

Weisung über

- die Nutzung und Überwachung des Internet- und E-Mailverkehrs und der Telefonate; sowie**
- die Einsichtnahme in das Benutzerkonto eines Mitarbeitenden**

04. Dezember 2014

Inhaltsverzeichnis

Präambel.....	3
1. Nutzung von Internet-Services und Telefondiensten	3
2. Überwachung von Internet-Services und Telefondiensten.....	3
2.1 Protokollierungen	3
2.2 Verbot von Spion-Programmen	3
2.3 Auswertung der Protokollierungen	3
2.4 Überwachung im Rahmen der Gewährleistung der Sicherheit und Funktionstüchtigkeit des betrieblichen EDV-Systems.....	4
2.5 Dauer der Aufbewahrung.....	4
3. Unterscheidung zwischen privaten und geschäftlichen E-Mails.....	4
4. Sanktionen bei Missbrauch	4
5. E-Mail-Verwaltung bei Abwesenheiten / Austritt von Mitarbeitenden.....	5
5.1 Vorhersehbare Abwesenheit.....	5
5.2 Unvorhersehbare Abwesenheit.....	5
5.3 Unvorhersehbare Abwesenheit mit langer Dauer	5
5.4 Austritt eines Mitarbeitenden	5
5.5 Abweichungen von den Ziffern 5.1 bis 5.4	6
6. Einsichtnahme in das Benutzerkonto von Mitarbeitenden	6
7. Verdacht eines strafbaren Verhaltens	6
8. Die Verwendung von Clouds.....	6
9. Abweichungen.....	7
10. Auskünfte	7
11. Inkrafttreten.....	7
Anhang 1: Antragsformular für das Einsichtsrecht in ein Benutzerkonto eines Mitarbeitenden.....	8
Anhang 2: Abweichungen von den Ziffern 5.1 bis 5.4 der Weisung betreffend die Überwachung und Nutzung von Internet, E-Mail und Telefon	9

Präambel

Die vorliegende Weisung legt dar, ob und wie Mitarbeitende von Konzerngesellschaften der AFG Arbonia-Forster-Holding AG (nachfolgend „AFG“) Internet-Services und Telefondienste nutzen dürfen. Ausserdem bezweckt diese Weisung den Schutz der Mitarbeitenden und der AFG bei der Überwachung dieser Dienste sowie bei der Einsichtnahme in ein Benutzerkonto. Lokale Vorschriften, die strengere Bestimmungen vorsehen oder die bei der Umsetzung der Weisung zur Anwendung kommen, sind zu beachten.

1. Nutzung von Internet-Services und Telefondiensten

Stehen Mitarbeitenden Internet-Services (Internet / E-Mail) und Telefondienste zur Verfügung, sind diese für geschäftliche Zwecke bestimmt und sollen dazu dienen, Arbeiten besser und / oder rationeller bzw. professioneller erledigen zu können.

Der BU-Leiter¹ entscheidet, ob sich die Nutzung ausschließlich auf dienstliche Belange erstreckt. Es dürfen keine Web-Seiten mit kriminellem, pornographischem und rassistischem Inhalt besucht werden. Ebenso ist die Teilnahme an entsprechenden Aktivitäten (z.B. mittels Gedankenaustausch über Chats, E-Mails etc.) verboten. Es können automatische Filter eingesetzt werden, die Inhalte bestimmter Kategorien blockieren. Es handelt sich dabei um Seiten mit folgenden Inhalten: Pornographie, kriminelle Aktivitäten, extremistische Inhalte, Chat, Drogen.

Aus Sicherheitsgründen werden alle E-Mails und Internetzugriffe inkl. Downloads automatisch auf Viren und gefährliche Inhalte überprüft und im Bedarfsfall geblockt. Dies gilt auch für verschlüsselte Verbindungen ins Internet (z.B. Onlinebanking). Trotzdem sind E-Mails von unbekanntem Absendern oder solche, die im Betreff auf Viren hinweisen, sofort ungelesen zu löschen. Keinesfalls dürfen E-Mail-Anhänge unbekannter Absender geöffnet werden.

