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

Konzept "Klassifizierung und Handhabung von Informationen"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | CON400002 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Konzept "Klassifizierung und Handhabung von Informationen" | [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](#_Toc84748711)

[Dokumentenhistorie 3](#_Toc84748712)

[Inhaltsverzeichnis 4](#_Toc84748713)

[Allgemeine Festlegungen 5](#_Toc84748714)

[Ziel / Zweck 5](#_Toc84748715)

[Geltungsbereich 5](#_Toc84748716)

[Zuständigkeiten 5](#_Toc84748717)

[Genehmigungs- und Änderungsverfahren 6](#_Toc84748718)

[Klassifizierung und Handhabung von Informationen 7](#_Toc84748719)

[Verantwortlichkeiten und Rollen 7](#_Toc84748720)

[Informationsverantwortlicher 7](#_Toc84748721)

[Verfasser 7](#_Toc84748722)

[Nutzer 7](#_Toc84748723)

[Kernnutzer 7](#_Toc84748724)

[Technischer Sachbearbeiter 7](#_Toc84748725)

[Prüfer und Ermittler 8](#_Toc84748726)

[Klassifizierung von Informationen – Vertraulichkeitsklassen 8](#_Toc84748727)

[Grundlagen 8](#_Toc84748728)

[Schadensgrößen 8](#_Toc84748729)

[Vertraulichkeitsklassen 9](#_Toc84748730)

[Änderung der Klassifizierung von Informationen 10](#_Toc84748731)

[Angebote, Verträge 10](#_Toc84748732)

[Informationen von Dritten 10](#_Toc84748733)

[Kennzeichnung von Informationen 11](#_Toc84748734)

[Explizite Kennzeichnung 11](#_Toc84748735)

[Implizite Kennzeichnung 11](#_Toc84748736)

[Dokumente im Entwurfsstadium 11](#_Toc84748737)

[Ausdrückliche Verpflichtungserklärungen 12](#_Toc84748738)

[Regeln zum Umgang mit Informationen 12](#_Toc84748739)

[Anhang 13](#_Toc84748740)

# Allgemeine Festlegungen

## Ziel / Zweck

Die <Institution> ist sich der Bedeutung des Schutzes von Informationen bewusst, da deren Missbrauch zu großen materiellen und immateriellen Schäden führen kann. Die Klassifizierung und angemessene Handhabung von Informationen ist daher ein wichtiger Baustein zur Vermeidung von Informations- und Datenschutzvorfällen.

Grundsätzlich können Informationen in unterschiedlicher Form vorliegen z.B. in elektronischer Form als Datei, in elektronischer Form in Webanwendungen und deren Datenbänken, in physischer Form als Ausdruck oder auch als gesprochenes Wort. Entscheidend für die Einstufung der Vertraulichkeit von Informationen ist deren Inhalt. Der Grad der Vertraulichkeit spiegelt das Maß der Auswirkungen auf die <Institution> wider, falls Informationen missbräuchlich benutzt werden. Ebenfalls bestimmt der Grad der Vertraulichkeit, wie mit Informationen umzugehen ist. Bei der Einstufung der Information wird darauf geachtet, dass diese unabhängig vom Trägermedium ist

Unter Berücksichtigung des „Need-To-know-Prinzip“ sollten grundsätzlich nur diejenigen Zugriff zu geschäftskritischen Informationen erhalten, die diese zur Erfüllung ihrer Aufgaben benötigen.

## 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

Dieses Dokument 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>.

# Klassifizierung und Handhabung von Informationen

## Verantwortlichkeiten und Rollen

### Informationsverantwortlicher

Der Informationsverantwortliche ist verantwortlich für die Klassifizierung von Informationen in seinem Verantwortungsbereich. Typischerweise gehört er der Bereichs-, Abteilungs- oder Projektleitung an oder hat übergreifende Aufgaben (z.B. Informationssicherheit, Arbeitsschutz, Datenschutz). Der Informationsverantwortliche legt den Kreis der Nutzer (interne und ggf. externe Personen) namentlich oder über Rollen sowie deren Berechtigungen fest. Die Verantwortlichkeit zur Klassifizierung von Informationen kann durch den Informationsverantwortlichen auch an andere Mitarbeitende delegiert werden.

Für bestimmte Gruppen von Informationsnutzern, bestimmte Arten des Informationsaustauschs oder für Einzelfälle kann von dem Informationsverantwortlichen aus sachlichen Gründen abgewichen werden. Jede Abweichung muss bekannt gegeben und dokumentiert werden.

