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

Standard "IT-Administrator"

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 | ISMS200004 | [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](#_Toc75207721)

[Dokumentenhistorie 3](#_Toc75207722)

[Inhaltsverzeichnis 4](#_Toc75207723)

[Allgemeine Festlegungen 6](#_Toc75207724)

[Ziel / Zweck 6](#_Toc75207725)

[Geltungsbereich 6](#_Toc75207726)

[Zuständigkeiten 6](#_Toc75207727)

[Genehmigungs- und Änderungsverfahren 6](#_Toc75207728)

[Standard "IT-Administration" 7](#_Toc75207729)

[Allgemeine Vorgaben 7](#_Toc75207730)

[Planung, Beschaffung und Freigabe von IT-Systemen 7](#_Toc75207731)

[Administrative Aufgaben 7](#_Toc75207732)

[Allgemeine Anforderungen 7](#_Toc75207733)

[Zugangskontrolle, Berechtigungsmanagement und Administrationszugriffe 8](#_Toc75207734)

[Administrations-, Installations- und Konfigurationstätigkeiten 9](#_Toc75207735)

[Entwicklung, Test und Freigabe 9](#_Toc75207736)

[Systemhärtung 9](#_Toc75207737)

[Migration 10](#_Toc75207738)

[Sicherheitszonen (Netz) 10](#_Toc75207739)

[Patch- und Änderungsmanagement 11](#_Toc75207740)

[Kryptographie 12](#_Toc75207741)

[Schutz vor Schadprogrammen 12](#_Toc75207742)

[Protokollierung und Monitoring 13](#_Toc75207743)

[Schwachstellenmanagement 13](#_Toc75207744)

[Behandlung von Sicherheitsvorfällen und IT-Forensik 13](#_Toc75207745)

[Datensicherung 14](#_Toc75207746)

[Penetrationstests 14](#_Toc75207747)

[Redundanzen 14](#_Toc75207748)

[IT-Infrastruktur 14](#_Toc75207749)

[Client-Systeme 14](#_Toc75207750)

[Mobile Endgeräte und Mobile Device Management (MDM) 15](#_Toc75207751)

[Server-Systeme 15](#_Toc75207752)

[Virtualisierung 16](#_Toc75207753)

[Telekommunikation und VoIP 16](#_Toc75207754)

[Drucker, Kopierer und Multifunktionsgeräte 17](#_Toc75207755)

[Netze und Kommunikationsverbindungen 18](#_Toc75207756)

[Firewalls 18](#_Toc75207757)

[Physische Sicherheitszonen 19](#_Toc75207758)

[Anwendungen, Webanwendungen und Webservices 19](#_Toc75207759)

[Datenbanken 19](#_Toc75207760)

[Fileserver 20](#_Toc75207761)

[Sensibilisierung und Schulung 20](#_Toc75207762)

[Audits und Revision 20](#_Toc75207763)

[Löschen und Vernichten von Informationen 21](#_Toc75207764)

[Außerbetriebnahme und Aussonderung von IT-Systemen 21](#_Toc75207765)

[Notfallmanagement 22](#_Toc75207766)

# Allgemeine Festlegungen

## Ziel / Zweck

Ausgehend von der allgemeinen Leitlinie zur Informationssicherheit sind die wesentlichen Kernaspekte für eine sichere Administration von IT-Systeme und -Anwendungen zu konkretisieren. Das vorliegende Dokument definiert verbindliche Vorgaben zur Beschaffung, Installation, Konfiguration und Administration von IT-Systemen und -Anwendungen sowie den darauf befindlichen Inhalten, welche durch die <Institution> verantwortet werden. Da die Geschäftstätigkeit an die ordnungsgemäße Funktion der in der Verantwortung der <Institution> befindlichen bzw. genutzten IT-Systeme und -Anwendungen gekoppelt ist, sind alle notwendigen Maßnahmen und Verfahren im Rahmen des Standards „IT-Administration“ zu beachten und ausreichend zu dokumentieren.

## 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

Der Standard „IT-Administrator“ 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>.

# Standard "IT-Administration"

## Allgemeine Vorgaben

### Planung, Beschaffung und Freigabe von IT-Systemen

Bei der Beschaffung von IT-Komponenten (Hard- und Software) bzw. Cloud-Ressourcen sind die Sicherheitsanforderungen an die IT-Komponenten bereits in der Planungsphase zu berücksichtigen. Insofern davon auszugehen ist, dass hohe Sicherheitsanforderungen an die IT-Komponente gestellt werden, ist der <Informationssicherheitsbeauftragter> in die Planungsaktivitäten einzubeziehen. Für den Fall, dass darüber hinaus personenbezogene Daten durch die IT-Komponente verarbeitet werden, ist zusätzlich der <Datenschutzbeauftragter> einzubeziehen.

### Administrative Aufgaben

Die Verantwortlichen für die IT-Administration sind für die ordnungsmäßige Installation und Betrieb von Anwendungen, IT-Systemen und Netzwerken zuständig. Diese Zuständigkeit umfasst dabei die Installation, Wartung und Überwachung von IT-Systemen und Netzwerken sowie den damit verbundenen Betriebssystemen und Anwendungen sowie deren Dokumentation. In diesem Zusammenhang nehmen die Verantwortlichen für die IT-Administration Tätigkeiten in den folgenden Bereichen wahr:

* Berechtigungsmanagement
* Schwachstellenmanagement
* In- und Außerbetriebnahme von IT-Systemen
* Änderungen an Daten und Logik von IT-Systemen und -Anwendungen
* Patch- und Change-Management

### Allgemeine Anforderungen

Für jedes IT-System ist grundsätzlich ein verantwortlicher Administrator bzw. Organisationseinheit zu benennen. Zur Vermeidung von Notsituationen sind angemessene Stellvertreterregelungen zu etablieren. Dabei sind die folgenden Aspekte zu berücksichtigen:

* Die Stellvertreterregelungen sind zentral zu dokumentieren und zu publizieren.
* Die benannten Stellvertreter sind jederzeit über die aktuelle Systemkonfiguration zu informieren.
* Den benannten Stellvertretern ist Zugriff auf die zur Administration notwendigen Authentifizierungsmerkmale zu geben.

