Festlegung des Geltungsbereiches

Diese IT-Sicherheitsrichtlinie gilt für die w3 GmbH. Sie erstreckt sich auf alle Standorte der w3 GmbH. Diese Sicherheitsrichtlinie verpflichtet alle Beschäftigten der w3 GmbH zur Einhaltung der hier festgelegten Pflichten. Die Sicherheitsrichtlinie wird den Beschäftigten in der jeweils geltenden Fassung über das „Datenschutz-Wiki“ der w3 GmbH zugänglich gemacht.

Betroffene Arbeitsvorgänge und Fachverfahren

Die w3 GmbH verfügt über eine IT-Infrastruktur, die den Beschäftigten im Zusammenhang mit ihrer Tätigkeit für die w3 GmbH als Arbeitsmittel zur Verfügung steht.

Mit IT-Infrastrukur sind ausnahmslos alle Geräte oder Anwendungen (Hard- und Software) zu verstehen, mit denen Informationen elektronisch verarbeitet oder übertragen werden können. Dazu gehören insbesondere PCs, Notebooks/Laptops, Tablet PCs (z.B. iPad), Telefone, Mobiltelefone, Server, Speichermedien, Netzwerktechnologie, Softwareprodukte und Drucker.

Betroffene Datenkategorien, Schutzbedarf und Schutzziele

Aufgrund gesetzlicher Vorgaben hat die Vertraulichkeit der Kundendaten einen hohen Stellenwert. Unberechtigte Datenzugriffe sollen daher verhindert werden. Virenschutz, eine sichere Internetanbindung sowie eine gute Ausbildung der Mitarbeiter sind daher zu gewährleisten.

Um die Integrität, Verfügbarkeit und Vertraulichkeit der IT-Systeme auf Dauer zu gewährleisten, sind die nachfolgenden IT-Sicherheitsrichtlinien von allen Beschäftigten einzuhalten.

Die w3 GmbH arbeitet zu großen Teilen mit personenbezogenen Daten (Personalisierter Druck, Lettershop, Email-Marketing & Newsletter, Datenbankmanagement u.ä.), auf deren Zugriff und Verwendung besonderes Augenmerk zu richten ist. Die einzelnen Bereiche sind im Zugriff so zu schützen, das ein Datenmissbrauch weitestgehend ausgeschlossen werden kann.

Ziel der Schutzmaßnahmen ist die sichere Annahme, Verarbeitung, Speicherung oder ggfs. Löschung sowie der Schutz vor Missbrauch von personenbezogenen Daten sowie die Ausfallvermeidung der internen IT-Systeme, um den Geschäftsbetrieb aufrecht zu erhalten.

Abzuwehrende IT-Risiken, bestehende Gefahren und mögliche Konsequenzen

Abzuwehrende IT-Risiken können sein:

- Feuer
- Wasser
- Stromausfall
- Ausfall von IT-Systemen

- Angriffe von außen (z.B. Viren, DoS usw.)
- Einbruch und Diebstahl
- Ausfall von IT-Administratoren
- Verlust von Daten durch Löschen oder Hardwaredefekte

Tritt einer dieser Fälle ein, spricht man von einem Notfall.

Genaue Erläuterungen hierzu gibt es unter Notfallplan

Konsequenzen dieser Notfälle sind meist immer der nicht mehr gewährleistete Geschäftsbetrieb, Gefahr für Leib und Leben der Mitarbeiter sowie der Missbrauch von personenbezogenen Daten.

Verhältnis zu anderen Sicherheits- und Benutzerrichtlinien

Die IT-Sicherheitsrichtlinie hat Vorrang vor allen anderen Richtlinien, sofern dadurch das Geschäftsinteresse vertreten wird oder durch zuwiderhandlung personen- oder finanzieller Schaden enstehen könnte.

Die Durchführung der IT-Sicherheit hat immer Vorrang vor dem normalen Tagesgeschäft.

Konkrete Verantwortlichkeiten für die Schutzmaßnahmen

Die Verantwortlichkeit obligt bei den IT-Administratoren, die für Installation, Wartung, Durchführung und Überwachung der Schutzmaßnahmen zuständig sind. Verstöße gegen Schutzmaßnahmen oder grundsätzlich gegen die IT-Sicherheitsrichtlinien sind umgehenden beim DST Das Datenschutzteam der w3 GmbH zu melden.

IT-Administratoren der w3 GmbH:

Ralf Gebhard, Tel: 0751-5607813, Mobil: 0172-9723690, gebhard@w3.de

Frank Hochdorfer, Tel: 0751-5607821, Mobil: 0162-9126323, hochdorfer@w3.de

Übersicht Verantwortlichkeiten w3 GmbH

Zu ergreifende Schutzmaßnahmen

Zugangs- und Zugriffskontrolle

Die Zugangs- und Zugriffsrechte sind vom Administrator einzurichten, zu dokumentieren und vor Manipulationen zu schützen. Der Administrator hat seiner Rolle angepasste Zugangsrechte zu nutzen (Trennung zwischen Administratoren- und Benutzerrechten). (siehe Sicherungsmaßnahmen)

Passwort-Regelungen

Die Passwort-Regeln der IT-Benutzer gelten für den Administrator gleichermaßen. (siehe IT-Richtlinie für Passwort-Gebrauch)

Virenschutz

Zum Schutz vor Schad-Inhalten werden im Unternehmen Virenschutzprogramme eingesetzt. Die Umsetzung des Virenschutzes erfolgt durch die IT-Administration. Der Virenschutz ist immer aktuell zu halten und muss auf allen Geräten mit Internetzugang ausgeführt werden. (siehe IT-Richtlinie für Schadsoftware)

Datensicherung

Daten auf Serversystemen von w3 GmbH werden mindestens täglich inkrementell und wöchentlich „voll“ gesichert. Die Datensicherung wird zusätzlich über Nacht verschlüsselt auf einen physisch getrennten Ort gespiegelt.

Das Einspielen von Backups wird regelmäßig getestet.

Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich ein Brandmelder sowie eine CO2-Löscheinrichtung. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst. (siehe IT-Richtlinie Verfügbarkeit)

Protokollierung

In der IT-Infrastruktur werden verschiedene Informationen protokolliert, um Störungen, Ausfälle und Sicherheitsvorfälle schnell identifizieren und beheben zu können. Dabei werden die einschlägigen datenschutzrechtlichen Bestimmungen eingehalten und die Persönlichkeitsrechte der Mitarbeiter gewahrt. (siehe IT-Richtlinie Protokollierung)

Hinweis auf Schulungsangebote

Die w3 GmbH trägt Sorge dafür, dass die Beschäftigten die erforderlichen Schulungen und Instruktionen/Anweisungen erhalten, die für den jeweiligen Umgang mit den IT-Systemen und/oder Applikationen erforderlich sind.

Konsequenzen bei Nichtbeachtung der Sicherheitsrichtlinie

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

Kontaktdaten von IT-Sicherheitsverantwortlichen und Datenschutzbeauftragten

Das Datenschutzteam der w3 GmbH

Ralf Gebhard

Ralf Gebhard, Tel: 0751-5607813, Mobil: 0172-9723690, gebhard@w3.de

From:
https://datenschutzwiki.w3.de/ - **w3 Datenschutzwiki**

Permanent link:
https://datenschutzwiki.w3.de/datenschutz:it-sicherheitsrichtlinie

Last update: **2026/03/16 13:57**