



KNOW**NOW**
TOOLS FOR BUSINESS SUCCESS

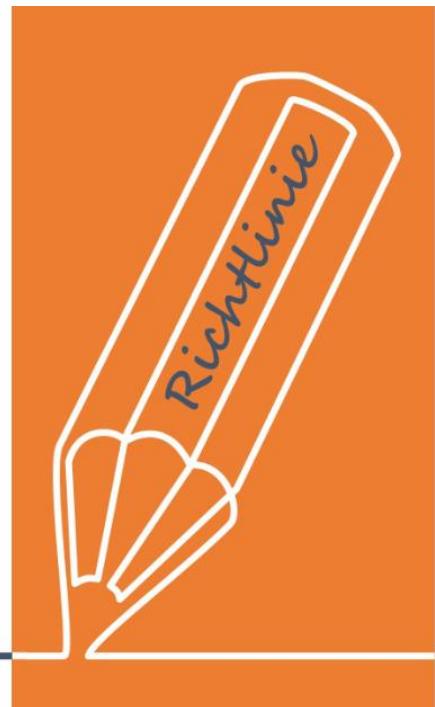
Richtlinie Informationsklassifizierung

UseNOW - TeachNOW - LearnNOW - FindNOW

- Sofort nutzbar: Auswählen - Anpassen - Anwenden
- In der Praxis erprobt und bewährt
- Im Tagesgeschäft sofort anwendbare Hilfsmittel
- Aktuell durch regelmäßige Updates

Richtlinie Informations- klassifizierung

des Unternehmens



Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

1.	Zweck und Zielsetzung	4
2.	Geltungsbereich	4
3.	Verantwortlichkeiten	4
4.	Definitionen	5
5.	Klassifizierungskriterien	5
6.	Klassifizierungsprozess	6
7.	Umgang mit klassifizierten Informationen	7
8.	Rechtliche Anforderungen und Compliance	8
9.	Überprüfung, Sensibilisierung und Verbesserung	8
10.	Dokumentenlenkung und Änderungshistorie	9

Sie möchten sich über dieses und weitere Tools
informieren?

... nutzen Sie unseren Tool-Online-Shop:
Registrieren und downloaden!

1. Zweck und Zielsetzung

Ihr Vorteil als Know-NOW User:

- **Freie Nutzung kostenloser Tools und Experten-Links**
- **Einrichtung und Nutzung eines Prepay-Kontos**
- **Einsparungen durch attraktive Bonusprogramme**

2. Geltungsbereich

Diese Richtlinie gilt für alle Beschäftigten, Dienstleister und alle anderen relevanten Parteien, die auf die auf sicherheitsrelevante Bereiche unserer IT-Systeme und geschützte Informationen des Unternehmens zugreifen.

3. Verantwortlichkeiten

- **Geschäftsführung:**
Sicherstellen, dass die Richtlinie unternehmensweit eingeführt und umgesetzt wird.
- **Informationssicherheitsbeauftragte(r):**
Überwachung der korrekten Umsetzung der Richtlinie und Einhaltung der Sicherheitsanforderungen. Erstellung, Wartung und regelmäßige Überprüfung der Richtlinie sowie Schulung und Sensibilisierung der Beschäftigten.

- **Führungskräfte / Prozessverantwortliche:**
Einstufung der von ihnen erstellten und genutzten Informationen. Klassifizieren von Informationen gemäß der Richtlinie und Kommunikation der Klassifizierung an andere Mitarbeiter oder Geschäftspartner.

Sie möchten sich über dieses und weitere Tools

informieren?

- **IT-Abteilung, IT-Dienstleister:**
Technische Umsetzung der Richtlinie (z.B. Implementierung von Zugriffsrechten, Verschlüsselung) bzw. Umgang mit klassifizierten Informationen gemäß der vertraglich vereinbarten Sicherheitsanforderungen. Bereitstellung von Tools zur Klassifizierung und Sicherstellung des Schutzes der IT-Systeme und Daten.

... nutzen Sie unseren Tool-Online-Shop:

- **Beschäftigte:**

Einhaltung der Richtlinie im täglichen Umgang mit Informationen. Richtiges Klassifizieren und Kennzeichnen von Informationen, sicherer Umgang und Meldung von Verstößen.

4. Definitionen

- **Information:**
Daten oder Wissen, das in einer bestimmten Form ausgetauscht, verarbeitet oder gespeichert wird.
- **Vertraulichkeit:**
Eigenschaft von Informationen, nur für autorisierte Personen zugänglich zu sein.
- **Klassifizierung:**
Prozess der Einstufung von Informationen nach ihrem Schutzbedarf oder ihrer Sensibilität.
- **Zugriff:**
Berechtigte Möglichkeit, Informationen einzusehen, zu verwenden oder zu bearbeiten.