### Zugangskontrolle, Berechtigungsmanagement und Administrationszugriffe

Gemäß der Sicherheitsrichtlinie „Identitäts- und Berechtigungsmanagement“ erfolgt die Berechtigungsvergabe grundsätzlich durch autorisierte Mitarbeiter. In Abstimmung mit dem <Informationssicherheitsbeauftragter> und dem <Notfallbeauftragter> kann eine alternative Berechtigungsvergabe durch den verantwortlichen Bereich erfolgen. Entsprechend den Anforderungen gemäß Sicherheitsrichtlinie „Identitäts- und Berechtigungsmanagement“ gelten folgende Vorgaben:

* Für IT-Anwendungen und -Systeme ist zu überprüfen, ob herstellereigene Default-Benutzerkonten und -Passwörter vorliegen, die nicht geändert oder gelöscht werden können. In diesem Fall sind entsprechende Korrekturmaßnahmen einzuleiten.
* Passwörter müssen auf Basis der Empfehlung „Umgang mit Passwörtern“ angewandt werden.
* Insofern eine Protokollierung von Fehleingaben technisch möglich ist, ist diese umzusetzen.

Für administrative Benutzer sind zusätzlich die folgenden Anforderungen einzuhalten:

* Die Administratoren der <Institution> sind für den Schutz ihrer Legitimationsmedien zuständig.
* Administrative Benutzerkonten dürfen nicht durch andere Benutzer verwendet werden.

Für technische Benutzerkonten sind zusätzlich die folgenden Anforderungen einzuhalten:

* Technische Benutzerkonten sind für den Login von Personen unzulässig.
* Es ist sicherzustellen, dass technische Benutzerkonten nie ablaufen.
* Legitimationsmedien technischer Benutzer sind sicher aufzubewahren und regelmäßig auf Missbrauch zu überprüfen.

Die Verwaltung von Benutzerzugängen und den dazugehörigen Berechtigungen hat über ein zentrales System zu erfolgen. Insofern sich IT-Systeme und -Anwendungen nicht in dieses System integrieren lassen, sind angemessene Konzepte vorzulegen.

Benutzer- und Administratorenzugänge sind vor ihrer Löschung für eine Dauer von drei Monaten zu sperren. Insofern eine Löschung nicht möglich ist, sind die Zugänge dauerhaft zu sperren. Ein Verlust von Daten der <Institution> oder des Zugriffs auf relevante Daten und Systeme muss bei der Sperrung oder Löschung ausgeschlossen sein.

Businessrollen der <Institution> haben auf den Geschäftsprozessen der Organisationseinheit zu basieren und sind als Dateneigentümer zu deklarieren. Im Rahmen des Berechtigungsmanagements sind grundsätzlich „sprechende“ Bezeichnungen für Rollen und Verantwortlichkeiten zu wählen.

Bei der Fernwartung von IT-Systemen und -Anwendungen sind die Anforderungen der Sicherheitsrichtlinie „Fernwartung“ einzuhalten. Daher ist die Verwendung von Fernwartung grundsätzlich als kritisch anzusehen. Es sind die folgenden Anforderungen bei der Durchführung von Fernwartungen mindestens zu beachten:

* Die Übertragung von Daten auf das IT-System des Fernwartungspersonals ist zu unterbinden.
* Der nicht-lokale Zugriff auf Server ist nur mittels freigegebener Verschlüsselungsverfahren durchzuführen.
* Bei unbeaufsichtigter Fernwartung sind alle Tätigkeiten der Session zu protokollieren, zu archivieren und bei Bedarf für forensische Zwecke zur Verfügung zu stellen.

### Administrations-, Installations- und Konfigurationstätigkeiten

Die Inbetriebnahme und Installation von IT-Systemen und -Anwendungen in der Verantwortung der <Institution> hat unter Berücksichtigung der freigegebenen Sicherheitsrichtlinie der entsprechenden IT-Komponente oder Anwendung zu erfolgen. Zusätzlich sind vorhanden Handlungsempfehlungen für die Installation und Konfiguration einzuhalten. In begründeten Ausnahmefällen können Sonderregelungen beim <Informationssicherheitsbeauftragter> beantragt werden. Insofern durch diese Sonderregelungen personenbezogene Daten betroffen sind, ist das Vorgehen zusätzlich mit dem <Datenschutzbeauftragter> abzustimmen. Sollten durch die Sonderregelungen bestehende Notfallmanagement-Konzepte betroffen sein, ist der <Notfallbeauftragter> mit einzubinden.

### Entwicklung, Test und Freigabe

Die Entwicklung, Überprüfung und Freigabe von Anwendungen hat gemäß den Anforderungen der Sicherheitsrichtlinie „Entwicklung und Einsatz von Allgemeinen Anwendungen“ sowie der Sicherheitsrichtlinie „Software-Tests und Freigaben“ zu erfolgen. Darüber sind die folgenden Vorgaben zu berücksichtigen:

* Die Anwendung und ihr zugrundeliegender Quellcode ist angemessen zu dokumentieren.
* Die in der jeweiligen Programmiersprache zutreffende Sicherheitsmaßnahmen sind zu berücksichtigen.
* Jeglicher Quellcode ist in einem Versionsverwaltungssystem zu pflegen und vor unberechtigter Einsichtnahme und Manipulation zu schützen.
* Die Schutzmaßnahmen der Testumgebung hat dem der Produktivumgebung zu entsprechen.
* Bei der Entwicklung von Individualsoftware durch Dienstleister sind Use-Cases, Anforderungen, Dokumentations- und Abnahmekriterien sowie Vorgaben an das Urheberrecht vertraglich festzuhalten.

Vor der Übernahme in den Betrieb ist die Anwendung einem dokumentierten Test- und Freigabeprozess zu unterziehen, bei dem alle sicherheitsrelevanten Funktionen abzunehmen sind. Im Rahmen der Freigabe ist für die einzuführende Software der Schutzbedarf zu definieren.

Die Administration und Nutzung der Anwendung darf erst nach einer entsprechenden Anwenderschulung und sofern benötigt nach der Freigabe durch die Vorgesetzten erfolgen.

