



Ein ITQ-Produkt

# NIS2 Status-Check

**Kriterienkatalog NIS2v01**

**Geprüftes Unternehmen**

**Produktvorstellung Bericht**

# Inhalt

Audit Facts	4
Disclaimer	5
Einleitung	6
Ziel der Prüfung	6
Prüfungsumgebung	6
Management Summary	7
Übersicht der durchgeführten Arbeiten	7
Nächste Schritte und Entscheidungshilfen	8
Erfüllungsgrad	9
Fazit	10
Maßnahmenempfehlungen	13
Prüfgruppen und Prüfpunkte	15
Organisation	15
1 Richtlinien für Informationssicherheit	15
2 Assetmanagement	16
3 Gebrauch von Assets	17
4 Informationsaustausch	17
5 Zugangssteuerung	18
6 Identitätsmanagement	18
7 Authentifizierung	19
8 Zugriffsrechte	19
9 Lieferantenmanagement (inkl. Cloud-Dienste)	20
10 Management von Sicherheitsvorfällen	21
11 Sicherstellung der Geschäftskontinuität	22
12 Interne Audits	22
13 Betriebsverfahren	23
14 Sicherheitspolitik	23
15 Risikomanagement	24
16 Kommunikation im ISMS	25
17 Überwachung	26
18 Management Review (Inhalte)	27
19 Maßnahmenmanagement	27
20 Physische Umgebungssicherheit	28
21 Registrierungspflichten gegenüber BSI	28
Personal	29
22 Personalsicherheit	29
23 Mitarbeitersensibilisierung	29
24 Fachkompetenz	30
Technik	31
25 Schwachstellenmanagement	31

26 Konfigurationsmanagement	31
27 Datensicherungsmanagement	32
28 Netzwerkmanagement	33
29 Kryptografie	34
33 Änderungsmanagement	35
34 Redundanz der IT	36
35 Monitoring und Logging	36
Anhänge	37
Firmenprofile und Kontakt	38
Übergabebestätigung	39

# Audit Facts

Geprüftes Unternehmen	Produktvorstellung Bericht
Ansprechpartner	Michael Scott / mscott@dunder-mifflin.de / 0800-600155
Prüfzeitraum	26.03.2024 - 06.05.2024
Berichtsnummer	B433.284
ITQ-Partner	FormaCom
Auditor	Dennis Joist
Auditor-Kennung	A485.102
Verteiler	
Audit-Typ	Ist Analyse
Prüferte	Dunder Mifflin Paper Company, Inc Bahnhofstr. 6 65501 Bogenberg

# Disclaimer

Die ITQ hat ein allgemeines Anforderungsprofil mit Voraussetzungen erstellt, die für den sicheren IT-Betrieb erforderlich sind. Wir weisen ausdrücklich darauf hin, dass auf Grund besonderer Umstände und individueller Eigenschaften Ihres Unternehmens, eventuell weitere Anforderungen gestellt werden müssten, um ein angemessenes Sicherheitsniveau zu erreichen.

Grundlage der Ermittlung, inwieweit Anforderungen erfüllt sind oder nicht vorliegen, sind neben persönlichen Gesprächen, auch übersendete Unterlagen. Die Vollständigkeit und Richtigkeit von Aussagen bzw. Unterlagen kann von uns nicht überprüft werden. Insofern können wir keine Haftung für die ganzheitliche Vollständigkeit oder Richtigkeit des Berichtes bzw. der Maßnahmenempfehlungen übernehmen.

# Einleitung

## Ziel der Prüfung

Das Ziel des NIS2 Status-Checks ITQ (Network and Information Systems Directive 2) liegt darin, die Sicherheit und Widerstandsfähigkeit digitaler Dienste und Netzwerke innerhalb kritischer Sektoren zu gewährleisten. Dieser Prüfprozess zielt darauf ab, die Einhaltung der NIS2-Richtlinie sicherzustellen und die Effektivität der implementierten Sicherheitsmaßnahmen zu überprüfen. Zentrale Aspekte der Prüfung sind die Identifikation kritischer Dienste, die Bewertung der getroffenen Sicherheitsvorkehrungen sowie die Feststellung von potenziellen Schwachstellen in Netzwerken und Informationssystemen.