Kostenlos und unverbindlich registrieren unter

5. Klassifizierungsstufen

www.know-now.de/join

Diese Richtlinie zur Informationsklassifizierung orientiert sich an den Klassifizierungsstufen, die durch den VDA (Verband der Automobilindustrie) im Whitepaper „Harmonisierung der Klassifizierungsstufen“ vorgeschlagen werden. In Kombination mit dem Traffic Light Protocol (TLP) entsteht eine klare Struktur für den Umgang mit sensiblen Informationen.

Tabelle mit den verschiedenen Klassifizierungsstufen und Beispielen zur Erläuterung:

Stufe	Beschreibung	Beispiele	Schutzklasse nach VDA ISA	TLP-Äquivalent
Öffentlich	Informationen, die ohne jegliche Einschränkungen veröffentlicht werden dürfen.	Prospekte, Kataloge, Pressemitteilungen, offizielle Webseiten.	keine	TLP: White
Intern	Informationen, die nur für Beschäftigte und engere Geschäftspartner zugänglich sein dürfen, aber keinen wesentlichen Schaden bei Offenlegung verursachen.	Verfahren, organisatorische Abläufe, Kontaktdaten von Beschäftigten, Schulungsprotokole, Anwesenheitslisten.	normal	TLP: Green
Vertraulich	Informationen, deren Offenlegung signifikante Schaden für das Unternehmen, seine Partner oder Beschäftigte verursachen könnte.	Entwicklungspläne, interne Projektdokumentation, Kundeninformationen, Gesundheitsdaten von Beschäftigten.	hoch	TLP: Amber
Extrem vertraulich	Informationen, deren Offenlegung gravierende Verluste für das Unternehmen, seine Kunden oder Partner haben könnte.	Technische Spezifikationen von Produkten, vertrauliche Verträge, strategische Geschäftspläne.	sehr hoch	TLP: Red

Sie möchten sich über dieses und weitere Tools informieren? ... nutzen Sie unseren Tool-Online-Shop: Registrieren und downloaden!

Erläuterungen zur Klassifizierung:

- **Öffentlich:** Keine Einschränkung in Hinblick auf Verbreitung. Es hat Zugriff, und es besteht keine Gefahr durch eine Veröffentlichung.

- **Intern:** Interne Informationen, die innerhalb des Unternehmens bleiben sollten, aber über interne Kanäle weitergeleitet werden können.

- **Vertraulich:** Sensible Daten, die nur einem eingeschränkten Personenkreis zugänglich gemacht werden sollen und die eine Reaktion erfordern.

- **Streng vertraulich:** Geheime, kritische Daten, bei deren Offenlegung es zu schwerwiegenden wirtschaftlichen oder sozialen Folgen kommen könnte. Hier gelten höchste Sicherheitsanforderungen.

Ihr Vorteil als Know-NOW User:

- **Freie Nutzung kostenloser Tools und Experten-Links**
- **Einrichtung und Nutzung eines Prepay-Kontos**
- **Einsparungen durch attraktive Bonusprogramme**

Kostenlos und unverbindlich registrieren unter

Die Klassifizierung hilft dabei den Zugriff auf sensible Daten entsprechend ihrer Sensibilität zu steuern und sicherzustellen, dass sie nur an autorisierte Personen weitergegeben werden.

www.know-now.de/join**Mitgeltende Dokumente:**

- VDA-Whitepaper „Harmonisierung der Klassifizierungsstufen“
- BSI-Merkblatt zum sicheren Informationsaustausch mit dem Traffic Light Protocol (TLP)

6. Klassifizierungsprozess

Zur Sicherstellung eines effizienten Vorgehens, ist der Klassifizierungsprozess klar strukturiert und einfach umsetzbar sein. Die folgenden Schritte sind zu beachten, um den Prozess optimal auszuführen:

• Identifikation der Informationen

Erfassen der zu klassifizierenden Informationen, wie Dokumente, E-Mails, Dateien oder andere Datenquellen durch operative Erfassung von neuen Informationen durch die jeweiligen Abteilungen oder durch automatisierte Systeme.

Sie möchten sich über dieses und weitere Tools informieren?

Klassifizierung durch Einstufung nach Sensibilität

Bewertung der Sensibilität der Informationen basierend auf ihrem Inhalt, ihrer Bedeutung und den potenziellen Risiken bei Offenlegung. Anhand der unter 5 definierten Vorgaben wird die Information der Klassifizierungsstufe „öffentliche, intern, vertraulich, streng vertraulich“ zugeordnet.

... nutzen Sie unseren Tool-Online-Shop:

Kennzeichnung der Informationen

Sichtbare oder elektronische Kennzeichnung der Information gemäß ihrer

Klassifizierung. Wir verwenden von Labels, Wasserzeichen, Metadaten oder Tags (z.B. auf Dokumenten, in Datensystemen oder E-Mail-Betreffzeilen). Unsere digitalen Systeme wenden die Kennzeichnungen automatisch an, oder leiten die Beschäftigten an, wie sie die richtige Markierung vornehmen.

