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

Standard "Klassifizierung 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 | ISMS200006 | [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](#_Toc75327217)

[Dokumentenhistorie 3](#_Toc75327218)

[Inhaltsverzeichnis 4](#_Toc75327219)

[Allgemeine Festlegungen 5](#_Toc75327220)

[Ziel / Zweck 5](#_Toc75327221)

[Geltungsbereich 5](#_Toc75327222)

[Zuständigkeiten 5](#_Toc75327223)

[Genehmigungs- und Änderungsverfahren 6](#_Toc75327224)

[Standard Klassifizierung von Informationen 6](#_Toc75327225)

[Verantwortlichkeit 6](#_Toc75327226)

[Informationseigentümer 6](#_Toc75327227)

[Informationsnutzer 6](#_Toc75327228)

[Informationsklassifizierung und Kritikalitätsmatrix 7](#_Toc75327229)

[Klassifizierung des Sicherheitsziels „Verfügbarkeit" 8](#_Toc75327230)

[Klassifizierung des Sicherheitsziels „Integrität" 9](#_Toc75327231)

[Klassifizierung des Sicherheitsziels „Vertraulichkeit" 10](#_Toc75327232)

# Allgemeine Festlegungen

## Ziel / Zweck

Informationen und die sie verarbeitenden Anwendungen spielen für die <Institution> eine entscheidende sowie tragende Rolle im Informationssicherheitsmanagement und stellen einen bedeutsamen unternehmerischen Wert dar. Aus diesem Grund haben alle Mitarbeitende die Verantwortung angemessen mit den bestehenden Unternehmenswerten umzugehen.

Die vorliegenden Kriterien zur Klassifizierung von Informationen soll jeden Mitarbeitenden dabei unterstützen, den richtigen Umgang mit Informationen zu wählen. Dazu zählen zum Beispiel Informationssicherheitsdaten, Partnerdaten, Personaldaten und personenbezogene Daten.

Der Standard beschreibt die im Zusammenhang stehenden Verantwortlichkeiten, Rechte und Pflichten jedes Einzelnen und definiert konkrete Vorgaben zum geeigneten Umgang mit den Ressourcen.

## 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 Klassifizierung von Informationen 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 Klassifizierung von Informationen

## Verantwortlichkeit

Um den geeigneten Umgang mit den Informationswerten zu gewährleisten, werden im Folgenden die Verantwortlichkeiten im Rahmen der Informationsklassifizierung beschrieben. Darauf aufbauend werden bestehende Sicherheitsklassen erläutert sowie geeignete und verpflichtend anzuwendende Sicherheitsmaßnahmen im Rahmen der Klassifizierung von Informationen definiert.

## Informationseigentümer

Für alle Informationen gibt es einen Verantwortlichen, der als Informationseigentümer bezeichnet wird. Dieser ist zuständig für

* Festlegungen der geschäftlichen Relevanz und Bedeutung seiner Informationen für die <Institution>,
* Festlegungen zur Ablage von Dokumenten gemäß Informationsklassifizierung und Sicherheitsziel unter Berücksichtigung der Zugriffsrechte Dritter auf Dokumente, Anwendungen oder IT-Systeme,
* die Berücksichtigung von Aufbewahrungsvorschriften und Löschfristen,
* die Einhaltung der rechtlichen und regulatorischen Anforderungen.

Bei elektronischen und papiergebundenen Informationsträgern, die keinen direkten technischen Bezug aufweisen (Anwendungen, IT-Systeme) oder aus Softwareprodukten heraus exportiert werden, übernimmt grundsätzlich der ausführende Informationseigentümer die Verantwortung. Bei Dokumenten ist dies stets der Ersteller des betroffenen Dokuments. Die Informationseigentumsverhältnisse können sich durch Nutzung, Verarbeitung und Weitergabe verändern.

### Informationsnutzer

Der Informationsnutzer ist verpflichtet ordnungsgemäß, sicherheitsbewusst und zweckgebunden mit den ihm anvertrauten Informationen umzugehen. Bei der IT-gestützten Informationsverarbeitung sind die Vorgaben zum Umgang mit der Informations- und Kommunikationstechnik und der Bedienung der IT-Systeme und Anwendungen zu beachten.