Ein weiteres Ziel besteht darin, sicherzustellen, dass angemessene Maßnahmen vorhanden sind, um auf Cyberbedrohungen oder Störungen zu reagieren und die Kontinuität kritischer Dienste zu gewährleisten. Der NIS2 Status-Check ITQ beinhaltet außerdem die Überprüfung der Compliance mit den Richtlinien, insbesondere hinsichtlich der Meldung von Sicherheitsvorfällen an die nationalen Behörden. Es soll darüber hinaus dazu dienen, die allgemeine Cyberresilienz zu verbessern und bewährte Sicherheitspraktiken zu identifizieren und zu fördern.

Insgesamt zielt die Prüfung darauf ab, die Widerstandsfähigkeit gegenüber Cyberbedrohungen zu stärken, potenzielle Risiken zu minimieren und somit die Integrität, Vertraulichkeit und Verfügbarkeit digitaler Dienste in kritischen Sektoren zu gewährleisten. Dies trägt dazu bei, die Sicherheit und Stabilität der Gesellschaft als Ganzes zu unterstützen.

## Prüfungsumgebung

Das Unternehmen aus der Branche der Lebensmittelindustrie hat seinem Hauptstandort in Bogenberg. Derzeit werden insgesamt 40 Mitarbeitende beschäftigt, denen derzeit 40 PC-Arbeitsplätze zur Verfügung stehen. Gegenstand der Prüfung ist der gesamte Geltungsbereich des Unternehmens ohne Ausschlüsse. Mangels Entwicklungstätigkeiten wurden die Prüfgruppen bezüglich dieses Sachverhaltes aus dem Anforderungskatalog entfernt. Die Infrastruktur besteht im Wesentlichen aus 3 Servern, 18 virtuellen Maschinen, sowie weiteren Netzwerkkomponenten, wie Firewalls, Switches etc. Daneben werden Dienste von Microsoft genutzt, die im externen Rechenzentrum bereitgestellt werden.

# Management Summary

## Übersicht der durchgeführten Arbeiten

Im Rahmen des ITQ NIS2 Status-Checks wurde durch unterschiedliche Auditmethoden der aktuelle Umsetzungsstand ermittelt.

Maßstab für die Bestimmung des Sicherheitsniveaus ist ein Anforderungskatalog, der von der ITQ entwickelt wurde und insgesamt 261 Fragen umfasst, die 35 unterschiedlichen Prüfgruppen zugeordnet wurden. Die jeweiligen Ergebnisse pro Prüfgruppe können dem Diagramm „Erfüllungsgrad“ entnommen werden.

Es wurde für alle festgestellten Mängel oder Sicherheitslücken eine Liste mit Maßnahmenempfehlungen erstellt. Eine detaillierte Übersicht der Prüfungsergebnisse zu den einzelnen Fragen kann dem beigefügten Bericht entnommen werden.

### **Dokumentationsprüfung**

Aktivitätsanalyse

Messdatenanalyse

Ansichtsnahme

**Befragung**

**Unterlagensichtung**

# Nächste Schritte und Entscheidungshilfen

Es wird empfohlen die erstellten Maßnahmen Schritt-für-Schritt im Rahmen eines kontinuierlichen Prozesses umzusetzen, da sich die Verwirklichung in einem großen Schritt in der Praxis als zu ehrgeizig erwiesen.

Die Maßnahmenempfehlung ist als erster unverbindlicher Umsetzungsplan zu verstehen und soll einen Überblick verschaffen, welche Aufgaben es zu erfüllen gilt. Zunächst sollte eine Einteilung in technische und organisatorische Maßnahmen erfolgen, um eine Zuweisung zu den jeweiligen Fachbereichen zu erleichtern. Im nächsten Schritt ist der jeweilige personelle, finanzielle und organisatorische Ressourcenaufwand zu bestimmen und die Reihenfolge der Umsetzung festzulegen, wobei wir folgende Empfehlungen und Hinweise geben möchten:

- ✓ Maßnahmen mit Flächenwirkung, d.h. es werden gleichzeitig mehrere Anforderungen erfüllt
- ✓ Maßnahmen, die ein hohes Risiko abstellen
- ✓ Maßnahmen im organisatorischen Bereich sind kurzfristig und günstig zu erledigen
- ✓ Maßnahmen für Bereiche mit auffallend vielen Mängeln
- ✓ Maßnahmen, die zur Erfüllung einer anderen erforderlich sind

Bei der Budgetierung sollte beachtet werden, dass Informationssicherheit als Prozess zu verstehen ist und Maßnahmen mitunter kontinuierlich wiederholt werden müssen. Ordnen Sie die unterschiedlichen Maßnahmen thematisch und definieren Sie Verantwortlichkeiten für deren Umsetzung.