- Festlegung der Zugriffsberechtigungen

Anhand der Klassifizierungsstufen werden rollenbasierte Zugriffsrechte zugeteilt (z.B. „Vertrauliche Informationen sind nur für Führungskräfte zugänglich“).

Die Grundlage bilden unsere IT-Systeme mit Zugriffssteuerungen und Berechtigungsmanagement.

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

Überprüfung und Aktualisierung
Klassifizierungen sind regelmäßig zu überprüfen, um sicherzustellen, dass sie noch gültig sind. Hierzu ist ein Überprüfungszyklus festzulegen, am besten mit einer Überprüfung alle 6 Monate. Alle Beschäftigten, Klassifizierungen zu überprüfen.

- Dokumentation und Protokollierung

Der Prozess der Klassifizierung mit dem Zugriff und Änderungen ist mit geeigneten IT-Tools zu protokollieren, um Transparenz und Nachvollziehbarkeit zu gewährleisten. Mit der Hilfe von Zugriffsprotokollen können Missbrauch oder Fehler zu identifiziert werden.

7. Umgang mit klassifizierten Informationen

Der Umgang mit klassifizierten Informationen, ist in Bezug auf die nachfolgenden Aspekte unter anderem in weiteren mitgeltenden Richtlinien oder Verfahren geregelt:

- Vorgaben für den sicheren Umgang, Speicherung und Transport von klassifizierten Informationen:
 - Richtlinie Clean-Desk
 - Richtlinie für den Zutritt
 - Richtlinie mobiles Arbeiten
 - Verfahren Kryptografie
- Verfahren zur Weitergabe und Teilung von Informationen, abhängig von ihrer Klassifizierung:
 - Richtlinie Bereitstellung von Rechtevergaben
 - Richtlinie Zugriffsmanagement

Sie möchten sich über dieses und weitere Tools informieren?

... nutzen Sie unseren Tool-Online-Shop:

Registrieren und downloaden!

Ihr Vorteil als Know-NOW User:

Diese Richtlinie zur Informationsklassifizierung trägt zur Erfüllung gesetzlicher als auch regulatorischer Vorgaben bei, die den Schutz sensibler Daten und die Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen betreffen. Sie ist ein wesentlicher Bestandteil unseres Compliance-Managements und hilft, uns rechtliche Risiken zu minimieren.

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Nachfolgend sind exemplarisch wichtige Anforderungen und Compliance-Aspekte aufgelistet:

Kostenlos und unverbindlich registrieren unter

- DSGVO (Datenschutz-Grundverordnung) bzw. BDSG-Bundesdatenschutzgesetz
- Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)
- NIS-Richtlinie (EU-Richtlinie über die Sicherheit von Netz- und Informationssystemen)
- Vertraulichkeitsvereinbarungen (NDAs): Verträge mit Geschäftspartnern oder Kunden
- Outsourcing- und Dienstleistungsverträge

www.know-now.de/join

- BSIG (Bundesamt für Sicherheit in der Informationstechnik Gesetz)
- NIS-Richtlinie (EU-Richtlinie über die Sicherheit von Netz- und Informationssystemen)
- Vertraulichkeitsvereinbarungen (NDAs): Verträge mit Geschäftspartnern oder Kunden
- Outsourcing- und Dienstleistungsverträge

9. Überprüfung, Sensibilisierung und Verbesserung

Die Richtlinie wird regelmäßig überprüft und aktualisiert, um sicherzustellen, dass sie den aktuellen Bedrohungen und gesetzlichen Anforderungen entspricht. Im Rahmen der Schulungsplanung finden regelmäßige Schulungen und Sensibilisierungsprogramme für alle Mitarbeiter statt, um das Bewusstsein für Informationssicherheit und den richtigen Umgang mit klassifizierten Informationen zu fördern.

Sie möchten sich über dieses und weitere Tools informieren?

... nutzen Sie unseren Tool-Online-Shop:
Registrieren und downloaden!

10. Dokumentenentwicklung und Änderungshistorie

Diese Richtlinie wird über das Intranet zur Verfügung gestellt.

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

Verantwortlicher

[z.B. URL der Datei auf dem Server]

Aktuelle Version

1.0

Datum Erstellung / letzte Änderung

19.07.2025

Nächstes Dokumenten-Review

19.07.2026

Dokumentenhistorie

Version	Freigegeben am	Freigegeben durch	Kommentar
1.0	19.07.2025		

Sie möchten sich über dieses und weitere Tools informieren?

