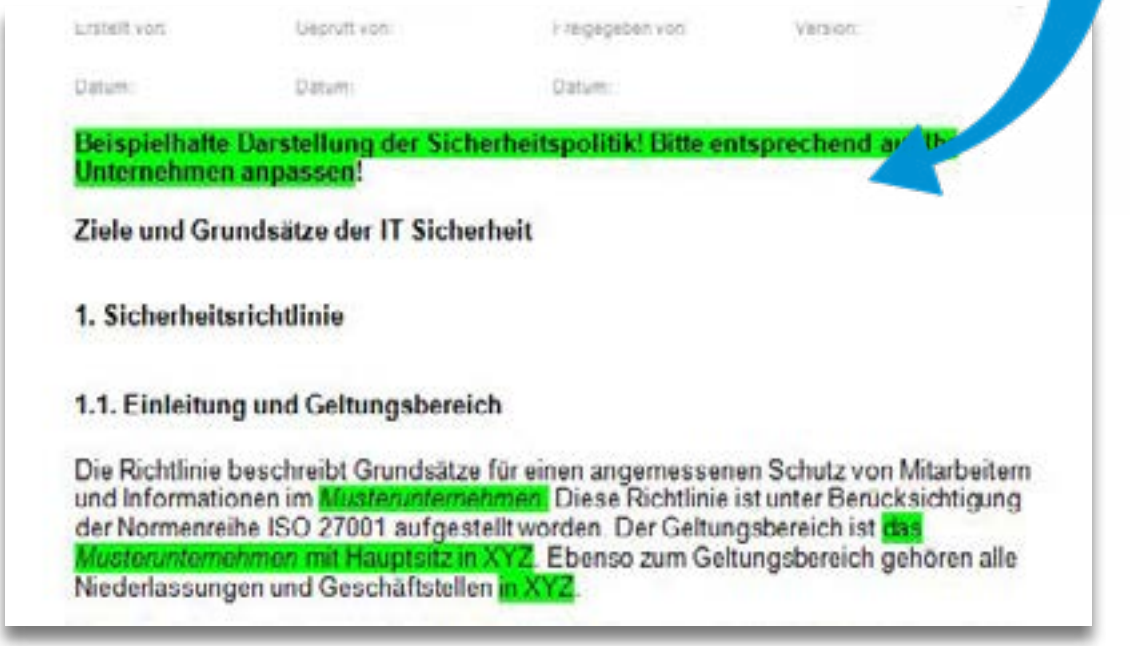
ISMS IT-Sicherheits-politik gem. ISO 27001 und ISO 27002

Word-Vorlage

Word-Vorschau

Hier werden nur Auszüge dargestellt!
Nach dem Erwerb steht Ihnen selbstverständlich die vollständige Version im offenen Dateiformat zur Verfügung.



Erstellt von: Geprüft von: Freigegeben von: Version:

Datum: Datum: Datum:

Beispielhafte Darstellung der Sicherheitspolitik! Bitte entsprechend a[illegible] Unternehmen anpassen!

