IT-NUTZUNG

RICHTLINIE

Version 1.0 • 08/2023

Richtlinie IT-Nutzung

Warum diese Richtlinie

Unser Unternehmen verfügt über eine IT-Infrastruktur, die unseren Mitarbeitenden als Arbeitsmittel zur Verfügung steht. Diese IT-Infrastruktur ist wichtig für unseren Geschäftsbetrieb.

Geltungsbereich

Für alle Mitarbeiterinnen und Mitarbeiter, die mit unserer IT-Infrastruktur arbeiten oder unser IT-Netzwerk angeschlossen sind oder auf Daten unseres Unternehmens zugreifen oder diese verarbeiten, gilt diese Richtlinie ausnahmslos.

Ziele

Die Einhaltung dieser Richtlinie gewährleistet dauerhaft die Integrität, Verfügbarkeit und Vertraulichkeit der IT-Systeme.

Allgemeine Nutzungsrichtlinien für IT-Systeme

Wenn im Folgenden von IT-Systemen die Rede ist, so sind damit ausnahmslos alle Geräte oder Anwendungen (Hard- und Software) gemeint, mit denen Informationen auf elektronischem Wege verarbeitet oder übertragen werden können. Hierzu zählen insbesondere PCs, Notebooks, Tablet-PC (z. B. iPad), Telefone, Mobiltelefone, Server, Speichermedien, Netzwerktechnik, Softwareprodukte und Drucker.

RICHTLINIE

Die Nutzung der IT-Systeme und -Anwendungen im Unternehmen ist ausschließlich für dienstliche Zwecke und in dem jeweils genehmigten Umfang zur Erfüllung der zu erledigenden Aufgaben zulässig. Eine private Nutzung der Systeme ist verboten. Ausnahmen sind nur mit Genehmigung des Vorgesetzten gestattet. Es darf nur vom Arbeitgeber bzw. der IT-Abteilung freigegebene Software auf den IT-Systemen des Unternehmens installiert werden.

Ohne Genehmigung ist es nicht gestattet, private Hard- und Software für dienstliche Zwecke zu nutzen.

Einhaltung von Rechtsvorschriften

Die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie sonstige Rechtsvorschriften und Unternehmensrichtlinien sind von allen Beschäftigten, die mit unseren IT-Systemen arbeiten, einzuhalten. Mitarbeitende, die unsicher sind, welche Vorschriften gelten, wenden sich an ihren Vorgesetzten.

Schulung

Das Unternehmen schult die Beschäftigten für den Umgang mit den jeweiligen IT-Systemen und/oder Applikationen sowie hinsichtlich Datenschutz und Datensicherheit.

Generelle Vorgaben zur Minimierung von Risiken

Folgenden Vorgaben sind einzuhalten, um Datenverluste und IT-Notfälle zu minimieren:

- Eine Speicherung von Daten erfolgt ausschließlich in den in der ”Richtlinie für Speicherorte” festgelegten Speicherorten bzw. -bereichen.
- Die Richtlinie „Regelungen für Lieferanten und sonstige Auftragnehmer“ ist bei der Beauftragung externer Dienstleister zu beachten. Der Einsatz externer Dienstleister, die Daten im Auftrag verarbeiten oder Kenntnis von unseren Geschäftsdaten erlangen können, ist zwingend mit der Geschäftsführung bzw. mit dem Datenschutzbeauftragten abzustimmen.

Vorgaben zur Gestaltung des Arbeitsplatzes

Bildschirme sind so auszurichten, dass Besucher oder Dritte nach Möglichkeit keinen Zugang zu (personenbezogenen) Daten bekommen können.

Büros müssen auch beim kurzfristigen Verlassen grundsätzlich abgeschlossen werden. Zusätzlich müssen Beschäftigte sich beim Verlassen des Arbeitsplatzes von ihrem PC abmelden. Eine erneute Nutzung des IT-Systems muss eine neue Authentifizierung (Benutzername/Passwort) erfordern.

