Computacenter

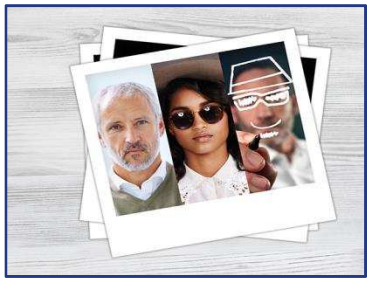
SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT – UMGANG MIT INFORMATIONEN

Klassifizierung von Informationen

iuii

KLASSIFIZIERUNG VON INFORMATIONEN

Einführung



‘Klassifizierung von Informationen’

Hier erfährst Du, was die Klassifizierung von Informationen bedeutet, welche Klassifizierungen bei Computacenter verwendet werden, und wie Du mit den Informationen aus den einzelnen Klassifizierungen umgehen, sie speichern und entsorgen solltest.

1. Je nachdem, wie sensibel die Informationen sind, müssen sie unterschiedlich stark geschützt werden.
2.
3. Um unsere Informationen effektiv zu schützen, verwendet Computacenter die folgenden Informationsklassifizierungen:
4. 1. unbeschränkt
5. 2. intern
6. 3. vertraulich
7. 4. streng vertraulichunrestricted
8. internal
9. confidential
10. str

Verfasser sind dafür verantwortlich, die von ihnen erstellten Inhalte zu klassifizieren und zu kennzeichnen.

In Fällen, in denen die Klassifizierung unbekannt ist (z. B. wenn ein Dokument nicht entsprechend gekennzeichnet wurde), sollte derjenige, der mit den Informationen umgeht, die Matrix zur Klassifizierung und Handhabung von Informationen verwenden, um die Klassifizierung der Informationen zu ermitteln.

Sollte dies nicht möglich sein, müssen die Informationen als „Vertraulich“ gekennzeichnet werden, um zu verhindern, dass unbeabsichtigt sensible Informationen offengelegt werden.

Informationsklassifizierungen

Nicht jede Information muss gleich stark oder schwach geschützt werden. Stelle Dir bei der Einschätzung immer die Frage „Welchen Schaden hätte unser Unternehmen, wenn die Information in falsche Hände käme?“

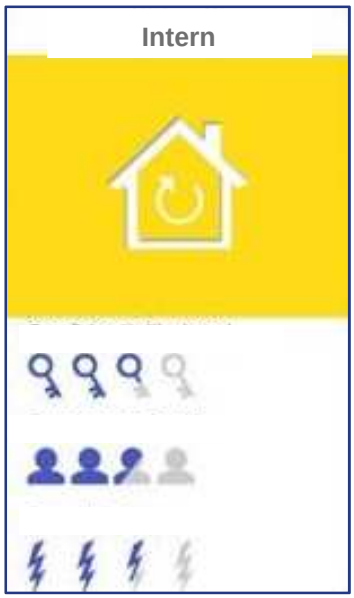
Je sensibler eine Information ist, umso stärker muss sie natürlich geschützt werden.

Unbeschränkt

‘Unbeschränkte’ Informationen beinhalten alle Informationen, die zum externen Gebrauch vorgesehen, nicht sensibel und für die Öffentlichkeit bestimmt sind, z. B. die Website von Computacenter, Produkt- und Servicebroschüren, Informationsbroschüren.

Für Umgang, Speicherung und Entsorgung dieser Art von Informationen gibt es keine Einschränkungen

Intern



Die Informationsklassifizierung „intern“ bezieht sich **auf Informationen, die allen Mitarbeitern frei zugänglich, aber nicht für die Öffentlichkeit bestimmt sind.**

Beispiele hierfür sind Computacenter-Richtlinien, Mitarbeiter-Newsletter oder Name, E-Mail-Adresse, Niederlassungsstandort, Position von Mitarbeitern.

Solche Informationen können bei Bedarf an Geschäftspartner weitergegeben werden, wenn klar ist, dass sie nicht an Dritte weitergegeben dürfen.