### Verfasser

Der Verfasser arbeitet im Auftrag des Informationsverantwortlichen und übernimmt die Einstufung der Information von diesem. Bezüglich der Weitergabe besitzt er keine Sonderrechte.

### Nutzer

Nutzer einer Information sind alle Personen, die berechtigt sind, diese Information zu erhalten. Der Nutzer handelt gemäß den Regeln dieser Richtlinie, sofern der Informationsverantwortliche nicht Abweichendes vorgegeben hat.

### Kernnutzer

Der Informationsverantwortliche legt die Kernnutzer fest. In der Regel wird der Kernnutzerbereich abteilungsübergreifend alle Mitarbeiter umfassen, die innerhalb eines Prozesses bestimmte Informationen regelmäßig bearbeiten. Kernnutzern einer Information ist der Umgang mit diesen Informationen vertraut; sie sind vom Informationsverantwortlichen dafür entsprechend geschult und sensibilisiert.

Beispiele für Kernnutzer einer Information sind die Mitarbeitenden der Personalabteilung bezüglich der Personalakten oder abteilungsübergreifende Projektteams und deren Projektdaten.

Das Kernnutzerkonzept reduziert den Kennzeichnungsaufwand (siehe Kapitel Implizite Kennzeichnung).

### Technischer Sachbearbeiter

Technische Sachbearbeiter (z. B. Administratoren, Archivare) haben aufgrund ihrer besonderen Rolle Umgang mit klassifizierten Informationen. Sie sind nicht berechtigt, diese Informationen außerhalb ihrer funktionsbezogenen Aufgabe (z. B. Monitoring, Auswertung für Verrechnungszwecke) zu verwenden.

### Prüfer und Ermittler

Dieser Personenkreis hat expliziten Zugriff auf Informationen zum Zwecke der Ermittlung oder Prüfung. Zum Personenkreis zählen öffentliche Regierungsstellen wie Polizei, Staatsanwaltschaft oder Steuer- und Wirtschaftsprüfer.

## Klassifizierung von Informationen – Vertraulichkeitsklassen

### Grundlagen

Die in der <Institution> vorhandenen Informationen werden nach ihrer Vertraulichkeit klassifiziert. Die Vertraulichkeit ist abhängig von ihrer Bedeutung für die Geschäftsprozesse oder dem potentiellen Schaden bei falschem Umgang mit den Informationen.

Informationen werden in folgende Klassen eingestuft:

* Offen
* Intern
* Vertraulich
* Streng vertraulich

### Schadensgrößen

Für die korrekte Einstufung von Informationen in die jeweiligen Vertraulichkeitsklassen ist das Wissen um den potentiellen Schaden bei unerwünschter Offenlegung oder Weitergabe an Dritte von Bedeutung.

| Schadensgröße | Schaden für die <Institution> | Vertraulichkeitskasse | Beispiel |
| --- | --- | --- | --- |
| Hoch bis existenz- gefährdend | * Betroffen ist die gesamte <Institution> * Sehr schwerer Schaden für die Geschäftszwecke und Ziele der <Institution> * Gravierende rechtliche Konsequenzen bis hin zu Haftstrafen * Erheblicher Verlust von Ansehen und Vertrauen bei Kunden oder Lieferanten | Streng vertraulich | * Strategieunterlagen * Daten von gravierenden Störfällen * Ergebnisse Technik-Benchmark * Passwörter * Brief an Lieferanten mit Daten zu Neuproduktentwicklung |
| Mittel | * Betroffen ist ein Bereich der <Institution> * Erheblicher finanzieller Schaden * Rechtliche Konsequenzen bis hin zu Ordnungswidrigkeiten und Geldstrafen * Verärgerung und Imageverlust bei einzelnen Kunden oder Lieferanten * Personenbezogene Daten gem. Bundesdatenschutzgesetz | Vertraulich | * Informationen, die im Rahmen von Vertraulichkeitsvereinbarungen erlangt wurden * Daten des CRM- Systems * Kalkulationen * Unterlagen von Bewerbern * Arbeitsverträge * Mitarbeiterbeurteilung * Monatsbericht der <Institution> |
| Gering | * Keine weit reichenden Konsequenzen | Intern | * Organigramme * Adressänderungen eines Mitarbeitenden |
| Kein | * Kein Schaden, da die Informationen für die Öffentlichkeit bestimmt sind | Offen | * Freigegebene Informationen * Informationen auf der Webseite (ohne zusätzliches Login) |

### Vertraulichkeitsklassen

Im Folgenden werden die vier Vertraulichkeitsklassen und die grundlegenden Regeln bezüglich Kennzeichnung, Weitergabe und Absicherung sowie das Schadenspotential bei unsachgemäßem Umgang dargestellt.

