**Vorlage: Weisung zur Nutzung der IT-Infrastruktur**

Diese Vorlage bietet eine Grundlage für Ihre Weisung zur Nutzung der IT-Infrastruktur. Sie finden hier diejenigen Punkte, die üblicherweise in einer solchen Weisung festgehalten werden – sofern sie nicht in den Einzelarbeitsverträgen geregelt sind.

**Weisungen zur Nutzung der IT-Infrastruktur**

der

## Geltungsbereich und Nutzungsgrundsatz

Diese Weisungen gelten für alle Mitarbeitenden der und für alle Benutzenden der IT-Infrastruktur der (wie Server, Internet, E-Mail, Kopierer), ebenso für Dritte (zum Beispiel externe Vertragspartner). Sie sind strikte einzuhalten.

## Zugang zu Internet und E-Mail

Jeder Benutzer / jede Benutzerin erhält einen persönlichen Netzwerkaccount, der ihm / ihr auch Zugang zum Internet ermöglicht. Auf den Internetzugang haben die Benutzenden keinen Anspruch; er kann jederzeit von entzogen werden. Zudem kann jederzeit den Zugang zu bestimmten Websites sperren.

Möglicher Zusatz
Der Zugang zum Server der Arbeitgeberin erfolgt über eine Zwei-Faktor-Authentifizierung: Benutzername, Passwort und Code per SMS. Die Mitarbeitenden haben ein Passwort zu wählen, das aus mindestens acht Zeichen besteht, darunter mindestens ein Grossbuchstabe, eine Zahl und ein Sonderzeichen.

## Nutzung der IT-Infrastruktur

Die IT-Infrastruktur ist grundsätzlich nur für geschäftliche Zwecke bestimmt, das heisst zur Erfüllung der zugewiesenen Aufgaben. Ausnahmsweise und in kleinem Rahmen sind private Nutzungen zulässig; sie sind jedoch auf ein Minimum zu beschränken und haben wenn möglich ausserhalb der Arbeitszeit stattzufinden.

Jeder Mitarbeiter / jede Mitarbeiterin ist dafür verantwortlich, dass an seinem / ihrem Arbeitsplatz keine Dokumente oder Datenträger mit sensiblen Daten unbeaufsichtigt sind. Jeder Benutzer / jede Benutzerin ist dafür verantwortlich, dass seine / ihre Benutzerkennung sowie die dazugehörenden Passwörter unberechtigten Dritten nicht zugänglich sind und diesen nicht weitergegeben werden. Der Arbeitscomputer darf nie ungesperrt verlassen werden (Sperrung des Bildschirms mit: Ctrl + Alt + Del).

Mögliche Ergänzung
Jeder Benutzer / jede Benutzerin kontrolliert seinen / ihren E-Mail-Briefkasten mehrmals täglich. Ist
er / sie länger abwesend, ist eine Abwesenheitsmeldung einzurichten. Eine automatische Umleitung eingehender Nachrichten an eine private E-Mail-Adresse ist aus datenschutzrechtlichen Gründen untersagt. Vertrauliche Informationen und personenbezogene Daten müssen verschlüsselt versendet werden (inklusive Anhänge).

## Untersagte Nutzung der IT-Infrastruktur

Bei der Benutzung der IT-Infrastruktur haben die Benutzenden die Interessen von zu berücksichtigen und alle Risiken auszuschliessen, die diese gefährden könnten. Untersagt sind deshalb: Surfen auf rechtswidrigen Websites, auf Websites mit rassistischen, pornografischen oder sexistischen, widerrechtlichen, urheberrechtsverletzenden, beleidigenden Inhalten das Verbreiten und das Speichern solcher Websites. Ebenso untersagt sind persönliche Finanztransaktionen (wie E-Banking, Börsengeschäfte) und das Nutzen von Chat-Rooms und interaktiven Multimediainstallationen.

Mitarbeitende dürfen keine Kopien von schriftlichen Unterlagen, Datenträgern, Lizenzprogrammen und eigenen Programmen für den privaten Gebrauch erstellen.

Ebenso sind das Herunterladen, das Installieren und das Versenden jeglicher Programme und Software untersagt.

Möglicher Zusatz
 kann in eigenem Ermessen Ausnahmen bewilligen; diesbezügliche Gesuche sind an zu richten.

