Muster-Betriebsvereinbarung
Internet- und Email-Nutzung

Bitte beachten Sie, dass es sich hier um Mustervereinbarungen handelt. Beim Einsatz von neuen Techniken und Systemen müssen immer die betrieblichen Besonderheiten beachtet werden. Eine Systemeinführung gleicht der anderen kaum, da unterschiedliche Absichten mit der Einführung verfolgt werden. Mustervereinbarungen können diese Individualität nicht leisten!

§ 1 Geltungsbereich

Diese Vereinbarung gilt für alle Arbeitnehmerinnen und Arbeitnehmer der Firma. Die Vereinbarung umfasst alle Betriebsstätten des Unternehmens.

§ 2 Gegenstand

Die Vereinbarung regelt die Einführung und Anwendung der Internet- und Emailnutzung im Unternehmen.

§ 3 Zweckbestimmung

Mit dem Ermöglichen der Internet- und Emailnutzung und dieser Vereinbarung werden ausschließlich die folgenden Zwecke verfolgt:

- die Unterstützung der Arbeit der Mitarbeiterinnen und Mitarbeiter durch die Nutzung von Internetdienstleistungen, Informations- und Kommunikationsdiensten
- die Gewährleistung des Schutzes der persönlichen Daten der Beschäftigten
- die Gewährleistung des Schutzes der Gesundheit der Beschäftigten bei der Nutzung von Internet und Email

§ 4 Grundsätze der Nutzung

(1) Die Freischaltung des Zugangs für einzelne Mitarbeiterinnen und Mitarbeiter erfolgt funktionsbezogen, d.h. wenn die Nutzung zur Unterstützung der Arbeit sinnvoll ist. Alle Mitarbeiterinnen und Mitarbeiter, auf die diese Bedingung zutrifft, erhalten die Berechtigung.

(2) Internet und Email werden primär für geschäftliche Zwecke eingesetzt. Die gelegentliche Nutzung dieser Systeme für persönliche oder nicht die Geschäfte der Gesellschaft betreffenden Zwecke wird gestattet. Sie darf jedoch nicht die geschäftlichen Abläufe beeinträchtigen.

(3) Um die berechtigten Geschäftsinteressen des Unternehmens bei der Nutzung von Internet und Email zu wahren, sind die folgenden Grundsätze einzuhalten.

(Die folgende Liste kann an das Unternehmen angepasst werden, etwa durch die Übernahme von akzeptablen Passagen aus vorhandenen Richtlinien (Policies).)

> *- Jegliche Nutzung des Namens oder der Service-Zeichen des Unternehmens außerhalb des Beschäftigungsrahmens der Mitarbeiter und Mitarbeiterinnen bei dem Unternehmen ist ohne die ausdrückliche Befugnis der Geschäftsleitung des Unternehmens untersagt.*
> *- Nur nach der vorherigen Genehmigung durch die entsprechenden Stellen des Unternehmens dürfen öffentliche Darstellungen über das Unternehmen ausgegeben werden.*
> *- Unter keinen Umständen dürfen Informationen vertraulicher, sensibler oder anderweitig gesetzlich geschützter Art im Internet plaziert oder dort eingegeben oder anderweitig an jemandem außerhalb des Unternehmens offen gelegt werden.*
> *- Das Emailsystem darf nicht in einer Weise genutzt werden, die Anderen gegenüber störend oder offensiv ist, noch in einer Weise, die mit dem professionellen Image des Unternehmens unvereinbar ist.*
> *- Die Anzeige oder die Übertragung von Bildern, Botschaften, Karikaturen oder Mitteilungen, die eine Belästigung oder Verunglimpfung von anderen darstellen, einschließlich solcher sexueller Art, basierend auf Rasse, Nationalität, Geschlecht, Alter, Invalidität oder einer sonstigen geschützten Klasse, sind verboten.*
> *- Manipulationen an der elektronischen Identität bei der Internet- und Emailnutzung sind verboten.*

(4) Für die Emailnutzung wird den Benutzern ein ausreichender Speicherraum zur Verfügung gestellt; vor Erreichung der Speichergrenzen erhalten Sie einen Hinweis.