#### Offen

Diese Informationen bedürfen keiner Kennzeichnung. Ein Schaden für die <Institution> kann in keinem Fall entstehen. Für die Handhabung offener Informationen existieren keine Einschränkungen.

Über die Veröffentlichung eines Dokumentes entscheidet der jeweilige Informationsverantwortliche.

#### Intern

Für diese Informationen genügt die implizite Kennzeichnung (siehe Kapitel „Kennzeichnung von Informationen“).

Interne Informationen können ohne Einschränkungen an Mitarbeitende der <Institution> oder an Dienstleister übermittelt werden, sofern diese dienstlich benötigt.

#### Vertraulich

Für diese Informationen genügt die implizite Kennzeichnung (siehe Kapitel „Kennzeichnung von Informationen“), sofern die Informationen den Kreis der Kernnutzer nicht verlassen.

Vertrauliche Informationen können bestimmten, d.h. von dem Informationsverantwortlichen benannten Nutzern (namentlich oder Rollen) übermittelt werden, sofern dienstlich benötigt.

Werden die Informationen anderen als Kernnutzern übermittelt, so sind sie vorher explizit als „vertraulich“ zu kennzeichnen.

#### Streng vertraulich

Diese Informationen bedürfen stets einer expliziten Kennzeichnung (siehe Kapitel „Kennzeichnung von Informationen“).

Sie dürfen nur an bestimmte von dem Informationsverantwortlichen namentlich benannte Nutzer übermittelt und von jedem Empfänger nur mit ausdrücklicher Einwilligung des Informationsverantwortlichen an andere Nutzer weitergeleitet werden.

Unabhängig davon ist der Kreis der Nutzer möglichst klein zu halten.

Unberührt von diesem Konzept bleiben die Sonderfälle der Geheimhaltungsbedürftigkeit gemäß § 79 BetrVG, § 96 SGB IX (Bekanntgabe von Betriebs- und Geschäftsgeheimnissen gegenüber Personal-, Jugend-, Auszubildenden- und Schwerbehindertenvertretung).

### Änderung der Klassifizierung von Informationen

Eine Information kann verschiedene Stufen an Vertraulichkeit durchlaufen. So können für eine Veröffentlichung vorgesehene Informationen noch als vertraulich einzustufen und zu behandeln sein, solange sie nicht veröffentlicht sind.

Eine Änderung der Klassifizierung kann nur durch den Informationsverantwortlichen erfolgen.

### Angebote, Verträge

Angebote und Verträge zu Geschäften über allgemein angebotene Leistungen zu allgemein bekannten Gegenleistungen ohne besondere Nebenabreden werden in die Vertraulichkeitsstufe „Intern“ eingestuft. Andere Angebote und Verträge sind je nach Inhalt als „Vertraulich“ oder „Streng vertraulich“ einzustufen.

Weitergehende Anforderungen (z. B. des Vergaberechts) bleiben unberührt.

### Informationen von Dritten

Die <Institution> wahrt die Vertraulichkeit von Kunden- und Lieferanteninformationen und trifft dafür entsprechende Vorkehrungen. Die gesetzlichen und vertraglichen Bestimmungen werden beachtet.

Grundsätzlich gelten für Informationen, die der <Institution> überlassen und mit einer Vertraulichkeitsklasse gekennzeichnet wurden, die gleichen Regelungen wie für interne Informationen der <Institution>.

## Kennzeichnung von Informationen

### Explizite Kennzeichnung

Sind Informationen explizit als „**Vertraulich**“ oder „**Streng vertraulich**“ zu kennzeichnen, so ist der Träger der Information deutlich erkennbar mit der Kennzeichnung „V**ertraulich**“ bzw. „**Streng vertraulich**“ zu versehen.

Mehrseitige Dokumente in Papier- oder Dateiform sind auf jeder Seite in der Mitte der Kopf- oder Fußzeile in Fettdruck entsprechend zu kennzeichnen; die Gesamtseitenzahl muss erkennbar sein.