Der Ergebnisbericht ist so ausgestaltet, dass sich Dokumente, Richtlinien und Prozessbeschreibungen von technischen Aufgaben unterscheiden, wodurch eine Zuteilung zu einzelnen Personen erleichtert wird. In einer Checkliste werden die einzelnen Anforderungen aufgezählt, die zur Erfüllung der Maßnahme erforderlich sind. So kann die Unternehmensleitung gezielt und konkret delegieren, was es zu erledigen gilt.

Bei weiteren Fragen stehen wir Ihnen gerne zur Verfügung!

# Erfüllungsgrad

Nachfolgend erhalten Sie eine grafische Übersicht der geprüften Bereiche, die jeweils in Prüfgruppen unterteilt sind. Der Erfüllungsgrad wird in Prozent angegeben, wobei 100% einer vollständigen Konformität der jeweiligen Prüfgruppe entsprechen.



# Fazit

Die Anforderung und Empfehlungen zur Umsetzung der NIS2-Richtlinie sind derzeit zu 50 Prozent erfüllt. Im weiteren Verlauf des Fazits wird erfolgt eine kurze Zusammenfassung des jeweiligen Standes des Prüfbereiches. Die konkreten Korrekturmaßnahmen können im Detail dem Bericht entnommen werden. Es empfiehlt sich, unter Berücksichtigung des jeweiligen Erfüllungsgrades, die unterschiedlichen Aufgabenbereiche zu projektieren, um eine zeitnahe Umsetzung sicherzustellen. Dabei sollten diejenigen Bereiche mit niedrigen Erfüllungsgrad vorrangig bearbeitet werden, so dass keine Lücken entstehen im Vergleich zu anderen Bereichen, die bereits gut aufgestellt sind. Es hat sich als zielführend erwiesen, einzelne Workshops zu den einzelnen Themen durchzuführen, um die Anforderungen nachhaltig umzusetzen.

Beachten Sie die zusammenfassenden Hinweise der jeweiligen Prüfgruppen, wobei der entwicklungsbezogene Bereich nicht Gegenstand der Prüfung gewesen ist mangels Relevanz. Prüfbereiche ohne Erwähnung sind bereits vollständig erfüllt.

## 1) Richtlinien für Informationssicherheit

Im Bereich des Dokumentenmanagements fehlen notwendige Nachweise bezüglich Freigabe, Versionierung und der Revision.

## 2) Assetmanagement

Eine vollständige Übersicht aller unternehmensrelevanten Assets ist derzeit nicht vorhanden, zudem ist deren jeweilige Kritikalität für den Unternehmenserfolg nicht festgehalten worden

## 3) Gebrauch von Assets

Eine Richtlinie zum Management von Assets fehlt bislang, zudem ist eine Klassifizierung hinsichtlich der jeweiligen Vertraulichkeit noch nicht durchgeführt worden.

## 5) Zugangssteuerung

Die Anforderungen sind nahezu vollständig umgesetzt, allerdings haben Benutzer noch lokale Administratorrechte auf ihren Endgeräten. Dieser Zustand sollte dringend beseitigt werden.

## 7) Authentifizierung

Es muss lediglich flächendeckend die geforderte Multi-Faktor-Authentifizierung umgesetzt werden.

## 8) Zugriffsrechte

Zugriffe auf Systeme müssen geloggt, analysiert und dokumentiert werden.

## 9) Lieferantenmanagement

Es existiert lediglich eine Übersicht der Lieferanten, allerdings ohne Berücksichtigung der notwendigen Anforderungen aus dem Bereich der Informationssicherheit.

#### 10) Management von Sicherheitsvorfällen

Es gibt bereits eine angemessene Dokumentation, die um einige weitere Notfallthemen angereichert werden sollte. (allen voran Ransomware-Angriffe)

#### 11) Sicherstellung der Geschäftskontinuität

Im Bereich des Business Continuity Management sind nahezu noch alle Maßnahmen offen.

#### 12) Interne Audits

Ein internes Audit-Management inkl. einer fortlaufenden Berichterstattung an die Leitungsebene ist bislang noch nicht etabliert.