2. Überwachung von Internet-Services und Telefondiensten

2.1 Protokollierungen

Die Informatikabteilung protokolliert die Internetaktivitäten. Ein- und ausgehende Telefonate werden protokolliert. Eine Protokollierung definiert sich als fortlaufende Aufzeichnung von Randdaten „wer“, „was“, „wann“ und findet in der AFG an folgenden Stellen statt:

- Internet (besuchte Internetseiten, Nutzer, Datum, Zeit)
- E-Mail (Absender, Empfänger, Datum, Zeit, Betreffzeile)
- Anmeldung am System (Nutzer, Datum, Zeit)
- Telefon (Telefonnummern aller Teilnehmer, Zeit, Datum, Dauer)

2.2 Verbot von Spion-Programmen

Es dürfen keine Spion-Programme (sog. Spyware) eingesetzt werden. Unter Spion-Programmen werden sämtliche Programme verstanden, die eine Überwachung von Mitarbeitenden ohne deren Wissen ermöglichen.

2.3 Auswertung der Protokollierungen

Die Auswertung der Protokolle erfolgt auf verschiedenen Ebenen.

¹ Für die Mitarbeitenden der AFG Management AG entscheidet der CEO.

Anonyme Auswertung: Diese dient der Erstellung von Statistiken, wie z.B. zur strukturierten Wiedergabe der durchschnittlichen Internetnutzung, der am häufigsten besuchten Webseiten etc. Die untersuchten Personengruppen sind genügend gross zu halten, so dass Rückschlüsse auf einzelne Mitarbeitende nicht möglich sind (z.B. sämtliche Mitarbeitende der AFG Management AG).

Personenbezogene Auswertung: Eine personenbezogene Auswertung ist nur gestattet, wenn durch die anonyme Auswertung ein Missbrauch festgestellt wurde oder sonst ein Missbrauchsverdacht besteht. Als Missbrauch gilt jede Verletzung der Nutzungsbestimmungen gemäss Ziffer 1 dieser Weisung oder anderer arbeitsvertraglicher Pflichten.

Die personenbezogene Auswertung erfolgt auf Antrag des Vorgesetzten und wird durch die zuständige Personalabteilung in Zusammenarbeit mit der Informatikabteilung und – falls vorhanden – dem Datenschutzbeauftragten durchgeführt. Wird ein Missbrauchsverdacht nicht erhärtet, werden die personenbezogenen Auswertungen sofort eingestellt und die erhobenen Daten vernichtet.

2.4 Überwachung im Rahmen der Gewährleistung der Sicherheit und Funktionstüchtigkeit des betrieblichen EDV-Systems

Manifestiert sich eine Störung des EDV-Systems trotz technischer Schutzmassnahmen, können bei der Suche nach deren Ursache die Protokollierungen beigezogen werden. Stellt die Ursache der Störung ein Missbrauch dar, kann der identifizierte Mitarbeitende nach Ziffer 4 dieser Weisung sanktioniert werden.

2.5 Dauer der Aufbewahrung

Zu Beweissicherungszwecken werden die Protokolle der Internetaktivitäten während vier Wochen aufbewahrt, es sei denn, ein allfälliges Sanktions- oder Strafverfahren macht eine längere Aufbewahrung notwendig. Die Aufbewahrung der Telefonprotokolle richtet sich nach den lokal gültigen Bestimmungen des Fernmelderechts.

3. Unterscheidung zwischen privaten und geschäftlichen E-Mails

Der E-Mail-Account dient in erster Linie Unternehmenszwecken. Private Mitteilungen sind auf ein Minimum zu beschränken. Die AFG nimmt keine Einsichtnahme oder Bearbeitung von E-Mails vor, welche als privat gekennzeichnet sind. Wenn kein Unterscheidungsvermerk zwischen privaten und geschäftlichen E-Mails besteht und die private Natur eines E-Mails aufgrund der Adressierungselemente nicht erkennbar oder sonst wie anzunehmen ist, darf die AFG davon ausgehen, dass das E-Mail geschäftlich ist. Bestehen Zweifel über die Natur eines E-Mails, ist sie mit dem Mitarbeitenden zu klären.

Zusätzlich zum System-Backup können die geschäftlichen E-Mails bei Bedarf ausserhalb des persönlichen Postfachs gespeichert werden. .

Sobald erkannt wird, dass eine E-Mail privater Natur ist, darf die AFG deren Inhalt nicht zur Kenntnis nehmen. Dies gilt selbst dann, wenn vermutet wird, dass mittels E-Mail eine Straftat begangen wurde oder ein sonstiger Missbrauchsfall gemäss Ziffer 1 dieser Weisung vorliegt.