Bei „**vertraulichen**“ Informationen ist der Empfängerkreis auf dem Informationsträger zu benennen, z.B. „Abteilung XY“.

Bei „**streng vertraulichen**“ Informationen ist der Empfängerkreis **Namentlich** (Verteilerliste) auf dem Informationsträger zu bezeichnen.

„**Vertrauliche**“ Informationen in Papierform sind bei internem Versand in der Hauspostmappe mit Klebestreifen zu verschließen und darauf ein Handzeichen des Absenders anzubringen, bei externem Versand im verschlossenen Kuvert ist der Empfänger mit dem Zusatz „**persönlich**“ zu benennen. Wenn bei „**vertraulichen**“ Informationen das Risiko der Öffnung durch nicht befugte Dritte be- steht und bei „**streng vertraulichen**“ Informationen generell sind Kuvertierungen doppelt auszuführen (Ausnahmen davon legt der Informationsverantwortliche fest); die innere ist mit der Kennzeichnung der Vertraulichkeitsklasse zu versehen, die äußere darf keinen Hinweis auf die Vertraulichkeit enthalten.

Die explizite Kennzeichnung hat immer Vorrang vor der impliziten.

### Implizite Kennzeichnung

Die implizite Kennzeichnung stellt innerhalb eines Kernnutzerbereiches (siehe 3.4) eine Erleichterung für die tägliche Arbeit dar. Die Informationen oder Informationsträger sind nicht selbst gekennzeichnet; der Nutzer kennt die Klassifizierung anhand der Art der Information und wurde vom Informationsverantwortlichen entsprechend geschult und sensibilisiert.

Die implizite Kennzeichnung ist maximal für vertrauliche Informationen möglich, solange diese den Kernnutzerbereich nicht verlassen. Wenn vertrauliche Informationen den Kernnutzerbereich verlassen sowie bei streng vertraulichen Informationen ist generell eine explizite Kennzeichnung mit der Vertraulichkeitsklasse erforderlich.

Bei neu erstellten Dokumenten sind die aktuellen Vorlagen für Microsoft Office-Dateien zu verwenden, sobald diese durch OI bereitgestellt werden. Wenn die Vorlage die Angabe einer Vertraulichkeitsklasse fordert, hat die Klassifizierung entsprechend zu erfolgen.

### Dokumente im Entwurfsstadium

Dokumente, die sich noch im Entwurfsstadium befinden, sind als solche mit dem Hinweis „Entwurf“ zu kennzeichnen.

Dies entbindet aber nicht von der Einstufung des Dokuments in die jeweilige Vertraulichkeitsklasse.

## Ausdrückliche Verpflichtungserklärungen

Jeder externe Dienstleister und Lieferant muss sich zur Verschwiegenheit verpflichten, sofern er potentiell Zugriff auf Daten oder Informationen der <Institution> hat. Das kann bereits vor Abschluss eines Vertrags, z.B. im Rahmen von Verhandlungen, der Fall sein. Dann hat er zuvor eine Erklärung zur Verschwiegenheitspflicht (Non Disclosure Agreement (NDA)) zu unterschreiben. Daneben ist darauf zu achten, dass ein mit ihm später geschlossener Vertrag ebenfalls eine Verschwiegenheitspflicht enthält.

NDAs für Lieferanten oder Dienstleister erstellt die Einkaufsabteilung. Für alle sonstigen Empfängergruppen erstellt sie die Rechtsabteilung. Der jeweilige Auftraggeber ist verantwortlich dafür, mit dem zuständigen Informationsverantwortlichen den Schutzbedarf der Daten zu klassifizieren und danach die Abteilung zu informieren, die das NDA ausstellt.

## Regeln zum Umgang mit Informationen

Die Regeln zum Umgang mit Informationen werden in Anlage zusammengefasst.