#### 13) Betriebsverfahren

Es liegen bereits Dokumentationen zu unterschiedlichen Betriebsverfahren vor, die jedoch erweitert werden müssten, um die im Bericht genannten Sachverhalte.

#### 15) Risikomanagement

Im Risikomanagement sind lediglich noch ein paar Details zu ergänzen, um einen nachhaltigen und fortlaufenden Prozess sicherzustellen. (Angaben in der Risikoleitlinie)

#### 16) Kommunikation im ISMS

Ein ISMS (Informationssicherheitsmanagementsystem ist bislang noch nicht umgesetzt worden.

#### 17) Überwachung

Mangels ISMS findet derzeit auch keine Überwachung desgleichen statt.

#### 18) Management Review

Reports für die Leitungseben bezüglich des Status des ISMS werden nicht erstellt.

#### 19) Maßnahmenmanagement

Eine zentrale Übersicht aller erforderlichen Maßnahmen zur Aufrechterhaltung eines angemessenen Sicherheitsniveaus gibt es derzeit nicht.

#### 20) Physische Umgebungssicherheit

Es fehlt hier lediglich an einer Definition der unterschiedlichen Sicherheitszonen im Unternehmen und der jeweiligen Berechtigungen zum Zutritt.

#### 21) Registrierungspflichten gegenüber dem BSI

Die Registrierungspflichten werden erst ausgelöst mit Verabschiedung des Gesetzes, sollen hier jedoch als Erinnerung offenstehen.

#### 22) Personalsicherheit

Das Personalmanagement hat die überwiegende Anzahl der Anforderungen bereits umgesetzt und sollte noch Geheimhaltungsvereinbarungen mit Mitarbeitenden bzw. Dritten abschließen.

#### 23) Mitarbeitersensibilisierung

Mit der NIS2-Richtlinie wird nunmehr auch die Leitungsebene verpflichtet an Schulungen

teilzunehmen, diese wurde bislang nicht durchgeführt.

#### 24) Fachkompetenz

Zur Sicherstellung der Kompetenz sollten die zuständigen Mitarbeitenden für das Thema Informationssicherheit Schulungen erhalten.

#### 25) Schwachstellenmanagement

Ein weitergehendes Monitoring von Schwachstellen durch entsprechende Analysen findet derzeit nicht statt.

#### 26) Konfigurationsmanagement

Eine umfassende IT-Dokumentation gibt es bislang nicht, zudem fehlt ein definierter Änderungsmanagementprozess.

#### 27) Datensicherungsmanagement

Die Sicherungsjobs sollten konkreter definiert werden unter Berücksichtigung der jeweiligen Kritikalität der verarbeiteten Informationen.

#### 28) Netzwerkmanagement

Im Netzwerkmanagement sollte die Dokumentation erweitert werden, so dass die Spielregeln klar definiert sind.

#### 29) Kryptografie

Das Verfahren zum Management von Schlüsseln (Encryption Keys) sollte nachvollziehbar dokumentiert werden.

#### 33) Änderungsmanagement

Änderungen an der IT-Infrastruktur, Software oder an Geschäftsprozessen werden bislang nicht ausreichend dokumentiert bzw. unterliegen keinem Freigabeverfahren.

#### 34) Redundanz der IT

Es sollte geprüft werden, in welchen Bereichen und für welchen Systeme bzw. Anwendungen weitere Redundanzen notwendig sind, um die Anforderungen des Unternehmens zu erfüllen.

#### 35) Monitoring und Logging

Es sind nicht alle relevanten Systeme im Monitoring berücksichtigt.

# Maßnahmenempfehlungen

Diese Übersicht mit offenen Maßnahmen ist als erster Umsetzungsplan zu betrachten, kann jedoch auch individuell an das Unternehmen angepasst werden. Die Sortierung der einzelnen Maßnahmen erfolgt auf Basis des jeweiligen Reifegrades.

Maßnahmen **ohne Umsetzung** sind in rot gekennzeichnet.

Maßnahmen **mit Hauptabweichungen** sind in apricot gekennzeichnet.

Maßnahmen **mit Nebenabweichungen** sind in orange gekennzeichnet.

Maßnahmen **im Planungsstatus** sind in blau gekennzeichnet.