(5) Für Abwesenheitszeiten (Urlaub, Dienstreisen...) erhalten die Nutzer die Möglichkeit, eine Person ihres Vertrauens mit der Verwaltung ihres Mail-Accounts zu beauftragen.

(*Hier lässt sich ein genaueres Verfahren für eine Vertretungsregelung beschreiben, etwa mit Hilfe von Abwesenheitsprofilen: Die Nutzer können ein „Abwesenheitsprofil" ausfüllen. Mit diesem elektronischen Formular können die Benutzer für die (internen?) Mail-Absender angeben, wie lange sie voraussichtlich nicht erreichbar sind. Zusätzlich kann eine kurze Mitteilung beigefügt werden. Die Abwesenheitsprofile werden nach Ablauf der von den Benutzern selbst angegebenen Fristen automatisch vom System gelöscht.*)

(6) Für die Versendung vertraulicher Informationen innerhalb des Unternehmens werden ausreichende Verschlüsselungsmöglichkeiten zur Verfügung gestellt.

(7) Das Unternehmen sorgt für einen systemseitigen ausreichenden Schutz vor Viren oder sonstigen Sicherheitsrisiken bei der Internet- und Emailnutzung.

(8) Die Berechtigung zur Nutzung von Internet und Email wird organisatorisch und programmtechnisch geregelt.

§ 5 Systembeschreibung

(1) Die technische Umgebung des Internet- und Emailzugangs ist in Anlage 1 in einer Übersicht dargestellt. Die Nutzung eines Firewall-Systems wird in einer eigenen Vereinbarung geregelt. Die für Internet und Email verwendeten Programme werden in der Anlage 2 abschließend aufgeführt. Eine Kurzbeschreibung der Programme ist ebenfalls in der Anlage 2 beigefügt. Aus ihr ergeben sich die wesentlichen Funktionen der Programme.

(2) Durch die zugriffsberechtigten Systemadministratoren darf nur Einsicht in solche Daten genommen werden, die für die Betriebsfähigkeit des Netzwerks und der dezentralen Einheiten von Bedeutung sind.

§ 6 Leistungs- und Verhaltenskontrolle

Die mit der Internet- und Emailnutzung zusammenhängenden Hard- und Software-systeme werden nicht zum Zweck der Leistungs- und Verhaltenskontrolle der Arbeitnehmer und Arbeitnehmerinnen genutzt.
Die bei der Nutzung von Internet und Email für Zwecke der Systemsicherheit und des ordnungsgemäßen Systembetriebs erfassten Benutzerdaten dürfen ausschließlich von den zugriffsberechtigten Personen für diese Zwecke verwendet werden. Zu anderen Zwecken dürfen die Daten nicht verwendet bzw. weitergegeben werden.

§ 7 Personenbezogene und -beziehbare Daten

(1) Bei der Nutzung von Internet und Email werden die in der Anlage 3 abschließend aufgeführten personenbezogenen Daten protokolliert und gespeichert. *(User-Id, Datum/Uhrzeit, Internetadresse (URL), IP aufrufender Rechner, Menge der übertragenen Dateien...)*

(2) Ein Muster der betroffenen Dateien, aus der deren jeweiliger Aufbau hervorgeht, ist ebenfalls in Anlage 3 aufzuführen.

(3) Eine Auswertung der Daten zu Aufkommen und Volumen des Datenverkehrs erfolgt ausschließlich summarisch pro Anschluss als Monatssumme. Bei der Internetznutzung ist dabei ein Zugriff auf die Internetadressen (URL) der einzelnen Seiten ausgeschlossen.
Bei der Internetnutzung wird eine Berechtigung zu Zwecken der Fehleranalyse und Analyse der Systemsicherheit eingerichtet, die Auswertungen auf die einzelnen Protokollzeilen einschließlich der Internetadressen (URL) der gelesenen Seiten erlaubt, allerdings ohne den Zugriff auf die Benutzer- oder Gerätekennung.

