sind bzw. verwendet werden und inwiefern Daten am Speicherort sowie Daten- und Kommunikationstransfers verschlüsselt werden. Der Auftragnehmer muss auch den Gebrauch, Schutz und den gesamten Lebenszyklus von Schlüsselmaterial dokumentieren.

Schlüssel, die Unbefugten zur Kenntnis gelangt sind, bei der Verteilung verfälscht worden sind oder aus unkontrollierter Quelle stammen, kompromittieren den kryptographischen Sicherheitsmechanismus unter Umständen genauso wie qualitativ schlechte Schlüssel, die auf ungeeignete Weise erzeugt worden sind. Solche Schlüssel und Schlüssel, die auf ungeeignete Weise erzeugt wurden, sind unverzüglich zu ersetzen.

5.6 Netzwerksicherheit

Folgende Aspekte sind durch den Auftragnehmer zu regeln:

- Verantwortlichkeiten und Verfahren für die Verwaltung der Netzwerktechnik;
- ob und wie eine Segmentierung in Sicherheitszonen umgesetzt wird;
- in welchen Fällen eine logische oder physische Netztrennung umgesetzt wird;
- welche Netz- und Anwendungsprotokolle zugelassen sind; und
- wie die interne, standortübergreifende und externe Kommunikation inklusive der erforderlichen Verschlüsselung erfolgt.

5.7 Firewall-Regeln

Jede Kommunikation zu externen Systemen oder Diensten muss über eine Firewall fließen (intern/extern). Des Weiteren muss sichergestellt werden, dass ausschließlich erlaubte Verbindungen aus dem Internet ins interne Netz (oder umgekehrt) aufgebaut werden (Whitelisting-Ansatz).

Um dies zu unterstützen, müssen eindeutige Firewall-Regeln für den Datenverkehr definiert werden. Alle vorhandenen Infrastruktur-Komponenten (z.B. Server), welche auf Verbindungen in nicht vertrauenswürdige Netze angewiesen sind (z.B. Internet), müssen im Rahmen ihres Datenverkehrs gewisse Kriterien erfüllen – diese werden als „**Firewall-Regeln**“ definiert.

Das Management der Firewall-Regeln muss mindestens folgende Kriterien erfüllen:

- Geregelter Freigabeprozess: Alle Änderungsanträge (Anlegen, Ändern, Löschen) müssen durch festgelegte Personen, die nicht mit dem jeweiligen Antragsteller identisch sind, formal beschlossen werden, bevor sie in Umsetzung gehen.
- Dokumentation: Alle Antrags- und Genehmigungsprozesse müssen schriftlich dokumentiert werden. Die letzte schriftliche Entscheidung je Firewall-Regel muss 24 Monate lang aufbewahrt werden.
- Rezertifizierung: Alle Firewall-Regeln müssen turnusmäßig, spätestens alle 12 Monate seit ihrer letzten Änderung, einer Rezertifizierung unterzogen werden. Nicht mehr benötigte Regeln sind im Rahmen der Rezertifizierung nach Rücksprache mit den Betroffenen zu löschen.
- Regelwerk: Alle Firewall-Regeln sind bei Bedarf (z.B. internes/externes Audit) in vollständiger und nachvollziehbarer Form der Bank vorzulegen (z.B. Auszug in Excel-Format).

5.8 Anschaffung und Instandhaltung von Software

Vor der Anschaffung von Hard- und Software, die der Auftragnehmer für die Leistungen (auch vor dem Bezug von Webanwendungen) einsetzt, muss er die genauen Anforderungen an die Informationssicherheit bestimmen, die sich aus dieser Informationssicherheitsanlage ergeben.

Der Auftragnehmer muss daher prüfen, welche Informationssicherheitsvorgaben aus dieser Informationssicherheitsanlage umzusetzen sind und ob die Soft- bzw. Hardware in der Lage ist, diese zu erfüllen. Ist die neu anzuschaffende Soft- bzw. Hardware nicht in der Lage, diese Anforderungen zu erfüllen, …

	Niedrig	Mittel	Hoch	Sehr Hoch
Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität	darf sie nicht ohne Beachtung entsprechender Auflagen der Bank		darf sie nicht	

… für die Leistungen eingesetzt werden.