Kennung	Bezeichnung	Prüfpunkt
ORG02	Einführung bzw. Verbesserung des Assetmanagements	2
ORG09	Einführung eines umfassenden Lieferantenmanagements	9
ORG17	Sicherstellung der kontinuierlichen Verbesserung des ISMS	17
TEC09	Änderungsmanagementprozess einführen bzw. verbessern	33
Kennung	Bezeichnung	Prüfpunkt
ORG01	Erstellung und Verwaltung von IT-Richtlinien umsetzen	1
ORG03	Regelung des zulässigen Gebrauchs von Assets	3
ORG05	Umsetzung eines restriktiven Rechtekonzeptes für alle Zugänge	5
ORG07	Verbesserung des internen Passwortmanagements samt MFA	7
ORG08	Verbesserung des Rechtemanagements	8
ORG11	Erstellung von Wiederherstellungs- und Geschäftsfortführungsplänen	11
TEC01	Umsetzung eines umfassenden Schwachstellenmanagements	25
TEC04	Schutzmaßnahmen für das Netzwerk erweitern	28
TEC05	Angemessene Kryptografie und Schlüsselverwaltung umsetzen	29
Kennung	Bezeichnung	Prüfpunkt
ORG15	Umsetzung eines umfassenden Risikomanagements für die Institution	15
ORG18	Erstellung regelmäßiger Management Reviews	18
ORG20	Schutz der Betriebsumgebung verbessern	20
PER02	Einführung eines umfassenden Schulungsmanagements	23
PER03	Sicherstellung der Fachkompetenz der Verantwortlichen	24
TEC02	Angemessene Kryptografie und Schlüsselverwaltung	26
TEC03	Verbesserung des Datensicherungsmanagements	27
TEC10	Redundanz der informationstechnischen Anlagen erhöhen	34
TEC11	Monitoring und Logging verbessern	35
Kennung	Bezeichnung	Prüfpunkt
ORG10	Verbesserung des Managements von IT-Sicherheitsvorfällen	10

# Prüfgruppen und Prüfpunkte

Es folgt eine detaillierte Aufführung der geprüften Bereiche, sowie der konkreten Maßnahmen zur Beseitigung von Nichtkonformitäten. Die Reihenfolge der Abschnitte stellt keine Priorisierung dar, sondern orientiert sich an den jeweiligen geprüften Themenbereichen. Daher sollte jedes Unternehmen, die für Sie zutreffenden Maßnahmen identifizieren und entsprechend eigenständig priorisieren, hinsichtlich der Umsetzungsreihenfolge.

## Organisation

### 1 Richtlinien für Informationssicherheit

Reifegrad IN PLANUNG UMGESETZT UMGESETZT MIT NEBENABWEICHUNGEN UMGESETZT MIT HAUPTABWEICHUNGEN NICHT UMGESETZT

In unserer zunehmend digitalisierten Welt sind klare IT-Richtlinien von entscheidender Bedeutung. Angesichts der wachsenden Komplexität und Vernetzung von IT-Systemen bieten solche Richtlinien nicht nur Schutz vor Bedrohungen für sensible Daten, sondern fördern auch Transparenz, Compliance und effiziente Ressourcennutzung. Sie sind essenziell, um den ständigen Veränderungen im digitalen Umfeld proaktiv zu begegnen und das Vertrauen von Kunden, Partnern und Mitarbeitern in die Integrität der IT-Systeme zu gewährleisten. In diesem Zusammenhang ist es unerlässlich zu verstehen, warum IT-Richtlinien eine grundlegende Rolle in der zeitgemäßen IT-Governance und im Risikomanagement spielen.

Kennung: **Korrekturmaßnahmen**

- 1.1 Richtlinien müssen von der Leitungsebene genehmigt sein samt Nachweis (Unterschrift bzw. digitale Genehmigung)
- 1.2 Die Richtlinie müssen an einem einsehbaren Ort veröffentlicht sein (Intranet, SharePoint, Fileserver)
- 1.3 Mitarbeiter müssen wissen, wo die Richtlinien auffindbar sind
- 1.4 Nachweise der Revision müssen vorgelegt werden können (Dokumentation im Ticket, Chronik, Revision SharePoint)

**Bemerkung:**

Es sind bereits eine Vielzahl der notwendigen Richtlinien vorhanden, diese sollten noch um die fehlenden Dokumente ergänzt werden.