### Systemhärtung

IT-Systeme und -Anwendungen sind auf Basis der Vorgaben der referenzierten Sicherheitsrichtlinien angemessenen Härtungsmaßnahmen zu unterziehen.

Insbesondere für Netzwerkkomponenten sind dabei die Vorgaben der entsprechenden Sicherheitsrichtlinien zu beachten. An dieser Stelle sind die wichtigsten zu beachtenden Themen aufgeführt:

* Client- bzw. Server-Systeme haben ihre IP-Adresse ausschließlich durch autorisierte Systeme zu erhalten.
* Sichere Grundkonfiguration
* Einspielen von Updates und Patches
* Restriktive Rechtevergabe
* Identitäts- und Berechtigungsmanagement
* Schutz der Administrationsschnittstellen
* Administration über ein gesondertes Managementnetz
* Protokollierung
* Sicherheitsaspekte von Routing-Protokollen
* Bogon- und Spoofing-Filterung
* Schutz vor "IPv6 Routing Header Type-0"-Angriffen
* Schutz vor DoS- und DDoS-Angriffen
* Schutz vor Missbrauch von ICMP-Nachrichten
* Schutz vor Fragmentierungsangriffen
* Einsatz von Netzzugangskontrollen
* Notfallzugriff auf Netzkomponenten
* Die Systemzeit ist über eine zentrale Zeitsteuerung zu synchronisieren.
* Lokale Administratorkonto sind umzubenennen und mit einem starken Passwort zu versehen.

Zusätzlich sind bei der Härtung von Servern die folgenden Vorgaben umzusetzen:

* Es sind ausschließlich die zur Aufgabenerfüllung notwendigen Pakete zu installieren.
* Nicht verwendete Dienste und Protokolle sind zu deaktivieren.
* Jeder Dienst hat über ein eigenes Dienstkonto zu laufen.
* Die Systemzeit ist über eine zentrale Zeitsteuerung zu synchronisieren.
* Lokale Administratorkonten sind umzubenennen und mit einem starken Passwort zu versehen.
* Eine direkte Anmeldung am Server als Administrator über das Netzwerk ist zu unterbinden.

### Migration

Für die Datenmigration von IT-Systemen und -Anwendungen sind die Vorgaben der jeweiligen Betriebshandbücher und Herstellerempfehlungen einzuhalten. Migrationstätigkeiten sind zu dokumentieren und möglichst von einem zentralen Managementsystem aus durchzuführen.

### Sicherheitszonen (Netz)

Netze sind in Sicherheitsbereiche und zugehörigen Sicherheitszonen zu unterteilen, die mit entsprechenden Schutzmaßnahmen abzusichern sind. Dabei sind die folgenden zusätzlichen Vorgaben zu berücksichtigen:

* Grundsätzlich dürfen keine direkten IP-Verbindung aus dem öffentlichen Netz im Netz der <Institution> existieren.
* Alle externen Verbindungen sind durch Sicherheitsgateways zu terminieren und zu authentisieren.
* Der Aufbau von Netzschnittstellen zu externen Netzen sowie die Änderung der Netzarchitektur ist mit dem Sicherheitsmanagement der <Institution> abzustimmen.

Ferner sind die betrieblichen und sicherheitsrelevanten Vorgaben des Zonenkonzepts umzusetzen.

### Patch- und Änderungsmanagement

Das Patch- und Änderungsmanagement hat gemäß den Anforderungen der korrespondierenden Sicherheitsrichtlinie zu erfolgen. Zusätzlich sind die folgenden Anforderungen zu berücksichtigen:

* Änderungen sind vom jeweiligen System- oder Anwendungsverantwortlichen fachlich zu beurteilen.
* Änderungen, die eine Freigabe benötigen, sind durch ein Change-Advisory-Board freizugeben.
* Rollbackszenarien sind für den Fall von Störungen zu entwickeln und bei Bedarf umzusetzen.

Bei der Ausführung von Patches und Updates sind zusätzlich die Anforderungen der Servicevereinbarungen und etablierten Architekturen zu berücksichtigen:

* Es ist ein spezifisches Zeitfenster für die Durchführung von Änderungen mit Serviceauswirkungen mit den Kunden zu definieren und zu berücksichtigen.
* Updates sind vor ihrer Ausführung zu testen und die Release Notes des Herstellers zu berücksichtigen.
* Die Systemperformance ist bei der Ausführung von Änderungen zu berücksichtigen.

Für die Planung für Patches und Updates ist folgendes zu berücksichtigen:

* Der Ablauf, Zeitplan und Einsatz von Werkzeugen ist zu dokumentieren.
* Patches sind ausschließlich in den vorgesehenen Wartungsfenstern zu installieren.

Beim Einspielen von Patches und Updates sind die folgenden Anforderungen zu berücksichtigen:

* Patches sind im Rahmen des Änderungsmanagements an die betroffenen Mitarbeitende zu kommunizieren.
* Insofern Härtungsmaßnahmen durch das Einspielen von Patches geändert werden, sind diese wiederherzustellen oder durch Alternative mit dem Informationssicherheitsbeauftragten abgestimmte Härtungsmaßnahmen zu ersetzen.

Die Durchführung von Patches und Änderungen hat über Werkzeuge zu erfolgen, welche die folgenden Aspekte berücksichtigen:

* Eingesetzte Werkzeuge müssen in der Lage sein, gegenwärtige und zukünftige Anforderungen zu erfüllen.
* Die eingesetzten Werkzeuge sind in einem separaten Netzwerksegment (Sicherheitsbereich „Administration“ zu platzieren.

### Kryptographie

Die Auswahl und der Einsatz von kryptographischen Maßnahmen erfolgt gemäß den internen Vorgaben aus der Sicherheitsrichtlinie und den freigegebenen Protokollen, kryptographischen Algorithmen und Werten. Der jeweilige system- oder anwendungsverantwortliche Administrator/Entwickler ist für die ordnungsgemäße Konfiguration kryptografischer Funktionen zuständig. Dafür hat der Administrator/Entwickler entsprechende Kenntnisse vorzuweisen bzw. muss die Möglichkeit besitzen, sich diese anzueignen.

