IT-Richtlinie für Nutzer

Einleitung

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. Die IT-Infrastruktur ist unerlässlich für den Geschäftsbetrieb der w3 GmbH.

Geltungsbereich

Diese IT-Richtlinien gelten für die w3 GmbH. Sie gelten für alle Standorte der w3 GmbH. Diese IT-Richtlinien sind von allen Beschäftigten der w3 GmbH einzuhalten.

Ziele

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

Allgemeine Nutzungsrichtlinien für IT-Systeme

Sofern nachfolgend von IT-Systemen die Rede ist, sind darunter 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.

Die Nutzung der IT-Systeme und Applikationen im Unternehmen ist ausschließlich zu dienstlichen Zwecken und in jeweils erlaubten Umfang zur Aufgabenerledigung zulässig. Abweichungen hiervon bedürfen der Erlaubnis des Arbeitgebers. Es darf nur die Software auf IT-Systemen des Unternehmens installiert werden, die vom Arbeitgeber oder der IT-Abteilung freigegeben worden ist.

Die Benutzung privater Hard-und Software zu dienstlichen Zwecken ohne Genehmigung ist nicht zulässig.

Die Nutzung von IT-Systemen bei der w3 GmbH erfolgt grundsätzlich nur für berufliche Zwecke. Eine private Nutzung von IT-Systemen der w3 GmbH ist grundsätzlich untersagt, sofern diese oder eine andere Unternehmensrichtlinie Ausnahmen hiervon regelt.

Einhaltung von Rechtsvorschriften

Bei der Benutzung der IT-Systeme und Applikationen bei der w3 GmbH sind von den Beschäftigten die

geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie sonstige Rechtsvorschriften und Unternehmensrichtlinien einzuhalten. Sollten Beschäftigte unsicher sein, ob und inwieweit Rechtsvorschriften oder Unternehmensregelungen einzuhalten sind, haben sie sich an ihren Vorgesetzten zur Klärung zu wenden.

Schulung

Das Unternehmen 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.

Generelle Vorgaben zur Minimierung von Risiken

Für die Minimierung der Risiken von Datenverlust und von IT-Notfällen sind die folgenden Vorgaben zu befolgen:

- Die Datenhaltung sowie der Betrieb von geschäftsrelevanten IT-Systemen erfolgt ausschließlich in den in der Richtlinie für Speicherorte festgelegten Speicherorten/-bereichen.
- Bei der Inanspruchnahme von externen Dienstleistern ist die Richtlinie mit „Regelungen für Lieferanten und sonstige Auftragnehmer“ zu befolgen. Eine Inanspruchnahme von externen Dienstleistern, die entweder Daten im Auftrag verarbeiten oder Kenntnis von Daten der w3 GmbH erhalten könnten, ist zwingend mit dem Datenschutz- und Informationssicherheitsteam (DST) abzustimmen.

Vorgaben zur Gestaltung des Arbeitsplatzes

Der Arbeitsplatz ist von den Beschäftigten so zu gestalten, dass Besucher oder sonstige Dritte keinen Zugang zu personenbezogenen Daten bekommen können, ohne hierfür berechtigt zu sein. So sind Büros nach dem Verlassen des Arbeitsplatzes grundsätzlich zu verschließen.

Beim Verlassen des Arbeitsplatz-PCs muss der jeweilige Mitarbeiter sich „abmelden“ bzw. seinen PC „sperren“, so dass vor der erneuten Nutzung des IT-Systems und/oder der Applikation(en) eine Authentifizierung (Benutzername/Passwort) erforderlich wird.

In Bereichen mit Publikumsverkehr sind die IT-Systeme – insbesondere die Bildschirme – so auszurichten, dass das Risiko der Kenntnisnahme durch Besucher oder Dritte nach Möglichkeit ausgeschlossen wird. Insbesondere sind in Meetingräumen die Verbindungen zu den Bildschirmen in den Pausen und am Ende des Meetings zu trennen und der Präsentationsrechner ist zu sperren.