4. Sanktionen bei Missbrauch

Wurden die Voraussetzungen und Regeln der Überwachung eingehalten und hat sich dabei herausgestellt, dass ein Missbrauch vorliegt, können arbeitsrechtliche Sanktionen ausgesprochen werden (Abmahnung, Sperrung des Internetzugriffs, Kündigung etc.).

Vor einer Löschung missbräuchlich erworbener Dateien wird der betroffene Mitarbeitende informiert und es wird ihm, sofern vertretbar, die Möglichkeit gegeben, die betreffenden Dateien (z.B. private E-Mails) auf einen privaten Datenträger zu speichern.

5. E-Mail-Verwaltung bei Abwesenheiten / Austritt von Mitarbeitenden

5.1 Vorhersehbare Abwesenheit

Bei Abwesenheiten ab einem Tag ist im Outlook der Abwesenheitsassistent zu aktivieren. In der Abwesenheitsmeldung ist zu vermerken, wer für dringende Angelegenheiten der Stellvertreter / die Stellvertreterin (inkl. Kontaktdaten) ist und ob die eingehenden E-Mails automatisch weitergeleitet werden oder nicht. Die automatische Weiterleitung sämtlicher E-Mails an den Stellvertreter / die Stellvertreterin darf nur in Ausnahmefällen erfolgen.

Hat ein Mitarbeitender versehentlich vergessen, den Abwesenheitsassistenten zu aktivieren, ist nach Ziffer 6 vorzugehen.

5.2 Unvorhersehbare Abwesenheit

Bei unvorhergesehener Abwesenheit (wie z.B. Krankheit, Unfall) stellt der Mitarbeitende sobald wie möglich sicher, dass dringende, eingehende E-Mails weitergeleitet werden. Dies kann z.B. durch die Benutzung des jeweiligen, sicheren Access Portals erfolgen. Der Mitarbeitende kann auch einen Stellvertreter / eine Stellvertreterin bezeichnen, der / die berechtigt ist, die eingehenden geschäftlichen E-Mails einzusehen und wenn nötig weiterzubearbeiten. Ist der Mitarbeitende nicht in der Lage, für die Weiterleitung der E-Mails besorgt zu sein, ist nach Ziffer 6 vorzugehen.

5.3 Unvorhersehbare Abwesenheit mit langer Dauer

Ist in Fällen unvorhergesehener Abwesenheit die Rückkehr an den Arbeitsplatz nicht absehbar oder dauert die Abwesenheit besonders lange (mehr als 4 Wochen), können nach Massgabe von Ziffer 6 (weitere) Einsichtnahmen vorgenommen werden.

5.4 Austritt eines Mitarbeitenden

Der austretende Mitarbeitende ist für die Übergabe sämtlicher Geschäftsdokumente verantwortlich. Er hat vor dem Austritt Laufwerke und den Posteingang zu bereinigen. Die noch hängigen Geschäfte wie E-Mails etc. oder andere für die AFG notwendige bzw. nützliche Informationen sind weiterzuleiten. Der austretende Mitarbeitende hat zudem den Abwesenheitsassistenten einzurichten, der darüber informiert, dass die E-Mail-Adresse nicht mehr gültig ist und die Kontaktdaten des Nachfolgers beinhaltet.

Der austretende Mitarbeitende hat die Möglichkeit, private E-Mails und andere private Dokumente zu löschen bzw. auf einem privaten Datenträger zu speichern.

Spätestens am letzten effektiven Arbeitstag wird das Benutzerkonto (inkl. E-Mail-Konto) gesperrt. Ist nach erfolgter Sperrung eine Einsichtnahme in das E-Mail-Konto oder einen Benutzerordner notwendig, richtet sich das Einsichtsrecht nach Ziffer 6. Sollte der Abwesenheitsassistent vom austretenden Mitarbeitenden nicht eingerichtet worden sein, ist analog der Ziffer 6 vorzugehen und der Abwesenheitsassistent ist zu aktivieren. Es ist darauf zu achten, dass keine Rückschlüsse auf die Art der Beendigung des Arbeitsverhältnisses möglich sind.

Spätestens 30 Tage nach dem letzten effektiven Arbeitstag wird das Benutzerkonto gelöscht. In Ausnahmefällen erfolgt die Löschung des Benutzerkontos spätestens 90 Tagen nach dem letzten effektiven Arbeitstag.