## 2 Assetmanagement

Reifegrad IN PLANUNG UMGESETZT UMGESETZT MIT NEBENABWEICHUNGEN UMGESETZT MIT HAUPTABWEICHUNGEN NICHT UMGESETZT

In der heutigen schnelllebigen IT-Landschaft spielt das IT-Assetmanagement eine entscheidende Rolle für den Erfolg von Unternehmen. Dieser strategische Ansatz ermöglicht es Organisationen, ihre IT-Ressourcen effizient zu planen, überwachen und verwalten. Von Hardware bis zu Softwarelizenzen stellt das IT-Assetmanagement sicher, dass Investitionen optimiert und Compliance sowie Sicherheitsstandards eingehalten werden. Nicht nur eine administrative Aufgabe, sondern ein strategisches Instrument, trägt es dazu bei, die Wettbewerbsfähigkeit in einer sich ständig wandelnden digitalen Welt zu erhalten.

Kennung: **Korrekturmaßnahmen**

- 2.1 Informationen und Werte sind zu identifiziert (z.B. durch Scans, Schutzbedarfsanalyse)
- 2.2 Der Schutzbedarf von Informationen und Vermögenswerten ist zu bestimmen (Schutzbedarfsanalyse)
- 2.3 Informationen und Werte inkl. virtuelle Maschinen müssen dokumentiert sein (Asset-Inventar)
- 2.4 Dokumentation ist aktuell und vollständig zu halten (keine leeren Informationsfelder)
- 2.5 Die Eigentümer der Werte sind festzulegen
- 2.6 Die Standorte von Vermögenswerten sind aufzuzeichnen
- 2.7 Vermögenswerte müssen klassifiziert werden nach Vertraulichkeit
- 2.8 Vermögenswerte müssen bei Änderungen angepasst werden (Anweisung zur Anpassung der Asset-Informationen, z.B. als Routineaufgabe)

### 3 Gebrauch von Assets

Reifegrad IN PLANUNG UMGESETZT UMGESETZT MIT NEBENABWEICHUNGEN UMGESETZT MIT HAUPTABWEICHUNGEN NICHT UMGESETZT

Die Regelungen zum Gebrauch von Assets erstrecken sich über Hardware, Software und Daten, und gewährleisten nicht nur Sicherheit und Compliance, sondern maximieren auch den Nutzen Ihrer IT-Ressourcen. Durch klare Anforderungen für den Zugang, die Nutzung und Pflege der Assets, wird die betriebliche Stabilität gefördert, der Schutz vor Sicherheitsrisiken verbessert und die langfristige Werthaltigkeit Ihrer IT-Investitionen gewährleistet. Zusätzlich minimiert sie rechtliche Risiken, indem sie die Einhaltung gesetzlicher Vorschriften und Industriestandards sicherstellt. Kurz gesagt, ist die Regelung zum Gebrauch von IT-Assets ein unverzichtbarer Bestandteil Ihrer Unternehmensstrategie zur Optimierung von Technologien, Risikominimierung und nachhaltigen Nutzung digitaler Ressourcen.

Kennung: **Korrekturmaßnahmen**

- 3.1 Zugangsbeschränkungen auf Informationen gem. Klassifizierung müssen vorhanden sein (restriktive Rechte)
- 3.2 Kennzeichnung von Speichermedien nach Klassifizierungsschema vornehmen (z.B. durch Aufkleber)
- 3.3 Es muss eine themenspezifische Richtlinie zur akzeptablen Nutzung geben (idR mehrere Richtlinien)
- 3.4 Verfahren zur akzeptablen Nutzung müssen dokumentiert, kommuniziert und vorhanden sein (Richtlinien für Datenträger, Dokumente, Anwendungen etc.)

**Bemerkung:**

Die Klassifizierung der Assets hinsichtlich ihrer Kritikalität ist elementar für die jeweiligen Anforderungen bezüglich deren Umgang. In Office Dokumenten lässt sich dies durch eine technische Richtlinie umsetzen.

### 4 Informationsaustausch

Reifegrad IN PLANUNG UMGESETZT UMGESETZT MIT NEBENABWEICHUNGEN UMGESETZT MIT HAUPTABWEICHUNGEN NICHT UMGESETZT

Effektive Regelungen zum Informationsaustausch von vertraulichen Informationen sind für Unternehmen unerlässlich. Sie gewährleisten nicht nur den sicheren Austausch sensibler Daten, sondern auch die Wahrung von Vertraulichkeit und Compliance. Solche Regelungen sind essenziell, um geschäftskritische Informationen zu schützen und gleichzeitig einen reibungslosen Austausch innerhalb des Unternehmens zu ermöglichen.