Ziele und Grundsätze der IT Sicherheit

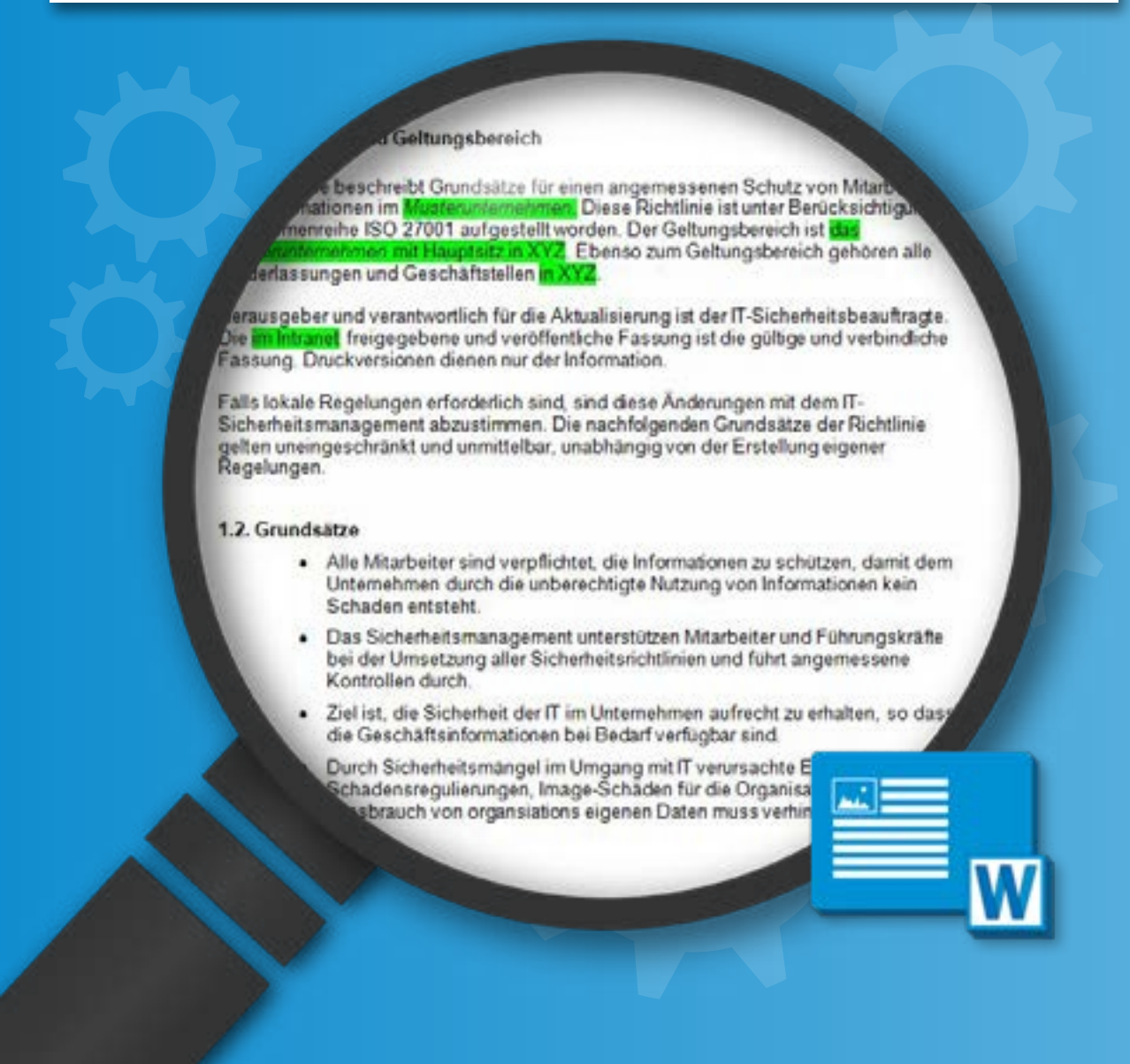
1. Sicherheitsrichtlinie

1.1. Einleitung und Geltungsbereich

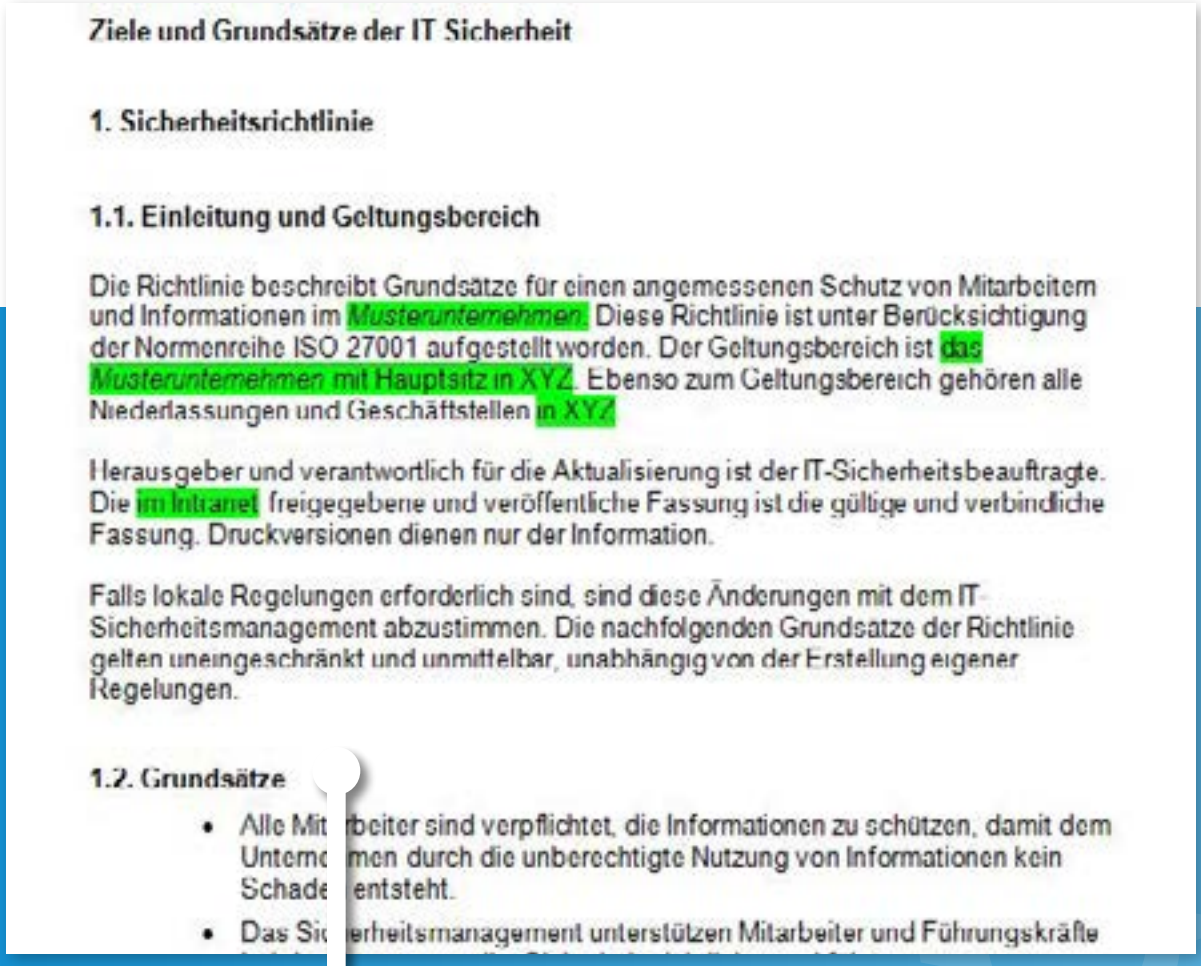
Die Richtlinie beschreibt Grundsätze für einen angemessenen Schutz von Mitarbeitern und Informationen im *Musterunternehmen*. Diese Richtlinie ist unter Berücksichtigung der Normenreihe ISO 27001 aufgestellt worden. Der Geltungsbereich ist das *Musterunternehmen* mit Hauptsitz in XYZ. Ebenso zum Geltungsbereich gehören alle Niederlassungen und Geschäftstellen in XYZ.

Übersicht

- Übersicht über eine beispielhafte IT Sicherheitspolitik
- Grundlage für die Entwicklung eines unternehmens-spezifischen IT Sicherheitskonzeptes
- Berücksichtigung gesetzlicher Regelungen und Forderungen



Inhalt



Ziele und Grundsätze der IT Sicherheit

1. Sicherheitsrichtlinie

1.1. Einleitung und Geltungsbereich

Die Richtlinie beschreibt Grundsätze für einen angemessenen Schutz von Mitarbeitern und Informationen im *Musterunternehmen*. Diese Richtlinie ist unter Berücksichtigung der Normenreihe ISO 27001 aufgestellt worden. Der Geltungsbereich ist das *Musterunternehmen* mit Hauptsitz in XYZ. Ebenso zum Geltungsbereich gehören alle Niederlassungen und Geschäftstellen in XYZ.

Herausgeber und verantwortlich für die Aktualisierung ist der IT-Sicherheitsbeauftragte. Die im Intranet freigegebene und veröffentliche Fassung ist die gültige und verbindliche Fassung. Druckversionen dienen nur der Information.