Beim Umgang mit elektronischen oder physischen Informationsträgern sind die Informationsklassifizierung und die sich hieraus ergebenden Anforderungen zu beachten. Wird ein Dokument durch einen Benutzer selbst erstellt, nimmt dieser zugleich die Rolle des Informationseigentümers ein (siehe Kapitel Informationseigentümer).

## Informationsklassifizierung und Kritikalitätsmatrix

Alle Daten (und damit auch die sie verarbeitenden Systeme) müssen gemäß den Sicherheitszielen Vertraulichkeit, Verfügbarkeit und Integrität durch den Informationseigentümer klassifiziert und dementsprechend gekennzeichnet sein, um jederzeit eine angemessene Verarbeitung der Informationen zu gewährleisten.

Die Informationsklassifizierungen erfolgen nach der im BSI-Standard 200-2 dargestellten Vorgehensweise und bezieht sich dementsprechend auf die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit. Der Schutzbedarf wird jeweils in den Stufen „normal“, „hoch“ und „sehr hoch“ zu geordnet.

|  |  |  |  |
| --- | --- | --- | --- |
|  | normal | hoch | sehr hoch |
| Verfügbarkeit | Ein Ausfall der Plattform bzw. des Verfahrens ab 14 Stunden und 21 Minuten (SLA 98,90% per Monat) führt zu Beeinträchtigungen der verarbeitenden Prozesse.  Die Verarbeitung der Daten lässt sich bis zu 14 Stunden und 21 Minuten verschieben oder ist während dieser Zeit lokal bei der datenverarbeitenden Organisationseinheit durchführbar.  m Jahr sind maximal 10 Ausfälle tolerierbar. | Ein Ausfall der Plattform bzw. des Verfahrens ab 7 Stunden (SLA 99,00% per Monat) führt zu Beeinträchtigungen der verarbeitenden Prozesse.  Bei der Datenverarbeitenden Organisationseinheit entstehen unaufhaltbare Arbeitsrückstände und/oder Datenverluste sind ohne größeren Aufwand rekonstruierbar.  Im Jahr sind maximal 5 Ausfälle tolerierbar. | Ein Ausfall der Plattform bzw. des Verfahrens ist nur bis maximal 4 Stunden tolerierbar (SLA 99,444% per Monat) und/oder Datenverluste sind nur mit sehr großem Aufwand rekonstruierbar.  Im Jahr sind 2 Ausfälle tolerierbar. |
| Integrität | Der Integritätsverlust verlangsamt interne Geschäftsprozesse. Daten können durch Abgleich mit integren Informationen innerhalb 14 Stunden und 20 Minuten wieder hergeleitet werden. Es ist keine negative Innen- und Außenwirkung für die <Institution> zu erwarten.  Der finanzielle Schaden beläuft sich auf bis zu 2% des Eigenkapitals. | Der Integritätsverlust verzögert interne Geschäftsprozesse. Eine negative Innen- und Außenwirkung kann für die <Institution> nicht ausgeschlossen werden.  Der finanzielle Schaden ist größer 2% und kleiner 5% des Eigenkapitals | Der Integritätsverlust verhindert interne Geschäftsprozesse. Der finanzielle Schaden ist größer als 5% des Eigenkapitals.  Eine sehr hohe Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist für die <Institution> denkbar.  Systematische fundamentale Verstöße gegen Vorschriften, Verträge und Gesetze sind möglich und es kann den Verlust der operativen Handlungsgrundlage des Kerngeschäfts zur Folge haben. |
| Vertraulichkeit | Der Verlust der Vertraulichkeit führt nur zu geringen Schäden. Insbesondere hat ein möglicher Missbrauch personenbezogener Daten nur geringfügige Auswirkungen auf die Betroffenen. | Der Verlust der Vertraulichkeit führt zu erheblichen Schäden. Insbesondere hat ein möglicher Missbrauch personenbezogener Daten erhebliche Auswirkungen auf die Betroffenen.  Durch den Verlust der Vertraulichkeit ist eine breite Ansehens- oder Vertrauensbeeinträchtigung für die <Institution> zu erwarten. Der Verlust der Vertraulichkeit kann zu erheblichen finanziellen Verlusten führen. | Der Verlust der Vertraulichkeit führt zu gravierenden, nicht tolerierbaren Schäden.  Ein möglicher Missbrauch personenbezogener Daten könnte den finanziellen oder gesellschaftlichen Ruin der Betroffenen bedeuten.  Es sind gravierende Beeinträchtigungen der persönlichen Unversehrtheit (Gefahr für Leib und Leben) möglich. Ein möglicher finanzieller Schaden ist für die <Institution> existenzbedrohend. |