Informationen in Papierform sind so abzulegen, dass Besucher oder sonstige Dritte keine Kenntnisnahme von den Daten erhalten können. Vertrauliche Informationen sind stets unter Verschluss zu halten.

Richtlinien für den Passwort-Gebrauch

Soweit technisch möglich sind alle IT-Systeme und Applikationen erst nach hinreichender Authentifizierung des Nutzers nutzbar. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Benutzername/Passwort. Soweit möglich oder angeordnet, werden Zwei-Faktor-Authentifizierungs-Systeme verwendet. Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist komplex gestalten und muss mindestens 3 der nachfolgenden 4 Kategorien enthalten:

1. Großbuchstaben
2. Kleinbuchstaben
3. Sonderzeichen
4. Ziffern

Soweit technisch möglich ist jeder Mitarbeiter verpflichtet, sein Initial-Passwort unverzüglich zu ändern.

Die Passwörter sind so zu wählen, dass sie nicht durch Dritte leicht zu erraten sind. Vor-und Familiennamen oder Geburtstage sowie Namen von Angehörigen sind nicht zur Passwortwahl geeignet. Gleiches gilt für trivial angeordnete Zahlenkombinationen (z.B. 12345678).

Passwörter sollten regelmäßig, mindestens nach 90 Tagen, gewechselt werden. Bereits genutzte Passwörter dürfen nicht noch einmal wiederverwendet werden. Von diesem Passwortwechsel kann in begründeten Fällen abgewichen werden. Voraussetzung dafür ist, dass die Passwortsicherheit dann in einer dem Stand der Technik entsprechenden anderen Weise gewährleistet werden. Dazu können Methoden der 2-Faktor-Authentifizierung oder erheblich höhere Passwortlängen gehören.

Schutz vor Schad-Inhalten

Zum Schutz vor Schad-Inhalten werden im Unternehmen Virenschutzprogramme eingesetzt. Die Umsetzung des Virenschutzes erfolgt durch die IT-Administration.

Zudem kommen Systeme zum Einsatz, mit denen E-Mails mit unverlangter Werbung gefiltert werden. Entsprechende E-Mails werden in einem gesonderten Ordner abgelegt. Die Beschäftigten sind verpflichtet, diesen Ordner regelmäßig – mindestens 1x täglich – im Hinblick auf falsch eingeordnete E-Mails zu sichten.

Richtlinie zur Nutzung von E-Mail/Internet

Beschäftigte erhalten einen dienstlichen E-Mail Account. Die Nutzung von E-Mail darf nur für dienstliche Zwecke erfolgen. Den Mitarbeitern kann gestattet werden, private E-Mails über ihren eigenen, privaten Webmail-Account zu empfangen und zu senden. Der Umfang dieser Nutzung kann aus betrieblichen Gründen vom Unternehmen eingeschränkt werden.

Verhalten bei Sicherheitsvorfällen

Sollte ein Mitarbeiter merken, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnte, hat dieser sich unverzüglich an das DST und seinen Vorgesetzten zu wenden. Dies gilt insbesondere dann, wenn die Gefährdung sich auf personenbezogene Daten bezieht.

Weisungen

Die Mitarbeiter sind verpflichtet, den Weisungen der IT-Abteilung in Bezug auf den Umgang mit IT-Systemen Folge zu leisten. Sofern Zweifel an der Richtigkeit oder der Sinnhaftigkeit von Weisungen bestehen, kann der IT-Verantwortliche eingebunden werden.

Definition Notfall und Notfallplan

Ein Notfall kann den Geschäftsbetrieb nachhaltig gefährden. Falls es zu Notfällen kommt, die die Funktionsfähigkeit der IT-Systeme beeinträchtigen, kommt ein Notfallplan zur Anwendung. Im Notfallplan ist eine Notfalldefinition, eine Angabe der Verantwortlichen, die Benachrichtigungen sowie die Notfallmaßnahmen definiert. Im Falle eines Notfalls gelten die Richtlinien des Notfallplans mit dem Zweck, den Geschäftsbetrieb aufrechtzuerhalten bzw. unverzüglich wieder einen Zustand einer funktionsfähigen IT-Infrastruktur herzustellen. Der Notfallplan ist in einem separaten Dokument geregelt und beschreibt diese Punkte.