Möglicher Zusatz
Externe Daten oder Dateien (inklusive E-Mail-Anhänge) dürfen nur heruntergeladen und/oder geöffnet werden, wenn sie:

* geschäftsrelevant sind und bei ihrer Verwendung und Beschaffung alle Anforderungen der sowie alle gesetzlichen Bestimmungen beachtet werden;
* von der Firewall bzw. dem auf dem Computer installierten Virenscanner nicht als sicherheitskritisch gemeldet werden.

Externe Datenträger dürfen nur verwendet werden, wenn sie vorgängig von der IT-Abteilung [oder: Vor- und Nachname des / der IT-Verantwortlichen] geprüft und auf Viren gescannt wurden.

Private Hard- und/oder Software darf im Unternehmensnetz nicht installiert werden. [Oder: Private Hard- und/oder Software darf im Unternehmensnetz nur mit vorgängiger Bewilligung von [Firmenname] installiert werden. Der Benutzer / die Benutzerin hat dafür ein Gesuch an [Vor- und Nachname der / des IT-Verantwortlichen] zu richten. Ein Anspruch auf Genehmigung des Gesuchs besteht nicht.]

## Sicherheitsrelevante Ereignisse

Stellt der Benutzer / die Benutzerin ein sicherheitsrelevantes Ereignis fest – etwa den Verlust oder die Veränderung von Daten oder Programmen, die Verfügbarkeit nicht freigegebener Dienste oder Websites) – oder hat er / sie den Verdacht, dass die eigene Benutzerkennung missbraucht wird, hat er / sie dies sofort zu melden.

Versuche, die Ursachen dafür selbst abzuklären, sind zu unterlassen.

## Kontrollen und Protokollierung

Die behält sich vor, die Einhaltung der Nutzungsregelung stichprobenweise und anonym zu überprüfen. Kommt ein begründeter Verdacht auf, dass einzelne Benutzende gegen die Nutzungsbestimmungen verstossen, kann eine personenbezogene Überprüfung anordnen.

Möglicher Zusatz
Das Betriebssystem der erstellt automatische Zugriffsprotokolle, die während Monaten [zum Beispiel: sechs] aufbewahrt werden. Dabei werden die geltenden Datenschutzbestimmungen beachtet, die Privatsphäre der Benutzenden wird im Rahmen der Gesetze gewahrt. Die erhobenen Daten dienen ausschliesslich dazu, einen ordnungsgemässen Betrieb sicherzustellen, den Datenschutz zu kontrollieren, die IT-Infrastruktur zu unterhalten sowie zur Datensicherung. Sie werden nicht zur Verhaltens- oder Leistungskontrolle verwendet.

## Sanktionen

Verursacht der Benutzer / die Benutzerin absichtlich oder grobfahrlässig Schäden, kann er / sie dafür haftbar gemacht werden. Liegt ein Verstoss gegen die Bestimmungen dieser Weisung oder eine missbräuchliche Nutzung der IT-Infrastruktur vor, können Mitarbeitende verwarnt oder in schweren Fällen auch fristlos entlassen werden. Zudem hat der Benutzer / die Benutzerin in solchen Fällen mit weiteren disziplinarischen und/oder strafrechtlichen Konsequenzen zu rechnen.

## Inkrafttreten

Diese Weisungen treten per in Kraft. Sie ersetzen diejenigen vom genauso wie alle früheren Weisungen, Merkblätter und Reglemente, die diesen Weisungen widersprechen.

Zusammen mit dem Zugang zur IT-Infrastruktur erhält jeder Benutzer / jede Benutzerin diese Weisung und bestätigt mit seiner / ihrer Unterschrift, dass er / sie diese zur Kenntnis genommen hat und sich verpflichtet, sich daran zu halten.

 [Wenn nötig, Zweitunterschrift]

[Rechtsgültige Unterschrift] [Rechtsgültige Unterschrift]
 [Vor- und Nachname, Funktion]

Lassen Sie eine Kopie dieser Weisung vom Mitarbeiter / von der Mitarbeiterin unterschreiben, wenn Sie sie nicht im Arbeitsvertrag als integrierenden Bestandteil aufführen sowie wenn Sie sie später ändern. So ist sie sicher gültig (mehr dazu im Lexikon unter «[Personalreglement](https://www.gryps.ch/kmu-lexikon/personalreglement/?source=attachment)»).

**Empfangsbestätigung**

Unterschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ort / Datum: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_