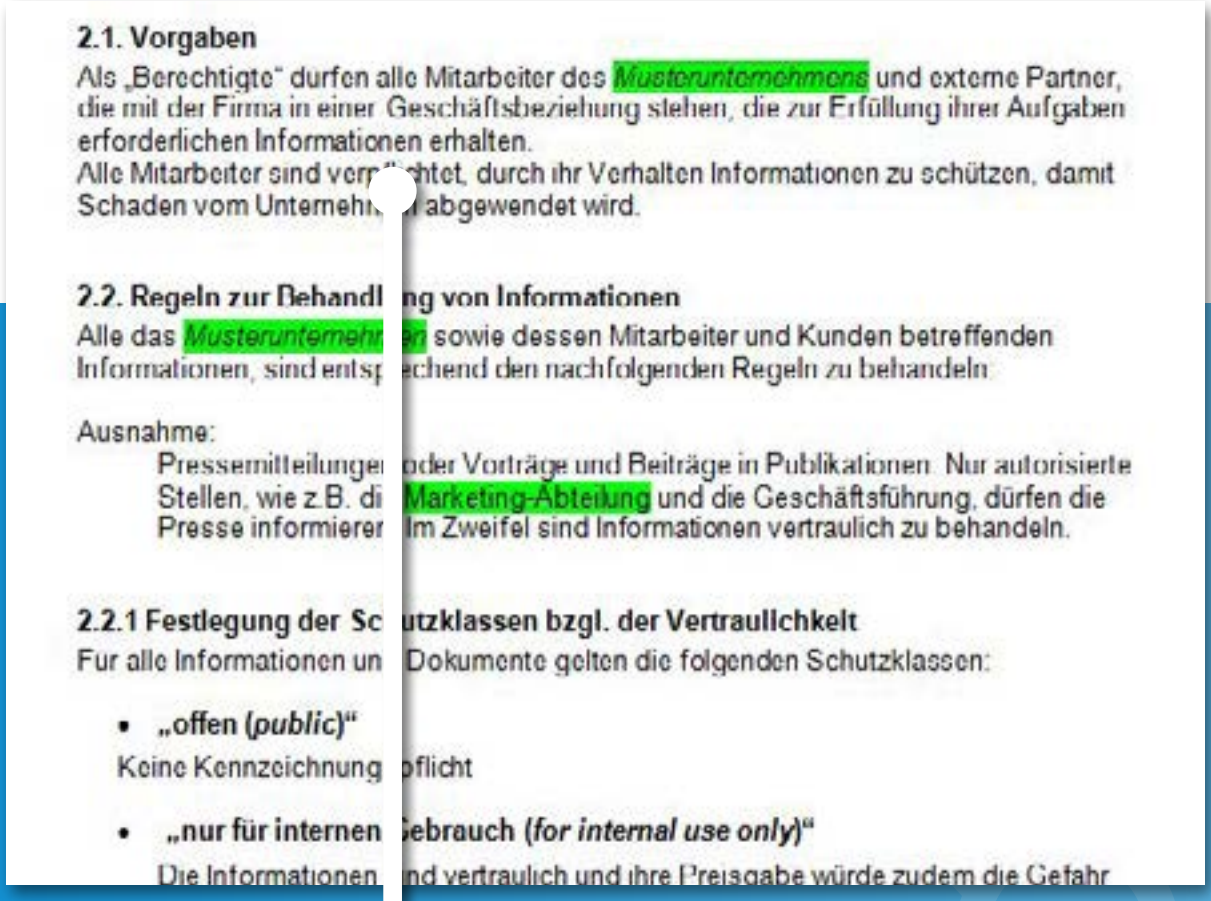
Falls lokale Regelungen erforderlich sind, sind diese Änderungen mit dem IT-Sicherheitsmanagement abzustimmen. Die nachfolgenden Grundsätze der Richtlinie gelten uneingeschränkt und unmittelbar, unabhängig von der Erstellung eigener Regelungen.

1.2. Grundsätze

- Alle Mit rbeiter sind verpflichtet, die Informationen zu schützen, damit dem Unterno men durch die unberechtigte Nutzung von Informationen kein Schade entsteht.
- Das Si erheitsmanagement unterstützen Mitarbeiter und Führungskräfte

In der Vorlage erhalten Sie einen Überblick, wie die IT Sicherheitspolitik aussehen kann. Hierzu werden bspw. die Oberpunkte „Sicherheit“, „Informationsschutz“ oder „Anweisungen, Leitlinien, Maßnahmen“ angesprochen.

Inhalt



2.1. Vorgaben

Als „Berechtigte" durfen alle Mitarbeiter des *Musterunternehmens* und externe Partner, die mit der Firma in einer Geschäftsbeziehung stehen, die zur Erfüllung ihrer Aufgaben erforderlichen Informationen erhalten.
Alle Mitarbeiter sind verp[illegible]chtet, durch ihr Verhalten Informationen zu schützen, damit Schaden vom Unternehm[illegible] abgewendet wird.