In Konferenzräumen ist die Verbindungen zu den Bildschirmen in den Pausen und am Ende des Meetings zu trennen und der Präsentationsrechner muss gesperrt werden. Weiterhin ist darauf zu achten, dass Besucher beim Wechseln von Inhalten keinen Einblick in die Dateistruktur auf dem Rechner bekommen.

Unterlagen in Papierform müssen so abgelegt werden, dass Dritte sie nicht einsehen können. Vertrauliche Informationen müssen unter Verschluss gehalten werden.

Passwörter

Der Zugang zu unseren IT-Systemen und -Anwendungen ist geschützt. Erst nach einer Authentifizierung mittels Benutzernamen und Passwort ist der Zugang möglich.

Eine Zwei-Faktor-Authentifizierung (2FAS) kann für zusätzlichen Schutz sorgen.

Alle weiteren Vorschriften für Passwörter regelt die Richtlinie Passwörter.

Schutz vor Malware

Wir schützen unsere IT-Systeme mit Virenschutzprogrammen vor Malware. Die Einrichtung des Virenschutzes wird von der IT-Administration vorgenommen. Die Systemeinstellungen des Virenschutzes darf vom Anwender nicht verändert werden.

Sollten Mitarbeitende das Gefühl haben, der Virenschutz wäre nicht aktiv oder falsch konfiguriert, müssen sie sich an den IT-Verantwortlichen wenden.

Verhalten bei Sicherheitsvorfällen

Nehmen Beschäftigte an oder stellen sie fest, dass der Datenschutz oder die Sicherheit von Daten gefährdet sein könnte, müssen sie sich **UNVERZÜGLICH** an ihren Vorgesetzten oder die IT-Abteilung wenden. Sind personenbezogene Daten gefährdet, hat die Meldung SOFORT (sogar am Wochenende oder im Urlaub) zu erfolgen.

Störungen & Ausfälle

Eine **Störung** ist eine Situation, in der Prozesse oder Ressourcen unserer IT-Systeme nicht wie vorgesehen funktionieren und die dadurch entstehenden Schäden als *gering* einzustufen sind. Die Beseitigung einer Störung kann im allgemeinen Tagesgeschäft von einem IT-Fachmann vorgenommen werden.

Ein **Ausfall** liegt vor, wenn ein Teil oder Teile der IT-Infrastruktur ihre Funktionsfähigkeit verloren haben.

Meldung

Störungen und Ausfälle beeinträchtigen die Funktionsfähigkeit unserer IT und verursachen in der Regel Kosten. Zu spät oder nicht gemeldete Problem können zu weiteren Schäden und höheren Kosten führen. Dies ist zu vermeiden.

Demzufolge müssen Störungen und Ausfälle umgehend gemeldet werden, damit sie schnellstmöglich behoben werden können.

Die Meldung erfolgt in der Regel an einen Administrator oder an den Vorgesetzten, der die Meldung entsprechend weiterleiten wird.

Wird ein Ausfall als gravierend eingestuft, benachrichtigt der Mitarbeiter parallel die Unternehmensleitung. Ein Ausfall ist gravierend, wenn entweder

- eine Verletzung von Leib oder Leben von Menschen;
- eine Störung der Finanzbuchhaltung;
- ein Störung der Auftragsbearbeitung droht oder besteht.

- Oder es besteht ein Verstoß gegen Gesetze, Verträge oder Normen und es sind Haftungsrisiken entstanden, die für das Unternehmen oder für einzelne Verantwortliche beträchtlich sind, insbesondere mögliche Verstöße im Bereich des Datenschutzes.

Notfall

Eine Notfallsituation tritt immer dann ein, wenn ein Vorfall die Geschäftstätigkeit nachhaltig beeinträchtigen kann. In einem solchen Fall kommt ein Notfallplan zum Einsatz. Neben anderen Notallplänen ist in Zusammenhang mit dieser Richtlinie der ”Notfallplan IT” relevant.

Dieser legt die Definition eines Notfalls, die Angabe der Verantwortlichen, die Benachrichtigungen sowie die Maßnahmen, nach denen zu handeln ist, fest.