## Anhang

| Wie wird gekennzeichnet? | Offen | Intern | Vertraulich | Streng Vertraulich |
| --- | --- | --- | --- | --- |
| Kennzeichnung von Informationen in Papierform | keine | Implizit (d.h. der Nutzer ist mit der Art der Information vertraut und erkennt daraus die Vertraulichkeits- klasse, ohne dass diese auf dem Informationsträger vermerkt ist) | Implizit innerhalb der Kernnutzer.  Explizit wenn die Information den Kreis der Kernnutzer verlässt:   * mit „Vertraulich“ auf jeder Seite in Kopf- oder Fußzeile und ggf. im Betreff * Verteilerkreis auf erster Seite * Seitenangabe mit „Seite x von y“. | Explizit:   * mit „Streng vertraulich“ auf jeder Seite in Kopfzeile oder Fußzeile und ggf. im Betreff * Verteilerkreis namentlich benannt auf erster Seite * Seitenangaben mit „Seite x von y“. |
| Kennzeichnung von elektronischen Informationen | Keine | Implizit | Implizit innerhalb der Kernnutzer.  Explizit mit "Vertraulich" wenn die Information den Kreis der Kernnutzer verlässt. | Explizit:   * mit "Streng vertraulich" |

| Was mache ich bei ...? | Offen | Intern | Vertraulich | Streng Vertraulich |
| --- | --- | --- | --- | --- |
| Vervielfältigung mittels Kopierer, Drucker | Keine Einschränkungen | Keine Einschränkungen | Beaufsichtigung des Vervielfältigungsvorgangs | Nur nach Freigabe durch den Informations- verantwortlichen, Beaufsichtigung des Vervielfältigungsvorgangs |
| Weitergabe | Keine Einschränkungen | An alle Mitarbeitenden der <Institution> bzw. beauftragte Dienstleister oder Kunden sofern dienstlich benötigt | Weitergabe an Kernnutzer oder an vom Informationsverantwortlichen definierte Nutzer (namentlich oder Rollen), sofern dienstlich benötigt. Bei externen Dienstleistern muss eine Vertraulichkeitsvereinbarung vorliegen. | Weitergabe nur an namentlich vom Informationsverantwortlichen definierte Nutzer. Vom Empfänger dürfen streng vertrauliche Informationen nur nach expliziter Freigabe des Informationsverantwortlichen weitergegeben werden. Bei externen Dienstleistern muss eine Vertraulichkeitsvereinbarung vorliegen. |
| Übermittlung auf d. Postweg (intern) | Keine Einschränkungen | Hauspost/Hauspostmappe | Hauspostmappe mit Klebestreifen verschließen und darauf Handzeichen anbringen; bei Risiko der Öffnung durch unbefugte Dritte Kuvertierung doppelt ausführen. | Kuvertierung doppelt ausführen; die innere ist mit der Kennzeichnung der Vertraulichkeitsklasse zu versehen, die äußere darf keinen Hinweis auf die Vertraulichkeit enthalten. |
| Übermittlung auf d. Postweg (extern) | Keine Einschränkungen | Normaler Brief | Verschlossener Umschlag, Empfänger mit Zusatz „persönlich“ benennen; bei Risiko der Öffnung durch unbefugte Dritte Kuvertierung doppelt ausführen. | Per Übergabe-Einschreiben, Kuriersendung; Empfänger mit Zusatz „persönlich“ benennen; Kuvertierung doppelt ausführen; die innere ist mit der Kennzeichnung der Vertraulichkeitsklasse zu versehen, die äußere darf keinen Hinweis auf die Vertraulichkeit enthalten. |
| Übermittlung per E-Main (intern) | Keine Einschränkungen | Keine Einschränkungen | Mit der Nachrichtenoption „Vertraulich“ zu versenden | Mit der Nachrichtenoption „Vertraulich“ zu versenden |
| Übermittlung per E-Main (extern) | Keine Einschränkungen  Anlagen der E-Mail üblicherweise als PDF | Keine Einschränkungen  Anlagen der E-Mail üblicherweise als PDF | Inhalt als Anlage mit 7Zip verschlüsselt (AES256), Anlagen üblicherweise als PDF-Dokument | Ordner (Inhaltsvorschau) und Inhalt als Anlage mit 7Zip verschlüsselt (AES256), Anlagen üblicherweise als PDF-Dokument |
| Übermittlung per Fax (intern) | Keine Einschränkungen | Keine Einschränkungen | Nur nach Vorankündigung | Nur nach Vorankündigung |
| Übermittlung per Fax (extern) | Keine Einschränkungen | Deckblatt mit Anzahl der Seiten | Nur nach Vorankündigung  Deckblatt mit Anzahl der Seiten | Verboten |
| Verbale Weitergabe | Keine Einschränkungen | Nur erlaubt, wenn keine Unberechtigten zuhören können. | Nur erlaubt, wenn keine Unberechtigten zuhören können. | Nur erlaubt, wenn keine Unberechtigten zuhören können.  Nachricht nicht auf Anrufbeantworter /Mailbox hinterlassen. Identität des Gesprächspartners sicherstellen. |
| Vernichtung von Informationen in Papierform | Keine Einschränkungen | Papierkörbe am Arbeitsplatz; nicht bei personenbezogenen Daten | Gesicherte Vernichtung z. B. im Datenschutz- Container | Sicher vernichten durch zugelassenen Shredder |