2.2. Regeln zur Behandl[illegible]ng von Informationen

Alle das *Musterunternehm*[illegible]en sowie dessen Mitarbeiter und Kunden betreffenden Informationen, sind entsp[illegible]echend den nachfolgenden Regeln zu behandeln:

Ausnahme:
Pressemitteilunge[illegible] oder Vorträge und Beiträge in Publikationen. Nur autorisierte Stellen, wie z.B. di[illegible] Marketing-Abteilung und die Geschäftsführung, dürfen die Presse informiere[illegible] Im Zweifel sind Informationen vertraulich zu behandeln.

2.2.1 Festlegung der Sc[illegible]utzklassen bzgl. der Vertraulichkeit

Für alle Informationen un[illegible] Dokumente gelten die folgenden Schutzklassen:

- **„offen (*public*)"**

Keine Kennzeichnung[illegible]pflicht

- **„nur für internen [illegible]Gebrauch (*for internal use only*)"**

Die Informationen[illegible]nd vertraulich und ihre Preisgabe würde zudem die Gefahr

Die Vorlage lässt sich selbstverständlich auf Ihre unternehmensspezifischen Daten und Gegebenheiten anpassen, sodass Sie letzten Endes eine individualisierte Vorlage erhalten.

Inhalt

3. Schutz des Eigentums

Jeder Mitarbeiter ist zum Schutz des Eigentums verpflichtet.

- Zum Eigentum zählen alle Sach- und Vermögenswerte des Unternehmens, das Privateigentum von Mitarbeitern und Besuchern auf Grundstücken und in Gebäuden des Unternehmens. Die Funktionen für Sicherheit unterstützen Führungskräfte und Mitarbeiter durch Beratung, Maßnahmen zur Vorbeugung und Überwachung, im Schadensfall durch Ermittlung und Aufklärung

4. Anweisungen, Leitlinien, Maßnahmen

Alle Policies, Anweisungen und Leitlinien des *Musterunternehmens* finden Sie im Intranet.

Neben den Maßnahmen und Regelungen zum IT-Grundschutz im *Musterunternehmen* werden hier auch Anweisungen für besonders schutzenswerte Informationen sowie nützliche Hilfsmittel für alle Mitarbeiter angegeben.

Das Dokument Informationssicherheitspolitik ist im Intranet hinterlegt und für jeden Mitarbeiter jederzeit einsehbar.

Verbindliche Verfahrens- und Arbeitsanweisungen und die Organisationsstruktur sind ebenfalls im Intranet hinterlegt und für jeden Mitarbeiter jederzeit einsehbar.

Gesetzliche Anforderungen, insbesondere des Bundesdatenschutzgesetzes, behördliche und vertragliche Anforderungen sind von allen Mitarbeitern einzuhalten.

Maßnahmen, die nach Eintritt eines Notfall auslösenden Ereignisses zu ergreifen sind, und alle dazu erforderlichen Informationen sind im Notfallhandbuch dokumentiert.

Das Notfallhandbuch ist im Intranet in elektronischer Form sowie an der Rezeption des Musterunternehmens in schriftlicher Form hinterlegt.

Inhalt

- Maßnahmen zur Wiederherstellung von Informationen und Verfahren.
- Einhaltung der Konformität zum internationalen Standard ISO 27001

7. Verstöße

Als Verstöße gelten beabsichtigte oder grob fahrlässige Handlungen, die

- eine Kompromittierung des Rufes des *Musterunternehmens* darstellen,
- die Sicherheit der Mitarbeiter, Vertragspartner, Berater und des Vermögens des *Musterunternehmens* kompromittieren,
- die Sicherheit von Informationen hinsichtlich deren Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gefährden,
- die dem *Musterunternehmen* tatsächlichen oder potenziellen finanziellen Verlust einbringen - durch die Kompromittierung der Sicherheit von Daten oder Geschäftsinformationen,
- den unberechtigten Zugriff auf Informationen, deren Preisgabe und/oder Änderung beinhalten,
- die Nutzung von Unternehmensinformationen für illegale Zwecke beinhalten.