Für den Betrieb von kryptographischen Produkten gelten die folgenden Anforderungen:

* Bekanntgewordene Schwächen in kryptographischen Produkten sind unverzüglich zu schließen.
* Kryptographischen Produkten und Verfahren ist derselbe Schutzbedarf wie dem geschützten Informationswert zuzukommen.

Die <Institution> hat für das Schlüsselmanagement folgendes zu berücksichtigen:

* Es ist eine Zugriffs- und Vertreterregelung zu etablieren.
* Außer Betrieb genommenes Schlüsselmaterial ist in separaten Teilen sicher aufzubewahren.

In der <Institution> dürfen ausschließlich etablierte und freigegebene kryptographische Verfahren eingesetzt werden.

### Schutz vor Schadprogrammen

Der Virenschutz der <Institution> hat gemäß den Anforderungen der korrespondierenden Sicherheitsrichtlinie zu erfolgen. Der Virenschutz sollte zentral verwaltet und betreiben werden. Dabei hat der Virenschutz mehrstufig unter Verwendung verschiedener Produkte zu erfolgen.

Im Falle eines Virenbefalls ist zu überprüfen, ob das betroffene System zur Beweissicherung die Netzkommunikation zu unterbinden oder außer Betrieb zu nehmen ist. Sofern dies nicht erforderlich ist, ist das System zu bereinigen und neu aufzusetzen.

Potenziell gefährliche Inhalte sind aus E-Mails automatisch zu entfernen. Dabei sind die folgenden Anforderungen zu berücksichtigen:

* Eingehende E-Mails sind durch ein zentrales Virusprogramm zu überprüfen.
* Sollten E-Mails in Folge einer Überprüfung unterdrückt werden, ist der Mitarbeitende darüber zu informieren.

Die zentrale Virenschutzsoftware ist im Rahmen des Patchmanagements zu aktualisieren. Die Virenschutzsoftware ist dabei so zu konfigurieren, dass Änderungen sicherheitsrelevanter Einstellung insbesondere durch Benutzer oder nicht autorisierte Administratoren nicht möglich sind.

### Protokollierung und Monitoring

Die Überwachung von IT-Systemen und Anwendungen hat auf Basis der hierfür erstellten Sicherheitsrichtlinien zu erfolgen. Kritische IT-Systeme und -Anwendungen der <Institution> sind dabei permanent zu überwachen. Für die Protokollierung und das Monitoring sind die folgenden zusätzlichen Aspekte zu berücksichtigen:

* Der Zugriff auf Log-Dateien erfolgt ausschließlich zur Aufklärung von Unregelmäßigkeiten sowie zum Erkennen und Behandeln von Sicherheitsvorfällen.
* Die Weitergabe von Log-Dateien für etwaige interne Revisionen oder Überprüfungen erfolgt ausschließlich durch Administratoren.
* Bei der Überwachung von kritischen IT-Systeme und -Anwendungen haben automatische Alarmierungen zu erfolgen.
* Die Protokollierung und Überwachung ist jederzeit aktiv zu halten.
* Bei der Auswertung von Aufzeichnungen sind datenschutzrechtliche Bestimmungen und etablierte Vereinbarungen einzuhalten.

### Schwachstellenmanagement

IT-Systeme und -Anwendungen der <Institution> sind durch angemessene Verfahren auf Schwachstellen zu überwachen. Für die Identifizierung von Schwachstellen sind zusätzlich eingängige und vertrauenswürdige Quellen zu berücksichtigen.

Identifizierte Schwachstellen sind bezüglich ihrer Kritikalität zu bewerten. Insofern keine sicherheitsrelevanten Patches bereitstehen, sind geeignete Korrekturmaßnahmen abzuleiten. Die Behandlung der Schwachstellen hat im Rahmen des Änderungsmanagements der <Institution> zu erfolgen.

Zusätzlich sind die IT-Systeme und Anwendungen regelmäßigen Sicherheitschecks zu unterziehen. Dabei sind die folgenden Anforderungen einzuhalten:

* Soll-Ist-Vergleiche zwischen der Dokumentation und der tatsächlichen Konfiguration sind durchzuführen.
* Sicherheitschecks sind ausschließlich durch qualifizierte Personen durchzuführen.
* Die Ergebnisse der Sicherheitschecks sind zu dokumentieren und dem Informationssicherheitsbeauftragten vorzulegen.

### Behandlung von Sicherheitsvorfällen und IT-Forensik

Sicherheitsvorfälle sind gemäß den internen Vorgaben der <Institution> zu behandeln. Die Administratoren/Entwickler des IT-Systems bzw. der Anwendung sind dazu angehalten, der Detektion von IT-Sicherheitsvorfällen rechtzeitig beizutragen. Bei der Behandlung von Sicherheitsvorfällen und Beweissicherung sind zusätzlich die folgenden Anforderungen zu berücksichtigen:

* Die Administratoren sind regelmäßig im Umgang mit Beweissicherungsmaßnahmen zu schulen. Bei der Beauftragung von externen Dienstleistern sind entsprechende Qualifikationen vorzuweisen.
* Insofern sich durch einen Sicherheitsvorfall Integritätsverluste ergeben, ist die entsprechende Komponente vor der Durchführung von Untersuchungsmaßnahmen vom System zu isolieren.
* Sicherheitsvorfalls- und Beweissicherungsmaßnahmen sind im jeweiligen Betriebshandbuch zu dokumentieren.

### Datensicherung

Bei der Sicherung von Daten sind die Vorgaben der freigegebenen Sicherheitsrichtlinie einzuhalten. Die Verantwortlichen der IT-Systeme und -Anwendungen sind für die konkrete Häufigkeit und Ausgestaltung der Datensicherung zuständig:

* Regulatorische Anforderungen sind bei der Ausgestaltung der Datensicherung zu berücksichtigen.
* Alle Konfigurationen von IT-Systemen und -Anwendungen sind auf geeigneten Speichermedien abzusichern.
* Jede Datensicherung unterliegt der Dokumentationspflicht.
* Bei der Durchführung von Patches sind diejenigen Daten zu sichern, die vom Patch betroffen sind.