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.

Während des Regelbetriebs der IT-Infrastruktur werden von verschiedenen Systemen (insbesondere von Servern und Firewalls) Verbindungsdaten (Datum, Uhrzeit, Adressen von Absender und Empfänger, die Art der übertragenen Daten, das übertragene Datenvolumen usw.) protokolliert.

Im Zuge der der Nutzung der IT-Infrastruktur werden Daten protokolliert, aus denen auch das Nutzerverhalten ganz oder in Teilen nachvollzogen werden kann (Zeitpunkt der An- und Abmeldung an IT-Systemen, Datum und Uhrzeit von Änderungen in Dateien, usw.).

Um gesetzliche Anforderungen zu erfüllen, archiviert das Unternehmen alle ein- und ausgehenden E-Mails mindestens für die Dauer gesetzlicher Aufbewahrungspflichten. Diese können bis zu zehn Jahre betragen.

Das Erheben dieser Protokolldaten ist für den sicheren und rechtskonformen Betrieb der IT-Infrastruktur notwendig. Die Protokolldaten werden ausschließlich zu folgenden Zwecken verwendet: • Analyse und Korrektur von Störungen, Ausfällen und Sicherheitsvorfällen • Gewährleistung der

Sicherheit der IT-Infrastruktur • Optimierung der IT-Infrastruktur • für Statistiken über die Nutzung der IT-Infrastruktur sowie für • nicht personenbezogene Stichprobenkontrollen sowie Auswertungen gemäß dieser Richtlinie (siehe Abschnitt „Missbrauchskontrolle“) • Die Protokolldaten werden nicht zur Leistungs- und Verhaltenskontrolle der Mitarbeiter eingesetzt.

Missbrauchskontrolle

Für das Erkennen von Störungen, Ausfälle und Sicherheitsvorfällen findet eine nicht-personenbezogene Auswertung der Protokolldaten durch einen gesondert beauftragten Mitarbeiter statt. Eine personenbezogene Auswertung der Protokolldaten findet nur statt, wenn aufgrund einer Stichprobenkontrolle, einer Meldung oder anderer Verdachtsmomente ein konkreter Verdacht auf eine missbräuchliche, unerlaubte oder strafbare Nutzung der IT-Infrastruktur besteht.

In diesem Falle ist folgende Vorgehensweise verbindlich:

- Eine personenbezogene Überprüfung der Protokolldaten erfolgt nur bei einem gewichtigen Missbrauchsverdacht, Bagatellfälle rechtfertigen die Überprüfung nicht.
- Sie wird nach dem Prinzip der Datensparsamkeit durchgeführt.
- Sie erfolgt unter zwingender Beteiligung des Datenschutzbeauftragten.
- Wird der Verdacht durch die Überprüfung nicht bestätigt, so werden die für die Überprüfung erhobenen Daten und Aufzeichnungen unverzüglich gelöscht. Der nicht bestätigte Verdacht darf keinerlei weitere Folgemaßnahmen – insbesondere keine gezielten Stichproben gegen den Mitarbeiter – nach sich ziehen.
- Bei Gefahr im Verzug werden durch die W3 GmbH weitere gefährdende oder strafbare Handlungen – eventuell unter Einschaltung der Strafverfolgungsbehörden – unmittelbar unterbunden, insbesondere werden die erforderlichen technischen Abwehrmaßnahmen ohne Verzögerung ergriffen, auch wenn hierbei personenbezogene Daten erhoben oder eingesehen werden müssen. Das DST wird schnellstmöglich über die Vorgänge informiert.

Sanktionen

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