5.5 Abweichungen von den Ziffern 5.1 bis 5.4

Zulässige Abweichungen von den Ziffern 5.1 bis 5.4 sind in Anhang 2 festgehalten.

6. Einsichtnahme in das Benutzerkonto von Mitarbeitenden

Ist trotz der Bestimmungen von Ziffer 5. eine Einsicht in das E-Mail-Konto eines Mitarbeitenden notwendig, ist zuerst der betroffene Mitarbeitende zu kontaktieren und seine Einwilligung zur Einsichtnahme einzuholen. Verweigert dieser die Einsichtnahme oder kann er nicht erreicht werden, hat der Vorgesetzte einen schriftlichen Antrag an die zuständige Personalabteilung zu stellen (vgl. Anhang). Die Bewilligung wird nur erteilt, wenn die AFG ein überwiegendes Interesse hat (z.B. dringende, betriebliche Gründe), auf die Rückkehr des Mitarbeitenden nicht gewartet werden kann und sämtliche Massnahmen getroffen worden sind, um eine Einsichtnahme zu verhindern. Eine automatische Weiterleitung aller E-Mails ist nur in Ausnahmefällen erlaubt.

Wird der Antrag bewilligt, erfolgt eine Mitteilung an die Informatikabteilung, welche den Zugang zum Benutzerkonto ermöglicht (mittels Zurücksetzen des Passworts oder Einrichtung eines Links). An der Einsichtnahme nehmen der Vorgesetzte sowie ein Mitarbeitender der Personalabteilung teil (Vieraugen-Prinzip). Der abwesende Mitarbeitende wird darüber spätestens am Tag seiner Rückkehr an den Arbeitsplatz informiert.

Die Einsichtnahme hat sich in zeitlicher und inhaltlicher Hinsicht auf die im Antragsformular gemachten Angaben zu beschränken. Es dürfen nur geschäftliche E-Mails eingesehen werden. Als privat erkannte E-Mails dürfen weder geöffnet, eingesehen, verschoben, kopiert, weitergeleitet und/oder gelöscht werden (vgl. auch Ziffer 3). Der Vorgesetzte leitet die notwendigen E-Mails an sich selbst weiter. Ausserdem ist der Abwesenheitsassistent zu aktivieren, mit dem Hinweis wer in dringenden Angelegenheiten kontaktiert werden kann.

Diese Bestimmungen gelten in analoger Weise nach dem Austritt eines Mitarbeitenden und für die Einsichtnahme in Benutzerordner.

7. Verdacht eines strafbaren Verhaltens

Wird durch die Auswertung der Protokollierungen oder durch andere Hinweise eine Straftat festgestellt oder vermutet, werden die entsprechenden Protokolle gesichert. Die AFG behält sich das Recht vor, Strafanzeige gegen die betroffene Person zu erstatten. Ist die Einsichtnahme in private E-Mails, Daten etc. notwendig, ist dies nur mit vorgängiger Zustimmung des verdächtigen Mitarbeitenden vorzunehmen. Ist die vorgängige Einholung nicht möglich oder wird die Zustimmung verweigert, ist die Angelegenheit grundsätzlich der zuständigen Strafverfolgungsbehörde zu übergeben. Ausnahmsweise kann die AFG die Einsichtnahme selbst vornehmen, wenn ein überwiegendes Interesse und konkrete Verdachtsmomente dies rechtfertigen. Die Einsichtnahme richtet sich nach Ziffer 6 vorstehend.

Die AFG verpflichtet sich, das Resultat der Ermittlungen gegenüber Dritten, insbesondere auch gegenüber anderen Mitarbeitenden, vertraulich zu behandeln.

8. Die Verwendung von Clouds

Clouds sind virtuelle IT-Infrastrukturen zur Speicherung von Informationen im Internet (z.B. Dropbox). Die Nutzung von Clouds kann grosse Vorteile mit sich bringen, kann man doch beispielsweise von zu Hause aus oder von unterwegs auf die in der Cloud gespeicherten Daten zugreifen. Gleichzeitig bergen Clouds aber auch gros-

se Sicherheitsrisiken. Aus diesem Grund ist die Verwendung einer Cloud nur gestattet, wenn diese vom zuständigen BU-Leiter² nach Einholung einer Empfehlung von der zuständigen IT-Abteilung freigegeben wurde.