### Penetrationstests

Penetrationstests sind vom <Informationssicherheitsbeauftragter> zu initiieren oder auf Anforderung des Fachbereichs durchzuführen. Dabei sind die folgenden Vorgaben zu berücksichtigen:

* Jedes IT-System und jede IT-Anwendung ist einem jährlichen Penetrationstest zu unterziehen.
* Relevante Dritte und Dienstleister sind gemäß den regulatorischen Anforderungen angemessen in die Durchführung von Penetrationstests zu involvieren.
* Penetrationstests sind ausschließlich durch qualifizierte Personen durchzuführen.
* Die Ergebnisse des Penetrationstests sind zu dokumentieren und dem Informationssicherheitsbeauftragten vorzulegen.

### Redundanzen

IT-Systeme und -Anwendungen sind gemäß deren vertraglich vereinbarten Verfügbarkeitsanforderungen redundant vorzuhalten.

## IT-Infrastruktur

### Client-Systeme

Client-Systeme sind gemäß den Vorgaben der Sicherheitsrichtlinie „Windows-Clients“, „Unix-Clients“ bzw. „MacOS Clients“ abzusichern. Im Falle von mobilen Arbeitsplätzen ist zusätzlich die Sicherheitsrichtlinie „Mobiler Arbeitsplatz“ einzuhalten. Bezüglich der Konfigurationen von Client-Systemen sind die folgenden Anforderungen zu berücksichtigen:

* Nicht benötigte Benutzerkonten, Schnittstellen und Dienste sind zu deaktivieren.
* Externe Peripheriegeräte sind nach Gebrauch abzuschalten.
* Die Festplatten von Notebooks sind zu verschlüsseln.
* Insofern Clients in Fremdnetzen betrieben werden, sind sie über lokale Firewalls zu schützen.

Ferner sind die folgenden zentralen Vorgaben einzuhalten:

* Ein zentrales Steuerungskonzept ist zur Vorgabe von Gruppenrichtlinien zu nutzen.
* Insofern ein Benutzer in Ausnahmefällen Installationen durchführen muss, sind ihm die jeweiligen Rechte temporär einzuräumen.

### Mobile Endgeräte und Mobile Device Management (MDM)

Bei der Administration von mobilen Endgeräten sind die Vorgaben der Sicherheitsrichtlinie „Mobile Device Management“ zu gewährleisten. Darüber hinaus sind folgenden Anforderungen umzusetzen:

* Alle unternehmensrelevanten Daten der <Institution> auf mobilen Endgeräten sind vollständig zu verschlüsseln.
* Mobile Endgeräte sind mit geeigneten Maßnahmen gegen nicht-autorisierte Einsichtnahmen oder Diebstahl zu sichern.
* Mobile Endgeräte, die von verschiedenen Benutzern verwendet werden, sind in einem zutrittsgesicherten Raum aufzubewahren.
* Die Herausgabe von mobilen Endgeräten ist durch den Vorgesetzten freizugeben und nach einem definierten Prozess durchzuführen.
* Externe Zusatzspeicherkarten sind ausschließlich zur Erweiterung des Hauptspeichers zu verwenden.
* Das mobile Endgerät ist nach einer definierten Anzahl an Fehlversuchen automatisch zu löschen und zu sperren.
* Aktive lokale Paketfilter oder Firewalls sind nach dem Need-to-know-Prinzip zu konfigurieren.
* Insofern externe Schnittstellen genutzt werden, sind diese in ihrer Sichtbarkeit auf die notwendige Dauer zu begrenzen.
* Die Verwendung von unsicheren Schnittstellen ist zu unterbinden.

### Server-Systeme

Für die Inbetriebnahme, Installation und Konfiguration von Server-Systemen sind die zentralen Vorgaben zur Installation und Konfiguration von IT-Systemen und -Anwendungen einzuhalten. Neben den jeweiligen Betriebshandbüchern sind zusätzlich die Sicherheitsrichtlinien zum „Patch- und Änderungsmanagement“, „Datensicherung“ sowie „Protokollierung“ zu berücksichtigen.

Bei der Installation, Grundkonfiguration und Administration der jeweiligen Server-Typen sind die Sicherheitsrichtlinien „Fileserver“, „Webserver“, „Windows-Server“, „Unix-Server“ sowie „DNS-Server“ einzuhalten.

Server-Systeme sind in der Notfallplanung wie folgt zu berücksichtigen:

* Als Grundlage von Notfallmaßnahmen ist das Notfallhandbuch für Server zu berücksichtigen.
* Für den Notfall müssen entsprechende Bootmedien zur Verfügung stehen, mit denen die physischen Server in einen kontrollierten Zustand überführt werden können.

### Virtualisierung

Virtualisierungsplattformen sind gemäß der Sicherheitsrichtlinie „Virtualisierung“ sowie den allgemeinen Vorgaben zur Inbetriebnahme und Konfiguration von Systemen zu betreiben.

Hinsichtlich der Grund-Konfiguration von Virtualisierungsplattformen sind zusätzlich die folgenden Anforderungen zu berücksichtigen:

* Vor der Inbetriebnahme sind angemessene Performance- und Ressourcenanforderungen für die virtuellen IT-Systeme zu definieren.
* Wiederkehrende Administrationsmaßnahmen sind in einem Betriebshandbuch zu dokumentieren.
* Funktionen, die zur Überbuchung des Hauptspeichers genutzt werden können, sind zu deaktivieren.

Virtualisierungsplattformen sind gemäß der Sicherheitsrichtlinie „Patch- und Änderungsmanagement“ zu ändern und zu aktualisieren. Darüber hinaus sind die folgenden Vorgaben zu berücksichtigen:

* Vor dem Einspielen eines Updates ist sicherzustellen, dass entsprechende Sicherheitskopien angefertigt wurden und das mittels eines Roll-back-Plans im Notfall die ursprüngliche Situation wiederhergestellt werden kann.
* Auf der Virtualisierungsplattform hinterlegte Applikationen sind ausschließlich zentral zu aktualisieren.