## Klassifizierung des Sicherheitsziels „Verfügbarkeit"

|  |  |  |
| --- | --- | --- |
| Feststellung des Schutzbedarfs | ****Informationsklassifizierung zur Kennzeichnung**** | ****Erläuterung**** |
| normal | Zeitlich gering kritisch | Ein Ausfall der Plattform bzw. des Verfahrens ab 14 Stunden und 21 Minuten (SLA 98,90% per Monat) führt zu Beeinträchtigungen der verarbeitenden Prozesse bei der <Institution>. Der maximale Wert für den Parameter Recovery Time Objective (RTO) beträgt 9 Stunden und 20 Minuten und für Work Recovery Time (WRT) 5 Stunden.  Der maximale Zeitraum für den Wert Recovery Point Objective (RPO) beträgt 7 Stunden. Dies bedeutet, die Zeit zwischen zwei Datensicherungen darf maximal 7 Stunden betragen.  Die Verarbeitung der Daten seitens der <Institution> lässt sich bis zu 14 Stunden und 21 Minuten verschieben oder ist während dieser Zeit lokal durchführbar.  Im Jahr sind maximal 10 Ausfälle tolerierbar. |
| hoch | Zeitlich kritisch | Ein Ausfall der Plattform bzw. des Verfahrens ab 7 Stunden (SLA 99,00% per Monat) führt zu Beeinträchtigungen der verarbeitenden Prozesse bei der <Institution>. Der maximale Wert für den Parameter Recovery Time Objective (RTO) beträgt 3 Stunden und 59 Minuten und für Work Recovery Time (WRT) 3 Stunden.  Der maximale Zeitraum für den Wert Recovery Point Objective (RPO) beträgt 3 Stunden. Dies bedeutet, die Zeit zwischen zwei Datensicherungen darf maximal 3 Stunden betragen.  Die Verarbeitung der Daten seitens der <Institution> lässt sich bis zu 6 Stunden und 59 Minuten verschieben oder ist während dieser Zeit lokal durchführbar.  Im Jahr sind maximal 5 Ausfälle tolerierbar. |
| sehr hoch | Zeitlich hoch kritisch | Ein Ausfall der Plattform bzw. des Verfahrens ist lediglich bis maximal 7 Stunden tolerierbar (SLA 99,444% per Monat) und/oder Datenverluste sind nur mit sehr großem Aufwand rekonstruierbar. Der maximale Wert für den Parameter Recovery Time Objective (RTO) beträgt 1 Stunden und 59 Minuten und für Work Recovery Time (WRT) 2 Stunden.  Der maximale Zeitraum für den Wert Recovery Point Objective (RPO) beträgt 1 Stunde. Dies bedeutet, die Zeit zwischen zwei Datensicherungen darf maximal 1 Stunde betragen.  Die Verarbeitung der Daten seitens der <Institution> lässt sich bis zu 3 Stunden und 59 Minuten verschieben oder ist während dieser Zeit lokal durchführbar.  Im Jahr sind 2 Ausfälle tolerierbar. |