9. Abweichungen

Abweichungen von den vorgenannten Ziffern sind nur nach Rücksprache mit dem Head of Legal & Compliance zulässig.

10. Auskünfte

Auskünfte im Zusammenhang mit der vorliegenden Weisung erteilt der Head of Legal & Compliance.

11. Inkrafttreten

Diese Weisung tritt per sofort Kraft und ersetzt die Weisung betreffend die Überwachung und Nutzung von Internet, E-Mail und Telefon vom 29. August 2013.

Arbon, 04. Dezember 2014

AFG Arbonia-Forster-Holding AG

William J. Christensen
Chief Executive Officer

Andrea Wickart
Head of Legal & Compliance
Generalsekretärin

² Für die Mitarbeitenden der AFG Management AG ist der CEO zuständig.

Anhang 1: Antragsformular für das Einsichtsrecht in ein Benutzerkonto eines Mitarbeitenden

Betroffener Mitarbeitender	
Name:	Gesellschaft:
Funktion:	
Gegenstand der Einsichtnahme	
<input type="checkbox"/> E-Mails	<input type="checkbox"/> Dateien
Grund der Einsichtnahme	
<input type="checkbox"/> geplante Abwesenheit	voraussichtliche Rückkehr am:
<input type="checkbox"/> unvorhergesehene Abwesenheit	
<input type="checkbox"/> Mitarbeitender ist bereits ausgetreten	Austritt am:
<input type="checkbox"/> Verdacht eines strafbaren Verhaltens	Konkrete Verdachtsgründe:
Die Einsichtnahme ist dringend notwendig, weil	
Umfang der Einsichtnahme (so detaillierte Angaben wie möglich)	
E-Mails bzw. Dateien zu folgenden Themen werden dringend benötigt:	Es soll nach E-Mails bzw. Dateien in folgendem Zeitraum gesucht werden:
Kontaktnahme mit dem betroffenen Mitarbeitenden	
<input type="checkbox"/> Ja, es wurde versucht, die Einwilligung des betroffenen Mitarbeitenden vorgängig einzuholen, mit folgendem Ergebnis:	<input type="checkbox"/> Nein, es wurde nicht versucht, die Einwilligung des betroffenen Mitarbeitenden vorgängig einzuholen, weil:
Alternativen	
Folgendes wurde unternommen, um die Einsichtnahme zu vermeiden:	
<input type="checkbox"/> im Gemeinschaftsordner (Laufwerk G: / gemeinsames E-Mail-Konto) wurde nach den benötigten Dateien gesucht.	<input type="checkbox"/> andere Teammitglieder des Abwesenden wurden nach den benötigten Dateien / E-Mails gefragt.
<input type="checkbox"/> Sonstiges:	
Ort / Datum	Unterschrift

Anhang 2: Abweichungen von den Ziffern 5.1 bis 5.4 der Weisung betreffend die Überwachung und Nutzung von Internet, E-Mail und Telefon

Aus betrieblichen und technischen Gründen gelten für die Division Gebäudetechnik folgende Abweichungen von den Ziffern 5.1 bis 5.4:

Einrichtung von Abwesenheitsassistenten

Innerhalb der Division Gebäudetechnik werden grundsätzlich im Aussenverhältnis keine Abwesenheitsassistenten eingerichtet. Die betroffenen Mitarbeitenden werden angewiesen, in Fällen von vorhersehbaren oder unvorhersehbaren Abwesenheiten sowie bei Austritt

- (a) einen Stellvertreter / eine Stellvertreterin zu bezeichnen, der / die berechtigt ist, die eingehenden geschäftlichen E-Mails einzusehen und wenn nötig weiterzubearbeiten; oder
- (b) die automatische Weiterleitung sämtlicher eingehender E-Mails einzurichten.

Die Bezeichnung des Stellvertreters / der Stellvertreterin bzw. das Einrichten der automatischen Weiterleitung kann ausschliesslich durch den Mitarbeitenden selbst erfolgen.

Löschung des Benutzerkontos bei Austritt eines Mitarbeitenden

Das Benutzerkonto wird in der Regel 30 Tage nach dem letzten effektiven Arbeitstag, jedoch frühestens mit Ablauf der Kündigungsfrist gelöscht. In Ausnahmefällen kann die Löschung zu einem späteren Zeitpunkt erfolgen, jedoch spätestens wenn der betriebliche Zweck erfüllt ist.