Virtualisierungsplattformen sind grundsätzlich in der Notfallplanung wie folgt zu berücksichtigen:

* Als Grundlage von Notfallmaßnahmen ist das Notfallhandbuch für Virtualisierungsplattformen zu beachten.
* Der Schutzbedarf der Virtualisierungsplattform hat sich an dem Schutzbedarf der zugrundeliegenden Komponenten und verarbeiteten Anwendungen zu orientieren.
* Es sind Architekturen und Wiederanlaufpläne zu erstellen, die den geregelten Neustart der virtuellen Systeme ermöglichen.
* Die Wiederinbetriebnahme eines Virtualisierungssystems darf nicht von einem Dienst eines virtuellen IT-Systems abhängen.
* Die Dokumentation der Systemkonfiguration ist so zu gestalten, dass ein kontrolliertes Konfigurieren auch in Notfällen möglich ist.
* Bei Kompromittierung des Virtualisierungsservers sind die Passwörter der jeweiligen Verwaltungskonten zu ändern.

### Telekommunikation und VoIP

Telekommunikationsanlagen sowie VoIP-Middleware-Lösungen sind entsprechend den folgenden allgemeinen Anforderungen zu betreiben:

* Administratoren für den Betrieb und die Wartung von Telekommunikationsinfrastrukturen sind festzulegen.
* Die Telekommunikationsanlage bzw. VoIP-Middleware ist in zutrittsgesicherten Räumlichkeiten zu betreiben.

Hinsichtlich der Konfiguration von Telekommunikationsanlagen sind zusätzlich die folgenden Vorgaben zu beachten:

* Es sind die Vorgaben der freigegebenen Sicherheitsrichtlinien angemessen umzusetzen und zu dokumentieren.
* Für die Administration der VoIP, UC bzw. TK-Anlagen sind geeignete Administrationswerkzeuge zu etablieren und zu dokumentieren.
* Voreingestellte Passwörter sind zu ändern.
* Wartungs- und Fernzugriffe sind durch geeignete technische und organisatorische Maßnahmen abzusichern.
* Telefonate und Signalisierungen sind zu verschlüsseln.
* Medienschlüssel sind regelmäßig auszutauschen.

VoIP-Anlagen sind gemäß den zentralen Vorgaben zum Patch- und Änderungsmanagement, zur Datensicherung sowie zum Berechtigungsmanagement zu betreiben.

Die Protokollierung und Überwachung von Telekommunikations- und VoIP-Anlagen erfolgt unter Rücksprache mit dem <Datenschutzbeauftragter >.

### Drucker, Kopierer und Multifunktionsgeräte

Bei der Verwendung von Drucker, Kopierern und sonstigen Multifunktionsgeräten sind die Vorgaben der Sicherheitsrichtlinie „Drucker, Kopierer und Multifunktionsgeräte“ einzuhalten. Ferner sind die jeweiligen Sicherheitsrichtlinien bzgl. des Zugriffs, der Härtung und etwaigen Verschlüsselung von papierverarbeitenden Geräten zu beachten.

Für die Platzierung und den Zutritt zu papierverarbeiten Geräten sind zusätzlich die folgenden Vorgaben zu berücksichtigen:

* Die Geräte sind so zu platzieren, dass ein unberechtigtes Auslesen von Dokumenten durch Dritte nicht möglich ist.
* Die Geräte sind so zu platzieren, dass sie von eigenem Personal gut eingesehen werden können oder der entsprechende Bereich nur durch interne Mitarbeitende oder Dienstleister zugänglich ist.

Papierverarbeitende Geräte werden ausschließlich kabelgebunden mit dem Netzwerk verbunden und in Betrieb genommen.

Die Festplatten von papierverarbeitenden Geräten sind vor unberechtigtem Auslesen und Diebstahl zu schützen. Alternativ sind papierverarbeitende Geräte so zu konfigurieren, dass die Druck-Dateien unmittelbar nach dem Ausführen gelöscht werden. Insofern papierverarbeitende Geräte oder ihre Komponenten außer Betrieb genommen werden, sind alle sicherheitsrelevanten Informationen von den Geräten zu löschen. Insbesondere bei vertraulichen Informationen sind die Speicherkomponenten physisch zu zerstören. Verbrauchsmaterialien sowie redundante Komponenten sind gemäß den Vorgaben des Notfallmanagements ausreichend vorzuhalten.

### Netze und Kommunikationsverbindungen

Beim Aufbau, Betrieb, Administration und Überwachung von Netzen und Kommunikationsverbindungen sind die Vorgaben der Sicherheitsrichtlinien „Netz und Netzmanagement“, „WLAN-Betrieb“ sowie „Router und Switche“ einzuhalten.

Durch den jeweiligen Netzwerkadministrator ist die angemessene Dokumentation der Netzwerkstrukturen und -Komponenten sicherzustellen. Die Namenskonvention für entsprechende Netze und Komponenten sind zentral zu erstellen und einzuhalten.

Bei der physischen und logischen Segmentierung und Separierung von Netzwerken sind die betrieblichen und sicherheitsrelevanten Anforderungen zu berücksichtigen. Zur Kommunikation zwischen unterschiedlichen Netzwerksegmenten und insbesondere dem öffentlichen Netzwerk sind ausschließlich sichere Protokolle zu verwenden. Dynamisches Routing ist nur dann einzusetzen, wenn es durch eine betriebliche Notwendigkeit unabdingbar ist.

Neben den zentralen Vorgaben zur Protokollierung und Überwachung ist die Auslastung der jeweiligen Netze zu überwachen.

Bei der Härtung von Netzwerkkomponenten sind die zentralen Vorgaben zur Härtung von IT-Systemen und -Anwendungen sowie die Härtungs-Leitfäden der Hersteller zu beachten.

Patches und Updates an Netzwerkkomponenten sind gemäß der Sicherheitsrichtlinie „Patch- und Änderungsmanagement“ durchzuführen.

Die Datensicherung und Wiederherstellung hat gemäß den globalen Anforderungen sowie den Vorgaben der Sicherheitsrichtlinie „Datensicherung“ zu erfolgen.

