

## Benutzungsreglement Informatikmittel

### Geltungsbereich

1. Sämtliche Anwender der durch Vebego AG zur Verfügung gestellten IT-Infrastruktur (Hardware, Software und Services). Sämtliche durch die Nutzung der IT-Infrastruktur generierte und zugegriffene Daten.

### Gesetzliche Grundlagen

2. Beim Einsatz der Informatikmittel sind die Sicherheitsrichtlinien des Datenschutzes gemäss „Bundesgesetz über Datenschutz“ (DSG) zu beachten.

### Installation und Konfiguration der Informatikmittel

- 3.1 Die Informatikmittel werden durch die Abteilung IT nach deren Richtlinien und Standards eingerichtet und gewartet.
- 3.2 Die Installation von privater Hard- und/oder Software ist untersagt.

### Berufliche Nutzung der Informatikmittel

- 4.1 Alle Informatikgeräte (z.B. PCs, Laptops, Mobilfunkgerät etc.) und Anwendungen sind ausschliesslich für betriebliche Zwecke, d.h. zur Erfüllung der zugewiesenen innerbetrieblichen Aufgaben einzusetzen.
- 4.2 Insb. gilt, dass die Benutzung des von Vebego AG den Mitarbeitenden zur Verfügung gestellten Mobilfunkgerät wie auch dessen Abo ausschliesslich zu betrieblichen Zwecken dient. Der Mitarbeiter ist ausdrücklich damit einverstanden, dass ihm/ihr Gesprächsgebühren, die CHF 100.- pro Monat übersteigen, ohne Rücksprache vom Lohn abgezogen werden. Sollten Gebühren von mehr als CHF 100.- pro Monat geschäftlich begründet sein, wird ein Gebührenauszug verlangt und die Abweichungen werden mit den Mitarbeitenden persönlich besprochen. MitarbeiterInnen, die im grenznahen Gebiet zu unseren Nachbarstaaten arbeiten, haben den Netzwahlmodus ihres Handys auf manuell zu schalten. Damit wird verhindert, dass über einen ausländischen Provider telefoniert wird und dadurch unnötig hohe Roaming-Gebühren entstehen.
- 4.3 Mitarbeitenden, welchen ein Tablet ausgehändigt wird, erklären sich damit einverstanden, dass ihnen bei Beschädigung oder Verlust des Geräts folgende Kosten vom Lohn abgezogen werden:
  - a) Im ersten Jahr (bis 12 Monate ab Datum Inbetriebnahme des Geräts): CHF 200 (2/3 Gerätepreis)
  - b) Im zweiten Jahr (bis 24 Monate ab Datum Inbetriebnahme des Geräts): CHF 150 (1/2 Gerätepreis)
- 4.4 Die Geräte sind generell mit der gebotenen Sorgfalt zu behandeln.
- 4.5 Vorgesetzte ab Stufe Betriebsleiter können den Gebrauch von Informatikgeräten ausserhalb des Arbeitsplatzes bewilligen, wenn eine dienstliche Notwendigkeit vorliegt. Sie tragen die Verantwortung für die vollständige und korrekte Instruktion der Mitarbeitenden.

### Vorgehen zur Nutzung der Informatikmittel

- 5.1 Die Mitarbeitenden erhalten mit der erstmaligen Nutzung von Informatikmitteln dieses Reglement und bestätigen dessen inhaltliche Kenntnisnahme und Befolgung mit ihrer Unterschrift.
- 5.2 Für jeden Mitarbeitenden wird in der Folge ein persönlicher Login für den Zugang zum Netzwerk sowie für E-Mails und (bei Bedarf) Internet erstellt.

### Umgang mit Benutzerkennung und Passwörter

- 6.1 Die Mitarbeitenden sind dafür verantwortlich, dass Dritte keinen Zugriff auf die durch die Informatikmittel vermittelten Daten und Informationen haben; sie gewährleisten dies durch konsequenten Einsatz von geeigneten Zugangskontrolleinrichtungen und -massnahmen (z.B. Passwort, Passwortwahl, -aufbau und -verwahrung usw.).
- 6.2 Persönliche Benutzerkennungen und dazugehörige Passwörter dürfen nicht an Dritte weitergegeben werden.

### **Internet**

- 7.1 Alle am Firmennetzwerk angeschlossenen Geräte haben ausschliesslich den zentral angebotenen Internetzugang zu verwenden.
- 7.2 Es besteht kein Rechtsanspruch auf den Zugang zum Internet. Die Geschäftsleitung behält sich das Recht vor, Informationen/Publicationen mit ungeeignetem Inhalt (bspw. pornografisch, rassendiskriminierend, unethisch, unmoralisch) oder mit erkennbaren Risiken für die Firma (Virengefahr) zu sperren oder zu filtern.

### **E-Mails**

- 8.1 Die automatische Umleitung von E-Mails an E-Mail-Adressen ausserhalb der Firma (z.B. die eigene private Mailbox) ist nicht erlaubt. In berechtigten Fällen wird ein alternativer Zugang eingerichtet.
- 8.2 Besonders schützenswerte, wie personenbezogene Informationen dürfen nicht unverschlüsselt via E-Mail nach Extern versendet werden. Dies gilt nicht nur für den Inhalt von E-Mails, sondern auch für beigefügte Dokumente/Anlagen (Attachments).

### **Fernzugriff**

- 9.1 Fernzugriff ist der Zugang auf das Firmennetzwerk oder an dessen angeschlossene Geräte, wenn dieser ausserhalb von Räumlichkeiten der VebeGo AG erfolgt.
- 9.2 Es werden nur die von der IT-Abteilung bezeichneten Geräte unterstützt.
- 9.3 Software, welche den Zugriff auf das Firmennetzwerk ermöglicht, darf nur durch die IT-Abteilung installiert werden.