(4) Auswertungen, die personenbezogene oder -beziehbare Daten enthalten, sind in der Anlage 4 abschließend aufgeführt. Dabei sind die folgenden Angaben zu dokumentieren:

- Bezeichnung des erstellenden Programmes
- Name der Auswertung
- Datenfelder
- Zweck der Auswertung
- Form der Auswertung (Ausdruck, Datei...)
- Aussagefähiges Muster der Auswertung

(5) Ergibt sich ein begründeter Mißbrauchsverdacht, erhält der Arbeitgeber nach Zustimmung des Betriebsrats unter Hinzuziehung eines Mitglieds des Betriebsrats Zugriff auf die pseudonymisierten Nutzungsdaten, die zur Aufklärung des Verdachts erforderlich sind.
Erhärtet sich der Verdacht bei dieser pseudonymisierten Untersuchung, erhält der Arbeitgeber nach Zustimmung des Betriebsrats unter Hinzuziehung eines Mitglieds des Betriebsrats und im Beisein des betroffenen Mitarbeiters oder der betroffenen Mitarbeiterin Zugriff auf die reidentifizierten Daten dieser Person für den entsprechenden Zeitraum. Zu diesem Zweck wird eine Berechtigung geschaffen, die an ein geteiltes Passwort gebunden ist und unter Eingabe der Benutzer- oder Gerätekennung die notwendigen personenbezogenen Informationen für den ausgewählten Zeitraum anzeigt. Über eines der beiden Passwörter verfügt der jeweils zuständige Betriebsrat.

(6) Weitere Auswertungen sind nicht zulässig.

(7) Personenbezogene Daten, die für den Zweck der Verarbeitung nicht mehr erforderlich sind, sind unverzüglich zu löschen. Für den Mißbrauchsverdacht des Absatzes 5 gilt dies für die Feststellung, daß der Verdacht unberechtigt war. In diesem Fall sind auch die erstellten Unterlagen zu vernichten. Für die gespeicherten Daten und Auswertungen nach den Regelungen dieses Paragraphen sind Löschfristen in den jeweiligen Anhang aufzunehmen.

(8) Daten von Mitarbeitern und Mitarbeiterinnen, die ausscheiden, sind zu löschen, soweit sie nicht für eine weitere zulässige Verarbeitung erforderlich sind.

§ 8 Zugriffsberechtigungen

(1) Die Zugriffberechtigungen mit Systemprivilegien zu den Programmen und Daten im Zusammenhang mit der Internet- und Emailnutzung werden organisatorisch und programmtechnisch geregelt. Die Zugriffs- und Verfügungsbefugnisse sind möglichst eng zu fassen.

(2) Die zugriffsberechtigten Personen sind abschließend in Anlage 5 aufgeführt.

(3) Die zugriffsberechtigten Personen sind nach § 5 BDSG auf das Datengeheimnis zu verpflichten und haben eine entsprechende Verpflichtungserklärung zu unterschreiben. Die Verantwortung aus dieser Verpflichtung ist ihnen angemessen zu erläutern. Bei Bedarf sind diese Personen vor diesem Hintergrund zu schulen.

§ 9 Qualifizierung

(1) Die betroffenen Mitarbeiter und Mitarbeiterinnen der Systembetreuung werden für die neuen Funktionen auf Kosten des Arbeitgebers geschult. Die Schulungen finden während der Arbeitszeit statt.

(2) Die Benutzer und Benutzerinnen von Internet und Email werden ausreichend qualifiziert. Die Maßnahmen schulen und informieren:

- in anwendungstechnischer Hinsicht, insbesondere in einer effektiven Nutzung und arbeitsorganisatorisch optimierten Einbindung in die übrigen Tätigkeiten der Nutzer und Nutzerinnen
- bezüglich gesundheitlicher Risiken
- in Fragen des Datenschutzes und der Persönlichkeitsrechte, wobei auch die Möglichkeiten des Systems zur Protokollierung und die diesbezüglichen Einflußmöglichkeiten der Nutzer erläutert werden (Löschen von Histories, Caches..)
- in Fragen der Daten- und Systemsicherheit, auch hinsichtlich der Verschlüsselung bei Emails
- in rechtlichen Fragen im Zusammenhang mit dem Zugriff auf Webseiten mit strafrechtlich relevanten Inhalten
- hinsichtlich der Regelungen dieser Vereinbarung

Die entsprechenden Informations- und Qualifzierungsmaßnahmen werden mit dem Betriebsrat abgestimmt.