### Firewalls

Bei der Auswahl, dem Betrieb und der Konfiguration von Sicherheitsgateways bzw. Firewalls sind die Vorgaben der Sicherheitsrichtlinie „Firewall“ umzusetzen. Die zentralen Vorgaben der Sicherheitsrichtlinien „Patch- und Änderungsmanagement“, Systemhärtung, „Protokollierung“ sowie Notfallmanagement sind zu erfüllen. Darüber hinaus sind die folgenden Anforderungen zu beachten:

* Firewalls sind vor unautorisiertem Zugang oder Manipulation zu schützen.
* Die Verfügbarkeit der Firewall hat sich aus den Verfügbarkeitsanforderungen an die zu überwachende Netzwerkschnittstelle zu ergeben.
* Der Firewall-Regelsatz ist anhand der zu überwachenden Dienste und Protokolle sowie der betrieblichen Notwendigkeit auszurichten.
* Dem <Informationssicherheitsbeauftragter> ist regelmäßig ein zusammengefasstes Bedrohungsbild aller Firewall-Abweisungen vorzulegen.
* Firewalls sind an das zentrale SIEM anzubinden, sodass kritische Ereignisse (insbesondere sicherheitskritische Ereignisse) unverzüglich an die Verantwortlichen kommuniziert werden.
* Jegliche Veränderungen an den Firewall-Einstellungen sowie alle wiederkehrenden administrativen Tätigkeiten sind im Betriebshandbuch zu dokumentieren.
* Bei einem Neustart einer Firewall ist sicherzustellen, dass der aktuellste Regelsatz und keine Standardeinstellungen wiederhergestellt werden.

Sofern die Firewalls durch Dienstleister betreut werden, sind im Rahmen der Notfallplanung Wartungsverträge mit externen Dienstleistern abzuschließen.

## Physische Sicherheitszonen

IT-Systeme und -Komponenten sind gemäß den zentralen Vorgaben physisch abzusichern. Demnach sind IT-Systeme und -Anwendungen gemäß ihrem Schutzbedarf zusammenzufassen und in entsprechenden Sicherheitszonen aufzustellen. Die Räumlichkeiten und Sicherheitszonen sind mit zusätzlichen Sicherheitsmaßnahmen auszustatten um eine etwaige Beschädigung, Manipulationen oder Einsichtnahme von IT-Systemen und Anwendungen zu unterbinden. Übergänge zwischen zwei unterschiedlichen physischen Sicherheitszonen sind geeignet abzusichern.

## Anwendungen, Webanwendungen und Webservices

Bei der Beschaffung, Installation und Administration von allgemeinen Anwendungen, Webanwendungen sowie Webservices sind die zentralen Vorgaben der <Institution> sowie die Anforderungen der Sicherheitsrichtlinie „Webanwendungen“ und „Standardsoftware“ umzusetzen.

Bei der Beschaffung von IT-Anwendungen sind die Vorgaben an den Test und die Freigabe der jeweiligen Anwendungen zu beachten. Insbesondere bei Eigenentwicklungen sind zusätzlich die Vorgaben für sichere Entwicklung und Projektmanagement umzusetzen.

Im Rahmen vom Patch- und Änderungsmanagement sind betriebliche und sicherheitsrelevante Daten durch eine Datensicherung abzusichern. Die Wiederherstellbarkeit regulärer Datensicherungen ist regelmäßig zu testen.

Jegliche IT-Anwendungen sind hinsichtlich ihrer Kritikalität und ihres Schutzbedarfs zu bewerten. Auf Basis dieser Bewertung sind angemessene Schutz- und Härtungsmaßnahmen abzuleiten.

Die Nutzung von IT-Anwendungen durch Benutzer oder Administratoren hat erst nach einer entsprechenden Einweisung und Schulung zu erfolgen.

Die Aussonderung von IT-Anwendungen ist so zu gestalten, dass Datenverluste oder Beeinträchtigungen der Integrität ausgeschlossen sind. Die Anwendungen sind sicher zu löschen und Lizenzen frei- bzw. zurückzugeben. Für die Verwaltung von Softwarelizenzen ist ein zentrales Lizenzmanagement zu etablieren.

## Datenbanken

Datenbanken sowie relationale Datenbanksysteme sind gemäß den Vorgaben der Sicherheitsrichtlinie „Datenbanksysteme“ aufzusetzen, zu betreiben und zu administrieren. Zusätzlich sind die zentralen Vorgaben zur Konfiguration, Installation sowie Patch- und Änderungssteuerung von IT-Systemen umzusetzen.

Die fachliche und administrative Administration von Datenbanken ist gemäß den zentralen Vorgaben der Sicherheitsrichtlinie „Identitäts- und Berechtigungsmanagements“ umzusetzen. Administrationsrechte innerhalb von Datenbanken sind ausschließlich technischen Nutzern einzuräumen. Der Zugriff auf Datenbanken durch interaktive Abfragesprachen unterliegt ausschließlich Administratoren. Der Zugriff auf Datenbanken hat ausschließlich über die jeweils verknüpfte Anwendung zu erfolgen. Etwaige Zugriffskontrollen sind dabei auf Datenbankebene zu installieren.

Für die Datensicherung und -Wiederherstellung von Datenbanken sind entsprechende Konzepte aufzusetzen und die jeweiligen Dienstprogramme der zugrundeliegenden Datenbank zu verwenden.

Im Rahmen einer Kapazitätsplanung ist der gegenwärtige und zukünftige Bedarf an anfallenden Datenvolumen zu überwachen.

Bei der Notfallplanung von Datenbanken sind die jeweiligen Notfallhandbücher umzusetzen. Zusätzlich sind für die jeweiligen Datenbankmanagementsysteme entsprechende Notfallpläne umzusetzen.

## Fileserver

Fileserver sind gemäß den zentralen Vorgaben zur Installation, Betrieb und Administration von IT-Systemen sowie der Sicherheitsrichtlinie „Fileserver“ zu betreiben.

Für die Inbetriebnahme, Installation und Konfiguration von File-Servern sind zusätzlich die zentralen Vorgaben zur Installation und Konfiguration von IT-Systemen einzuhalten. Neben den jeweiligen Betriebshandbüchern sind zusätzlich die Sicherheitsrichtlinien zum „Patch- und Änderungsmanagement“, „Datensicherung“ sowie „Protokollierung“ zu berücksichtigen.