Die Nichteinhaltung oder bewusste Verletzung der IT-Sicherheitspolitik führt zu einer der nachfolgenden Aktionen, ist aber nicht auf diese beschränkt:

- disziplinarische oder arbeitsrechtliche Folgen,
- straf- und/oder zivilrechtliche Verfahren,
- Haftung und Regressforderungen

8. Ansprechpartner und Organisationsstruktur

IT-Sicherheitsbeauftragter für ISMS, IT Sicherheit, Geräte, Anlagen und Verfahren ist:
Max Mustermann
E Mail: mmustermann@abc.de
Tel. 123 456 781

Inhalt

Stichworterklärungen

Informationen	Daten, die auf Systemen oder Medien, wie z. B. auf Disketten, in der Infrastruktur oder im Rahmen von Geschäftsabläufen gespeichert oder verwaltet werden.
Sicherheit	Schutz von Informationsquellen vor unberechtigten Anderungen, Zerstorungen oder Preisgabe - unabhangig davon, ob sie absichtlich oder unabsichtlich erfolgten.
Vertraulichkeit	Schutz gegen unberechtigte Kenntnisnahme.
Integrität	Vermeidung unberechtigter Anderungen, Erstellung oder Duplizierung von Informationen
Verfügbarkeit	Hohe Betriebsbereitschaft der verwendeten Systeme und hohe Ausfallsicherheit, Verfügbarkeit der erforderlichen Informationen.
Authentizität	Grundsatz, dass der Empfänger zweifelsfrei sicher sein kann, dass eine Information tatsachlich von dem angeblichen Verfasser geschaffen und nicht gefalscht wurde oder anderweitig durch Dritte verändert worden ist
Rechenschafts-pflicht	Grundsatz, dass Einzelpersonen für die Folgen ihrer Handlungen verantwortlich sind, die zu einer Verletzung der Sicherheit führen könnten oder bereits geführt haben.
Verbindlichkeiten	Dieser Grundsatz besagt, dass später nachgewiesen werden kann, dass die an einer Transaktion Beteiligten die Transaktionen tatsächlich autorisiert haben und sie über keinerlei Mittel verfugen, ihre Beteiligung zu bestreiten.

Stichworterklärungen und Hinweise zur Nutzung des Dokuments runden diese Vorlage ab.

VOREST AG
Bausteine Ihres Erfolgs

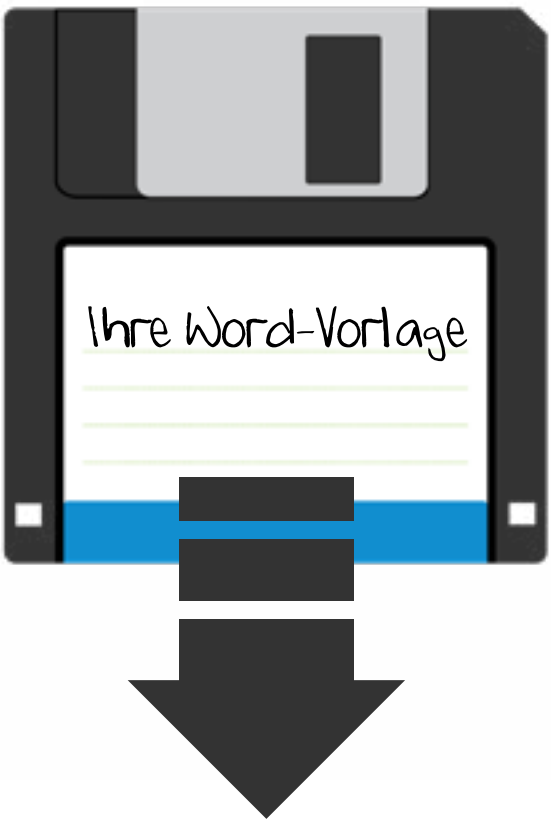
Kostenloser Update-Service

Bei ISO-Revisionsänderungen **binnen 1 Jahres**
nach Kauf dieser Vorlage wird Ihnen
das Dokument inklusive aktueller Normrevision
kostenfrei zur Verfügung gestellt.

VOREST AG
Bausteine Ihres Erfolgs

Sofortdownload

Ihre Vorlage steht Ihnen nach
dem Kauf als Download zur Verfügung.



VOREST AG
Bausteine Ihres Erfolgs

Zufriedenheitsgarantie

Ihre Autoren - mit **Erfahrung für Sie!**

Aus der **Praxis für Ihre Praxis**. Unsere Vorlagen, Checklisten, Formblätter und Schulungsunterlagen stammen alle von **erfahrenen Beratern**, die diese Musterdokumente mit ihrem ganzen **Erfahrungsschatz** für Sie erstellt haben.