| Informationen in IT-Systemen | Offen | Intern | Vertraulich | Streng Vertraulich |
| --- | --- | --- | --- | --- |
| Speicherung in IT-Systeme / Anwendungen der <Institution> | Keine Einschränkungen | Speicherung unter Berücksichtigung der Zugriffsrechte, ggf. explizite Vergabe von Zugriffsrechten | Speicherung unter Berücksichtigung der Zugriffsrechte, ggf. explizite Vergabe von Zugriffsrechten | Speicherung unter Berücksichtigung der Zugriffsrechte, regelmäßig Prüfung der aktuellen Zugriffsrechte, ggf. explizite Vergabe von Zugriffsrechten |
| Mobile Geräte (Notebook, Smartphone, Tablet) | Keine Einschränkungen | Keine Einschränkungen | Verschlüsselung der internen Speicher erforderlich. | Verschlüsselung der internen Speicher erforderlich. |
| Mobile Datenträger | Keine Einschränkungen | Keine Einschränkungen | Verschlüsselung erforderlich | Verschlüsselung erforderlich |
| Bereitstellung im Internet (Blogs, Foren, Soziale Medien) | Keine Einschränkungen | verboten | verboten | Verboten |
| Löschen von Informationen | Löschen im Filesystem | Loschen im Filesystem | Sicheres Löschen | Sicheres Löschen |
| Entsorgung / Vernichtung von Hardware und mobilen Datenträgern | Keine Einschränkungen | Hardware: Abgabe beim IT-Support  Mobile Datenträger: physische Vernichtung | Hardware: Abgabe beim IT-Support  Mobile Datenträger: physische Vernichtung | Hardware: Abgabe beim IT-Support  Mobile Datenträger: physische Vernichtung |

| Physische Aufbewahrung und Ablage von Informationen | Offen | Intern | Vertraulich | Streng Vertraulich |
| --- | --- | --- | --- | --- |
| Allgemein | Keine Einschränkungen | Unbefugten Zugriff durch Dritte über einfache Mittel verhindern. Eine angemessene technische Umsetzung ist durch den Informationsverantwortlichen im Einzelfall in Abhängigkeit von den Gefährdungen zu gewährleisten. | Zugriff durch unbefugte Dritte verhindern. Eine angemessene technische Umsetzung ist durch den Informationsverantwortlichen im Einzelfall in Abhängigkeit von den Gefährdungen zu gewährleisten. | Zugriff durch unbefugte Dritte verhindern. Eine angemessene technische Umsetzung ist durch den Informationsverantwortlichen im Einzelfall in Abhängigkeit von den Gefährdungen zu gewährleisten. |
| In Gebäuden der <Institution> | Keine Einschränkungen | Absperren des Büros wo möglich. Bei physisch extra abgesicherten Bereichen sind Sonderregelungen möglich. | Absperren des Büros, wo möglich. Falls gewährleistet ist, dass niemand außer dem Schlüsselbesitzer das Büro betreten kann, ist diese Maßnahme ausreichend.  Sonst: Bei längerer Abwesenheit (> 30 Minuten) Wegsperren der Informationen. Bei physisch extra abgesicherten Bereichen sind Sonderregelungen möglich. | Absperren des Büros, wo möglich. Falls gewährleistet ist, dass niemand außer dem Schlüsselbesitzer das Büro betreten kann, ist diese Maßnahme ausreichend.  Sonst: Bei längerer Abwesenheit (> 30 Minuten) Wegsperren der Informationen. Bei physisch extra abgesicherten Bereichen sind Sonderregelungen möglich.  Bei physisch nicht gesondert abgesicherten Bereichen Wegsperren der Informationen bei einer Abwesenheit von mehr als 10 Minuten. |
| Unterwegs oder im Homeoffice | Keine Einschränkungen | Abgesperrter Raum | Vor Zugriff sicher aufbewahren (Verschlüsseln und z. B. Wegsperren in Hotelsafe) | Vor Zugriff sicher aufbewahren (Verschlüsseln und z. B. Wegsperren in Hotelsafe) |