Tritt ein Notfall ein, gelten die Vorgaben der Notfallpläne mit dem Ziel der Aufrechterhaltung des Geschäftsbetriebes oder der raschen Wiederherstellung eines funktionsfähigen Zustandes der IT-Infrastruktur.

Die Notfallpläne und die Richtlinien für den Notfall sind verbindlich einzuhalten

Protokollierung

Damit Störungen, Ausfälle und Sicherheitsvorfälle schnell identifizieren und beheben werden können, werden verschiedene Informationen von den Servern und der IT-Abteilung protokolliert.

Alle relevanten datenschutzrechtlichen Bestimmungen werden eingehalten. Die Persönlichkeitsrechte der Beschäftigten bleiben gewahrt.

Folgende Daten werden u. a. protokolliert:

- **Verbindungsdaten von Servern und Firewalls**
  (Datum, Uhrzeit, Adressen von Absender und Empfänger, die Art der übertragenen Daten, das übertragene Datenvolumen usw.)

- **Protokolldaten vom Anwendungen**
  (Zeitpunkt der An- und Abmeldung an IT-Systemen, Datum und Uhrzeit von Änderungen in Dateien, usw.).
  Aus diesen Daten kann auch das Nutzerverhalte rekonstruiert werden.

- Im Rahmen der gesetzlichen Aufbewahrungsfristen werden alle ein- und ausgehenden E-Mails mindestens für diese Dauer (bis zu zehn Jahren) gespeichert.

Das Erheben dieser Protokolldaten ist für den sicheren und rechtskonformen Betrieb der IT-Infrastruktur notwendig. Für die nicht-personenbezogene Auswertung der Protokolldaten ist ein Mitarbeiter verantwortlich, der in den Belangen des Datenschutzen ausgebildet ist.

Die Daten werden ausschließlich zu folgenden Zwecken verwendet:

- Dokumentation und Analyse von Störungen, Ausfällen und Sicherheitsvorfällen;
- Gewährleistung der Sicherheit,
- Optimierung und für
- Statistiken über die Nutzung der IT-Infrastruktur;
- für nicht personenbezogene Stichprobenkontrollen;
- für Auswertungen der Missbrauchskontrolle

- Die Protokolldaten werden nicht zur Leistungs- und Verhaltenskontrolle der Mitarbeiter eingesetzt.

Missbrauchskontrolle

Sollten sich aus den Stichprobenkontrollen Hinweise auf eine missbräuchliche, unerlaubte oder strafbare Nutzung der IT-Infrastruktur durch einen Mitarbeiter ergeben, findet eine personenbezogene Auswertung der Protokolldaten statt. Gleiches gilt, wenn sich ein konkreter Verdacht aufgrund einer Meldung oder anderer Verdachtsmomente ergibt.

Die verbindliche Vorgehensweise für eine personenbezogene Auswertung der Protokolldaten sieht vor, dass

- eine personenbezogene Überprüfung der Protokolldaten nur bei einem schwerwiegendem Missbrauchsverdacht durchgeführt wird.
- die Überprüfung nach dem Grundsatz der Datensparsamkeit und
- unter Beteiligung eines Datenschutzbeauftragten durchgeführt wird.
- Bestätigt sich der Verdacht, werden umgehend weitere Aktivitäten des betroffenen Mitarbeiters durch Einleitung der erforderlichen technischen Abwehrmaßnahmen unterbunden. Dabei kann es notwendig sein, dass der Schutz personenbezogener Daten eingeschränkt oder aufgehoben wird. Der hinzugezogene Datenschutzbeauftragte wird schnellstmöglich über die Vorgänge informiert.
- Verläuft die Überprüfung mit einem negativen Ergebnis, werden die für die Überprüfung erhobenen Daten und Auf-

zeichnungen unverzüglich gelöscht. Der nicht bestätigte Verdacht hat keinerlei negative Folgen für den Mitarbeiter.

Sanktionen

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

RICHTLINIE