5.9 Installation von Software im Betrieb

Bei der Installation von Software im Betrieb muss sichergestellt werden, dass:

- die Änderungskontrolle bei Software auf Systemen im Betrieb beachtet wird;
- die Aufgaben von geschulten Administratoren durchzuführen ist;
- die notwendigen internen Genehmigungen des Auftragnehmers vorliegen;
- die Software getestet wurde;
- eine Rollback-Strategie existiert; und
- die ersetzten Softwareversionen langfristig – die letzten 2 Versionen (Minor Release) – vorgehalten werden.

5.10 Redundanzen

IKT-Systeme sind vorbehaltlich spezifischer Regelungen des Hauptvertrages wie folgt auszulegen:

- Mindestverfügbarkeit von 95% bei niedrigem oder mittlerem Schutzbedarf und 99% bei hohem oder sehr hohem Schutzbedarf.
- Betrieb in getrennten Rechenzentren, sofern der Schutzbedarf hoch oder sehr hoch ist. Die Entfernung zwischen den Rechenzentren muss sich an den Empfehlungen des BSI orientieren.

5.11 Kapazitätsmanagement

Ein Ziel der Informationssicherheit ist unter anderem die nachhaltige Aufrechterhaltung der Verfügbarkeit von Informationen und damit der informationsverarbeitenden Systeme und Ressourcen. Die Nutzung von IT-Ressourcen ist zu überwacht und intern abzustimmen. Es sind Prognosen zu zukünftigen Kapazitätsanforderungen zu erstellen, um die erforderliche Systemleistung sicherzustellen.

5.12 Mobile Geräte

Den eingesetzten Mitarbeitern sind Vorgaben zum sicheren Umgang mit Mobilgeräten zu geben. Der Auftragnehmer hat die Implementierung ergänzender technischer Schutzmaßnahmen sicherzustellen, welche die Risiken aus der Nutzung von Mobilgeräten lindern, z.B. durch eine Verschlüsselung der Datenträger.

5.13 – einstweilen freibleibend –

5.14 Mobiles Arbeiten / Telearbeitsplätze

Den eingesetzten Mitarbeitern sind Vorgaben zum sicheren Umgang mit mobilem Arbeiten/Telearbeit zu geben. Der Auftragnehmer hat die Implementierung ergänzender technischer Schutzmaßnahmen sicherzustellen, weclhe die Risiken aus der Nutzung von mobilen Arbeiten/Telearbeiten mindern.

5.15 Entsorgung von Datenträgern und anderen Betriebsmitteln

Nicht mehr benötigte Datenträger sind sicher unter Anwendung formaler Verfahren zu entsorgen. Bei der Entsorgung von allen Betriebsmitteln muss sichergestellt werden, dass Datenträger sicher entsorgt werden.

Datenträger, die nicht entsorgt werden können, müssen sicher gelöscht werden. Dazu ist der gelöschte Datenträger mehrfach, mindestens…

	Niedrig	Mittel	Hoch	Sehr Hoch
Vertraulichkeit	3		7	

… mal mit Zufallsdaten zu überschreiben.

Die Entsorgung oder sichere Löschung von anderer Hardware (z.B. aus Leasing oder aus Eigentum des Auftragnehmers) ist mit der Bank vorab individuell abzustimmen.

5.16 Übertragung von Daten auf bewegliche Datenträger

Die Übertragung von Daten auf Datenträger (z.B. USB-Sticks, externe Festplatten, CDs, DVDs usw.) darf nicht ohne vorherige Freigabe der Bank erfolgen.

5.17 Transport von Datenträgern

Datenträger müssen vor unbefugtem Zugriff und Missbrauch geschützt verwahrt und transportiert werden, z.B. durch Verschlüsselung.

***