Ferner sind die zentralen Vorgaben zur Härtung und Absicherung von Server-Systemen umzusetzen.

## Sensibilisierung und Schulung

Benutzer und Administratoren der <Institution> sind gemäß ihrer betrieblichen Funktion angemessen in die Informationssicherheit und Funktionalität von IT-Systemen und -Anwendungen einzuweisen. Dabei sind die Vorgaben des Standards „Sensibilisierung und Schulung“ umzusetzen. Die <Institution> hat sicherzustellen, dass eine operative Nutzung des IT-Systems oder der Anwendung erst nach erfolgreicher Einweisung erfolgt.

Zusätzlich sind regelmäßige Sensibilisierungsmaßnahmen zur Informationssicherheit durch den <Informationssicherheitsbeauftragter> abzustimmen und durchzuführen. Die Inhalte der Maßnahmen haben sich anhand der aktuellen Bedrohungslage sowie eingängigen Quellen zu orientieren.

## Audits und Revision

Geschäftsprozesse, IT-Systeme und -Anwendung sind regelmäßig auf die Umsetzung interner und externen Vorgaben an die Informationssicherheit zu überprüfen. Die Durchführung, Verantwortlichkeiten sowie Zyklen der Überprüfungen sind dabei anhand der Sicherheitsrichtlinie „Audits-Revisionen“ umzusetzen.

Bei der Auditierung der Informationssicherheit ist dabei sicherzustellen, dass die Überprüfung durch angemessen qualifiziertes und unabhängiges Personal oder einen externen Dienstleister erfolgt.

Die Ergebnisse der Überprüfung sind dem <Informationssicherheitsbeauftragter> vorzulegen und als vertrauliche Dokumente vor unberechtigter Einsichtnahme oder Manipulation zu schützen.

## Löschen und Vernichten von Informationen

Bei der Löschung und Vernichtung von Informationen und Datenträgern sind die Sicherheitsrichtlinien „Speicherlösungen“ sowie „Löschen und Vernichten von Informationen“ umzusetzen. Darüber hinaus sind die folgenden Vorgaben zu berücksichtigen:

* Interne, externe sowie regulatorische Anforderungen zur Aufbewahrung bzw. Wiederherstellung von Geschäftsinformationen sind bei der Löschung von Speichern und Datenträgern zu berücksichtigen. Relevante Geschäftsdaten sind entsprechend ihrer Aufbewahrungsdauer zu speichern und archivieren.
* Zur Entsorgung und Vernichtung von Datenträgern ist ein Dienstleistungsverhältnis zu einem zertifizierten Entsorgungsunternehmen zu etablieren.
* Das Entsorgungsunternehmen ist einer jährlichen Zertifizierung zu unterziehen.
* Datenträger sind vor ihrer Entsorgung und Vernichtung zentral zu sammeln und vor unberechtigter Einsichtnahme zu schützen.

## Außerbetriebnahme und Aussonderung von IT-Systemen

Bei der Außerbetriebnahme von IT-Systemen sind die Anforderungen der Sicherheitsrichtlinie „Löschen und Vernichten von Informationen“ zu berücksichtigen. Darüber hinaus sind die folgenden Anforderungen umzusetzen:

* Interne, externe sowie regulatorische Anforderungen zur Aufbewahrung bzw. Wiederherstellung von Geschäftsinformationen sind bei der Außerbetriebnahme von IT-Systemen zu berücksichtigen. Relevante Geschäftsdaten sind entsprechend zu sichern und zu archivieren.
* Lokale Daten, Programme sowie lizenzpflichtige Programme sind zu entfernen.
* Datenträger, auf denen sich vertrauliche oder schützenswerte Informationen befinden, sind sicher zu entfernen, zu löschen, zu vernichten oder frei- bzw. zurückzugeben.
* Etwaige Beschriftungen oder Aufkleber sind zu entfernen.

Bei der Aussonderung von IT-Systemen und Anwendungen sind die zentralen Anforderungen an die Außerbetriebnahme von IT-Systemen und Anwendungen umzusetzen. Bei der Aussonderung von IT-Systemen und Anwendungen sind zusätzlich die folgenden Vorgaben zu berücksichtigen:

* IT-Systeme sind nach der Bereinigung gemäß ihres Schutzbedarfs zu entsorgen.
* Zur Entsorgung von IT-Systemen im Rahmen einer Aussonderung ist ein Dienstleistungsverhältnis zu einem zertifizierten Entsorgungsunternehmen zu etablieren.
* Das Entsorgungsunternehmen ist einer jährlichen Zertifizierung zu unterziehen.
* IT-Systeme sind vor ihrer Entsorgung und Vernichtung zentral zu sammeln und vor unberechtigter Einsichtnahme zu schützen.

## Notfallmanagement

Die IT-Systeme und -Anwendungen sind gemäß den Anforderungen der Sicherheitsrichtlinie „Notfallmanagement“ angemessen in die Notfallplanung einzubinden.

Die <Institution> stellt sicher, dass im Rahmen eines Notfallkonzepts die Notfallpläne und -maßnahmen für die nachfolgenden Szenarien entwickelt und implementiert werden, die die angemessene Notfallhandhabung und zeitnahe Wiederaufnahme von kritischen Geschäftsprozesse gewährleisten:

* Teilausfall eines Rechenzentrums,
* Ausfall der Infrastruktur durch langanhaltenden DOS/DDOS,
* Ausfall eines Outsourcing-Dienstleisters,
* Ausfall eines Public-Cloud-Dienstleisters,
* Ausfall der Identity und Access Management (IAM) Infrastruktur,
* Ausfall der selbstbetriebenen privaten Cloud-Infrastruktur,
* Verschlüsselung von geschäftskritischen Informationen durch Malware sowie
* Ausfall der Administrationsinfrastruktur.

Zur Sicherung von administrativen Zugriffsmöglichkeiten während Notfällen sind zusätzlich die folgenden Anforderungen umzusetzen:

* Passwörter bzw. Keys für lokale bzw. Notfall-Administrator-Accounts sind in geeigneter Form vorzuhalten und vor unberechtigter Einsichtnahme sicher aufzubewahren.
* Notfallpasswörter sind nach ihrer Nutzung auszutauschen.