### **Unangemessene und private Benutzung**

- 10.1 Die Benutzung der Rechner, des Internets und von E-Mail muss unter Berücksichtigung der Interessen von VebeGo AG erfolgen, wobei insbesondere rechtliche und operationelle Risiken auszuschliessen sind.
- 10.2 Es ist insbesondere verboten, auf Material mit widerrechtlichem, urheberrechts- verletzendem, rassistischem, beleidigendem, pornografischem oder herabwürdigendem Inhalt zuzugreifen oder solches zu verbreiten.
- 10.3 Die private Nutzung der Office-Anwendungen, des Internets und von E-Mail ist erlaubt, sofern die beanspruchten Ressourcen (Arbeitszeit, Netzwerkkapazität, Speicherplatz) vernachlässigbar sind. Die private Nutzung darf die Erfüllung zugewiesener Aufgaben nicht beeinträchtigen und ist auf das absolut Notwendige zu beschränken.
- 10.4 Private Daten (inkl. private E-Mails) sind in einem gesonderten Ordner abzulegen, der mit "Privat" oder "Persönlich" kenntlich gemacht wird.
- 10.5 VebeGo AG behält sich vor, bei unsachgemäsem Gebrauch, technische Einschränkungen vorzunehmen oder einzelne Benutzerkennungen zu sperren.

### **Herunterladen (Download) oder Kopieren von Informationen**

- 11.1 Den Mitarbeitenden ist es untersagt, Softwareprogramme aus dem Internet bzw. E-Mail oder von anderen Datenträgern zu kopieren bzw. herunterzuladen und dann zu installieren oder zu verteilen.
- 11.2. Andere Daten (einschliesslich solcher mit Multimediainhalten) dürfen nur unter den folgenden Bedingungen auf das Netzwerk der Verwaltung heruntergeladen werden:
  - a) Die Daten müssen betrieblich relevant sein und es dürfen die speziellen Bestimmungen über die private Nutzung (vorstehend, Ziff. 10.1-4) nicht verletzt werden;
  - b) Die Daten müssen unter Einhaltung aller Anforderungen von VebeGo AG sowie den gesetzlichen Bestimmungen beschafft oder verwendet werden;
  - c) Die Daten dürfen durch den auf allen Computern von VebeGo AG installierten Virenschanner nicht als sicherheitskritisch gemeldet werden.

### **Newsletter**

- 12 Newsletter-Dienste sind bei Austritt zu kündigen.

### **Sicherheitsrelevante Ereignisse**

- 13 Alle sicherheitsrelevanten Ereignisse (z. B. Verlust eines Gerätes, unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste, Verdacht auf Missbrauch der eigenen Benutzererkennung usw.) sind unverzüglich dem Helpdesk IT zu melden. *Beachte:* Ausser bei einem Geräteverlust unternehmen Sie keinesfalls eigene Aufklärungsversuche, weil dabei allenfalls wertvolle Hinweise und Spuren verwischt werden oder verloren gehen können.

### **Kontrollen und Protokollierung**

- 14.1 Die Protokolldaten dienen ausschliesslich der Datensicherung und zur Sicherstellung eines ordnungsgemässen Betriebes, zu Zwecken der Datenschutzkontrolle und der IT-Revision. Sie werden nicht für Zwecke einer präventiven Verhaltens- oder Leistungsbewertung verwendet.
- 14.2 Die Protokollierung erfolgt im Rahmen der Vorgaben des Bundesgesetzes über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1), den Schutz der Privatsphäre im Rahmen der anwendbaren gesetzlichen Bestimmungen und weitere Bestimmungen zur Aufbewahrung von Dokumenten.
- 14.3 Um die Sicherheitsanforderungen von Vebego AG zu gewährleisten, prüft der Helpdesk IT periodisch eine summarische Auswertung (ohne Rückschluss auf bestimmte Personen) der Benutzung der Systeme, Anwendungen, Netzwerke, E-Mail, Fernzugriff und Internet sowie die auf den Servern abgelegten Datenbestände. Ergibt sich aus der Überprüfung ein Verdacht auf Verstoss gegen dieses Reglement, bleiben angemessene personenbezogene Prüfungen vorbehalten. Eine präventive personenbezogene Kontrolle ist nicht erlaubt.
- 14.4 Grundsätzlich werden die Mitarbeitenden im Voraus darüber informiert, wenn eine personenbezogene Prüfung vorgenommen wird. Auf die Vorankündigung kann verzichtet werden, wenn
- a) die Datensicherheit, insbesondere die Verfügbarkeit des Systems nicht mehr garantiert werden kann oder
  - b) Anhaltspunkte für ein rechtswidriges, insbesondere strafbares Handeln vorliegen.
- 14.5 Wird aufgrund der personenbezogenen Prüfung ein Missbrauch festgestellt, wird die zuständige Dienststelle bzw. die Strafverfolgungsbehörde informiert.
- 14.6 Die vorgesetzte Person darf die geschäftlichen Daten überprüfen, soweit dies für seine/ihre Aufsichtstätigkeit notwendig ist. Besondere Geheimhaltungsbestimmungen bleiben vorbehalten.

### **Inkrafttreten**

- 15.1 Dieses Reglement wurde von der Geschäftsleitung am 1. Januar 2004 in Kraft gesetzt und am 17.05.2019 überarbeitet.
- 15.2 Das vorliegende Benutzungsreglement Informatikmittel ist von allen Mitarbeitenden, welche Informatikmittel einsetzen, zu unterschreiben. Die letzte Seite (Seite 3) mit der Bestätigung wird doppelt abgegeben, das Exemplar mit der Unterschrift wird im Personaldossier abgelegt.