Hinweise zur Zuordnung zur DIN EN ISO 27001 bzw. TISAX®

... nutzen Sie unseren Tool-Online-Shop:

VKA Softwareentwicklung 1347-Softwarelösungen (Viktoria)

„Ein einheitliches Schema zur Klassifizierung von Informationswerten hinsichtlich des Schutzzieles Vertraulichkeit ist verfügbar.“

Registrieren und downloaden!

DIN EN ISO 27001, Anhang A 5.12, Klassifizierung von Informationen:

„Informationen müssen entsprechend den Informationssicherheitsforderungen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen der interessierten Parteien klassifiziert werden.“

Hinweise zur Nutzung der Vorlage

Diese Arbeitshilfe soll nur eine ausführliche Vorlage für eine „Richtlinie zum Umgang mit Informationssicherheitsvorfällen“ darstellen. Sie wurde nach bestem Wissen und Gewissen recherchiert, zusammengestellt und überprüft. Sie erhebt aber keinen Anspruch auf Vollständigkeit oder Eignung für den Einzelfall und erlaubt keine ausschließliche Anwendbarkeit für ein Unternehmen.

Jede Person, die dieses Produkt erwirbt ist verpflichtet, ihre individuellen Ergänzungen und Anpassungen vorzunehmen und alle Inhalte für den eigenen Anwendungsfall zu prüfen, d.h. diese ggf. mit eigenen Texten zu erweitern oder nicht passende Inhalte zu entfernen.

Die nachfolgende Liste gibt Ihnen einige Hinweise, worauf Sie bei der Ergänzung mit eigenen Texten bzw. Textmodulen unbedingt achten sollten:

1. Wählen Sie einfache, allgemein verständliche Formulierungen und schreiben Sie keine „Bandwurmsätze“.
2. Benutzen Sie eine verständliche Wortwahl und erklären Sie nicht vermeidbares Fachvokabular.
3. Formulieren Sie nicht zu sehr ins Detail gehend.
4. Geben Sie den Mitarbeitern im Rahmen von Workshops die Gelegenheit auf die Formulierungen Einfluss zu nehmen.

Hinweise zur Anpassung des Dokumentes an die Organisation:

Um das Tool an Ihre Dokumentenstruktur anzupassen, gehen Sie (hier am Beispiel der Version MS Office 2010 dargestellt) bitte folgendermaßen vor:

1. Aktivieren Sie in der Leiste „Start“, Gruppe „Absatz“ das Symbol „Alle anzeigen“. Alternativ können Sie in der Leiste „Datei“ auf „Optionen“ klicken, im sich öffnenden Fenster „Anzeige“ auswählen und das Häkchen bei „alle Formatierungszeichen anzeigen“ setzen.
2. Löschen Sie nun zuerst das Textfeld mit dem Titel und danach die Grafik, indem Sie diese Objekte jeweils markieren und die Entfernen-Taste (Entf) betätigen.
3. Danach löschen Sie den verbliebenen Abschnittswechsel (oben), indem Sie diesen markieren und ebenfalls die Entfernen-Taste (Entf) betätigen.
4. Mittels „Doppelklick“ auf die Kopf- oder Fußzeile können Sie diese nun öffnen und die Texte und deren Formatierungen entsprechend Ihren Wünschen gestalten.
5. Löschen Sie das Kopfzeilen-Logo wie vorher, indem Sie dieses markieren und die Entfernen-Taste (Entf) betätigen.
6. Ein neues Logo fügen Sie ein, indem Sie in der Leiste „Einfügen“, Gruppe „Illustrationen“ auf das Icon „Grafik“ klicken und Ihre Datei auswählen.
7. Diese Hinweise Seite entfernen Sie, indem Sie (ab dem letzten Seitenumbruch) alles markieren und die Entfernen-Taste (Entf) betätigen.

Nutzungsbedingungen von Fachinformationen:

- (1) Für vorsätzliche oder grob fahrlässige Pflichtverletzungen haftet der Lizenzgeber. Dies gilt auch für Erfüllungsgehilfen.
- (2) Für Garantien haftet der Lizenzgeber unbeschränkt.
- (3) Für leichte Fahrlässigkeit haftet der Lizenzgeber begrenzt auf den vertragstypischen, vorhersehbaren Schaden.
- (4) Der Lizenzgeber haftet nicht für Schäden, mit deren Entstehen im Rahmen des Lizenzvertrags nicht gerechnet werden musste.
- (5) Für Datenverlust haftet der Lizenzgeber nur, soweit dieser auch bei der Sorgfaltspflicht entsprechender Datensicherung entstanden wäre.
- (6) Eine Haftung für entgangenen Gewinn, für Schäden aus Ansprüchen Dritter gegen den Lizenznehmer sowie für sonstige Folgeschäden ist ausgeschlossen.
- (7) Der Lizenzgeber haftet nicht für den wirtschaftlichen Erfolg des Einsatzes der Tools oder Trainings.
- (8) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.