## Klassifizierung des Sicherheitsziels „Integrität"

|  |  |  |
| --- | --- | --- |
| Feststellung des Schutzbedarfs | ****Informationsklassifizierung zur Kennzeichnung**** | ****Erläuterung**** |
| normal | normal | Der Integritätsverlust verlangsamt interne Geschäftsprozesse. Daten können durch Abgleich mit integren Daten innerhalb 14 Stunden und 20 Minuten wieder hergeleitet werden. Mangelnde Korrektheit und Vollständigkeit der Daten beeinflusst die Aufgabenerfüllung nicht oder nur in sehr geringem Umfang und führt zu keinen oder nur geringen Schäden.  Mangelnde Korrektheit und Vollständigkeit der Daten führt zu einem Verstoß gegen Vorgaben, Verträge oder externe Regularien, die keinen oder nur geringen Schaden (z. B. durch Strafzahlungen) nach sich ziehen. Der finanzielle Schaden beläuft sich auf bis zu 2% des Eigenkapitals.  Mangelnde Korrektheit und Vollständigkeit der Daten hat keine Folgen für die Außenwirkung, sondern lediglich interne Auswirkungen. Insbesondere ergeben sich keine oder nur geringe Auswirkungen auf die Ertragslage. |
| hoch | hoch | Der Integritätsverlust verzögert Geschäftsprozesse. Eine negative Innen- und Außenwirkung kann für die <Institution> nicht ausgeschlossen werden. Mangelnde Korrektheit und Vollständigkeit der Daten beeinflusst im geringen bis mittleren Maß die Aufgabenerfüllung und führt zu mittleren Schäden. Der finanzielle Schaden ist größer 2% und kleiner 5% des Eigenkapitals.  Mangelnde Korrektheit und Vollständigkeit der Daten hat nur geringe und nur kurz-/mittelfristige Außenwirkung national. Es ergeben sich mittlere Auswirkungen auf die Ertragslage. Es ist mit dem Verlust einzelner Kunden zu rechnen. |
| sehr hoch | Sehr hoch | Der Integritätsverlust verhindert interne Geschäftsprozesse. Mangelnde Korrektheit und Vollständigkeit der Daten beeinflusst die Aufgabenerfüllung bis hin zur Aufgabenverhinderung und führt zu erheblichen bis existentielle Schäden. Der finanzielle Schaden ist größer als 5% des Eigenkapitals.  Eine sehr hohe Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist für die <Institution> denkbar.  Systematische fundamentale Verstöße gegen Vorschriften, Verträge und Gesetze sind möglich und es können den Verlust der operativen Handlungsgrundlage des Kerngeschäfts zur Folge haben.  Mangelnde Korrektheit und Vollständigkeit der Daten hat große u. langfristige Außenwirkungen. Es ist mittel-/langfristig ein signifikanter Einfluss spürbar. |

## Klassifizierung des Sicherheitsziels „Vertraulichkeit"

|  |  |  |
| --- | --- | --- |
| Feststellung des Schutzbedarfs | ****Informationsklassifizierung zur Kennzeichnung**** | ****Erläuterung**** |
| normal | intern | Diese Schutzbedarfsklasse beinhaltet interne Daten und Informationen der <Institution>, die nicht nach außen gelangen sollen und Informationen, deren Missbrauch geringe direkte oder indirekte Schäden hervorrufen können. In diese Klassifizierung fallen alle Informationen und Daten, sofern sie nicht in einer höheren Informationsklasse eingestuft sind.  Die Kenntnisnahme durch Unbefugte kann für die Interessen der <Institution> nachteilig sein. |
| hoch | vertraulich | Diese Schutzbedarfsklasse beinhaltet Daten und Informationen die nur einem eingeschränkten, definierten Personenkreis zugänglich sein dürfen und Informationen, deren Missbrauch einen hohen direkten oder indirekten Schaden für die <Institution> hervorrufen kann. Grundsätzlich sind personenbezogene Daten dieser Kategorie zuzuordnen.  Die Kenntnisnahme durch Unbefugte kann für die Interessen der <Institution> schädlich sein. |
| sehr hoch | Streng vertraulich | Diese Schutzbedarfsklasse beinhaltet Daten und Informationen die nur einem kleinen, dedizierten Kreis zugänglich sein dürfen und die Möglichkeit der Kenntnisnahme muss auf vorher festgelegte Personen beschränkt bleiben. Informationen, deren Missbrauch einen sehr hohen Schaden für die <Institution> hervorrufen kann.  Die Kenntnisnahme durch Unbefugte kann die Sicherheit der <Institution> gefährden oder ihren Interessen schweren Schaden zufügen. |