Interne Informationen können über alle möglichen Geschäftsanwendungen weitergegeben werden, z. B. über die Digital Me-Tools OneDrive, Jabber, SharePoint und Yammer, sie dürfen aber nicht über öffentliche Netzwerke wie Social Media-Websites oder -Foren verbreitet werden.

Es gibt für die Entsorgung dieser Art von Informationen keine Einschränkungen, außer wenn eine große Menge interner Informationen auf einmal entsorgt werden soll. Werden nämlich große Mengen interner Informationen offengelegt, können die Auswirkungen dazu führen, dass die Klassifizierung der Informationen insgesamt auf „Vertraulich“ heraufgestuft wird. Dieses Prinzip wird als Informationsaggregation bezeichnet und sollte beim Umgang mit allen Arten von Informationen stets berücksichtigt werden.

Vertrauliche Informationen

Information, die als „vertraulich“ eingestuft werden, dürfen bei Bedarf nur an bestimmte Mitarbeitergruppen weitergegeben werden. Hierzu gehören beispielsweise Verträge, Angebote und zugehörige Informationen, Client-IP-Adressen, unternehmensinterne Finanz-, Geschäfts-, Prüfungs- oder Vorfallsberichte.

Sie müssen unter Kontrolle von Computacenter bleiben und dürfen ohne die Zustimmung des Eigentümers weder intern noch extern weitergegeben werden. Sollten Kunden oder Partnern Einsicht benötigen und sich die Informationen auf sie beziehen, darf das betreffende Dokument ausschließlich an sie weitergegeben werden.

Vertrauliche Informationen können über alle Arten von Digital Me-Geschäftsanwendungen weitergegeben werden. Eine Ausnahme bildet hier Yammer und Jabber, bei denen die Informationsweitergabe nur per Bildschirmfreigabe zulässig ist. Im Fall von personenbezogenen Daten (PBD) ist die Weitergabe nur innerhalb der EU bzw. dem Europäischen Wirtschaftsraum (EWR) zulässig. Vertrauliche Informationen dürfen nicht über öffentliche Netzwerke wie Social Media-Websites oder -Foren verbreitet werden.

Papierbasierte Unterlagen, die vertrauliche Informationen enthalten, müssen bei Nichtgebrauch sicher in Aktenschränken verschlossen und entweder in einem geheimen Abfallbehälter entsorgt oder geschreddert warden.

Elektronische Medien müssen vor der Entsorgung mit einer zuverlässigen Methode gelöscht bzw. neuformatiert werden. Alle unternehmenseigenen Geräte können zu diesem Zweck zu ihrer Ausgabestelle zurückgebracht werden. Elektronische Informationen dürfen nur in Bereichen gespeichert werden, für die der Zugriff eingeschränkt und bedarfsabhängig ist.

Streng vertrauliche Informationen

Streng vertrauliche Informationen dürfen nur an Einzelpersonen und wenn dies zwingend erforderlich ist weitergegeben werden. Bei den Informationsempfängern handelt es sich in der Regel um Mitarbeiter von Computacenter, die namentlich benannt werden.

Zu streng vertraulichen Informationen gehören Informationen aus Finanz- und Kundendatenbanken, strategische Geschäftspapiere, Kennwörter und private Verschlüsselungsschlüssel, sensible personenbezogene Daten (PBD) über das Unternehmen, Kunden oder Dritte in Bezug auf: Ethnische Herkunft, politische Ansichten, religiöse oder philosophische Einstellungen, Mitgliedschaft in einer Gewerkschaft, Zahlungsdaten (Transaktionen) usw.

Bei Offenlegung dieser Art von Informationen ist mit erheblichem finanziellen, rechtlichen oder regulatorischen Schaden für Computacenter zu rechnen.