(3) Weitere zugriffsberechtigte Personen nach dieser Vereinbarung werden ebenfalls angemessen qualifiziert, um ihre mit der Zugriffsberechtigung verbundenen Aufgaben kompetent ausüben zu können. Z.B. der betriebliche Datenschutzbeauftragte.

§ 10 Rechte des Betriebsrats

(1) Der Betriebsrat hat das Recht, jederzeit unter Wahrung der Persönlichkeitsrechte der Beschäftigten diese Vereinbarung zu kontrollieren. Dem Betriebsrat sind, soweit nicht anders geregelt, auf Anforderung die erforderlichen Unterlagen zur Verfügung zu stellen. Der Betriebsrat kann auch in unregelmäßigen Abständen und unangemeldet Kontrollausgaben zu allen personenbezogenen Daten der Beschäftigten, auch gruppen- und abteilungsweise verlangen. Er hat das Recht, sämtliche Unterlagen der Systemdokumentation einzusehen und sich erläutern zu lassen.

(2) Der Betriebsrat kann hierfür dem Arbeitgeber einen Beauftragten benennen, der die Kontrollen durchführt.

(3) Dem Betriebsrat ist auf Verlangen Einblick in die Räume, Funktionseinheiten und Unterlagen zur Prüfung der Einhaltung dieser Vereinbarung zu geben. Er kann auch jederzeit Systemverwaltungsprotokolle sowie die Konfigurationen einsehen.

(4) Der Betriebsrat ist darüber hinaus berechtigt, jederzeit einen Sachverständigen seiner Wahl zur Kontrolle dieser Vereinbarung hinzuzuziehen.

§ 11 Änderung, Ergänzung und Erweiterung

Änderungen, Ergänzungen und Erweiterungen der in dieser Vereinbarung beschriebenen Hard- und Softwaresysteme, insbesondere von Funktionen, Datenkatalogen, sowie der Auswertungen dürfen nur nach vorheriger Zustimmung des Betriebsrats erfolgen. Der Betriebsrat ist vorher rechtzeitig und umfassend zu informieren.

§ 12 Sanktionen/Verstöße

(1) Personelle Maßnahmen, die auf einer mißbräuchlichen oder unzulässigen Anwendung der mit dem Internetzugang zusammenhängenden Hard- und Softwaresysteme basieren, sind unwirksam. Personenbezogene Erkenntnisse und Maßnahmen aus einer solchen Anwendung dürfen weder bei internen Beurteilungen noch bei arbeitsgerichtlichen Verfahren als Beweismaterial verwendet werden. Weitere Rechte des Betriebsrats bleiben von dieser Regelung unberührt.

(2) Werden die mit der Internet- und Emailnutzung zusammenhängenden Hard- und Softwaresysteme entgegen den hier vereinbarten Regelungen anderweitig genutzt, wird der entsprechende Teil dieser Systeme so lange nicht genutzt, bis durch geeignete Maßnahmen sichergestellt ist, daß eine Wiederholung ausgeschlossen ist.

§ 13 Schlußbestimmungen

(1) Soweit in Gesetzen, Tarifverträgen und Betriebsvereinbarungen für Mitarbeiter und Mitarbeiterinnen günstigere Regelungen getroffen sind, gehen sie den Regelungen dieser Vereinbarung vor.

(2) Alle angeführten Anlagen zu dieser Vereinbarung sind Bestandteil der Vereinbarung.

(3) Die Vereinbarung tritt mit Unterzeichnung in Kraft.

(4) Sie kann von beiden Vertragsparteien mit einer Kündigungsfrist von 6 Monaten zum Monatsende gekündigt werden.

(5) Nach Eingang der Kündigung müssen unverzüglich Verhandlungen über eine neue Vereinbarung aufgenommen werden. Bis zum Abschluss einer neuen Vereinbarung gilt diese Vereinbarung weiter.