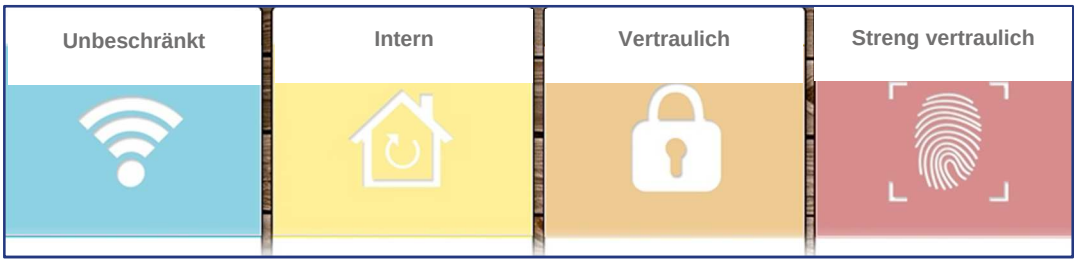
Streng vertrauliche Informationen dürfen nicht über unsere Digital Me-Geschäftsanwendungen weitergegeben werden, mit Ausnahme von OneDrive/OneNote, solange sie dort in einem hochgradig verschlüsselten Bereich gespeichert und ausschließlich für Deine eigenen Zwecke genutzt werden.

Wenn Du sie per E-Mail an einen Empfänger außerhalb von Computacenter sendest, musst der Inhalt in einem per Kennwort geschütztem Anhang übermittelt werden.

Papierbasierte Unterlagen müssen bei Nichtgebrauch sicher in Aktenschränken verschlossen und entweder in einem geheimen Abfallbehälter entsorgt oder geschreddert werden.

Elektronische Medien müssen vor der Entsorgung mit einer zuverlässigen Methode gelöscht bzw. neuformatiert werden. Alle unternehmenseigenen Geräte können zu diesem Zweck zu ihrer Ausgabestelle zurückgebracht werden. Elektronische Informationen dürfen nur in Bereichen gespeichert werden, für die der Zugriff eingeschränkt und strikt bedarfsabhängig ist.

Scenarios



Unbeschränkt	Intern	Vertraulich	Streng vertraulich
• Computacenter-Richtlinien • Pressemitteilung • Werbematerial	• Organigramme • Sensible personenbezogene Daten (PBD), z. B. Lohn- und Gehaltsdaten	• Technische Design Dokumente und Betriebshandbücher	• Kennwörter und private Verschlüsselungsschlüssel • Operative Berichte

Selbst wenn Informationen nicht speziell gekennzeichnet sind, musst Du als Mitarbeiter trotzdem in der Lage sein, sie der richtigen Informationsklasse zuzuordnen. Hierzu solltest du die Matrix zur Klassifizierung und Handhabung von Informationennutzen. Je höher der potenzielle Schaden wäre, desto höhere Sicherheitsmaßnahmen sind nötig. Für Werbung ist ein anderer Schutzbedarf erforderlich als für die Unterlagen, die unsere Marktstrategie betreffen.

Für Dokumente, die sich mit unserer Geschäftsstrategie befassen, ist eine andere Vertraulichkeitsstufe erforderlich als für Werbematerialien

Sei im Zweifelsfall besser zu vorsichtig als zu sorglos.

Zusammenfassung

In diesem Abschnitt hast Du gelernt...

- dass bei Computacenter vier unterschiedliche Kategorien zur Klassifizierung von Informationen eingesetzt werden.
- dass diese Kategorien die unterschiedlichen Vertraulichkeitsstufen repräsentieren, die für die verschiedenen Informationstypen gelten.
- dass Verfasser dafür verantwortlich sind, die von ihnen erstellten Inhalte zu klassifizieren und zu kennzeichnen.
- wie Du mit Informationen umgehst und sie über die Digital Me-Tools von Computacenter weitergibst.

<u>Datenschutzverletzungen und Informationssicherheitsvorfälle:</u>

Bei nicht vorschriftsmäßiger Handhabung und Entsorgung von Informationen besteht die Möglichkeit, dass es zu einer unbefugten Weitergabe oder Offenlegung gekommen ist. In diesem Fall muss ein Informationssicherheitsvorfall über das NGSD gemeldet werden.