Benutzerrichtlinie für die Nutzung der Internet-Dienste und des E-Mail-Systems

1. Vorwort

Für die Netze der.....(Firmenname einsetzen)..... ist ein Internet-Zugang hergestellt worden. Die Mitarbeiter, die zur Nutzung der Dienste des Internets berechtigt sind, können Informationen über das Internet an andere übermitteln bzw. im Internet bereitstellen. Weiterhin können sie beliebige Inhalte aus dem Internet abrufen.

Das Internet selbst sieht grundsätzlich keine Maßnahmen zur Sicherstellung der Integrität, Vertraulichkeit und Authentizität der übertragenen Daten sowie der Kommunikation und der Kommunikationspartner vor. Die Auswahl und die Anwendung von geeigneten Datensicherheits- und Datenschutzmaßnahmen im Rahmen der Internetnutzung ist damit jedem Internet-Teilnehmer selbst überlassen.

Für die.....(Firmenname einsetzen)..... wurden die notwendigen Sicherheitsmaßnahmen durch .....(ggfls. externen Dienstleister einsetzen)..... ausgewählt und realisiert. Diese Maßnahmen können aber nur zu einem gewissen Teil von sich aus ihre Wirksamkeit entfalten. Ein ganz entscheidender Faktor zur Gewährleistung und Verbesserung der vorhandenen Sicherheitsmaßnahmen ist deren konsequente und gewissenhafte Anwendung in der täglichen Arbeit durch jeden Einzelnen.

Daher sind die Kenntnisse dieser nachfolgenden Regelungen und deren Einhaltung durch jede/n berechtigte/n Mitarbeiter/in eine wesentliche Voraussetzung für die Sicherheit dieses Kommunikationsmittels.

Die Missachtung und Nichteinhaltung dieser Regelungen gefährdet nicht nur die Vertraulichkeit, Verfügbarkeit und Integrität der von den Mitarbeitern auf ihrem eigenen DV-System unmittelbar be- und verarbeiteten Daten, sondern es wird dadurch auch die Vertraulichkeit, Verfügbarkeit und Integrität aller sonstigen Daten der .....(Firmenname einsetzen)..... gefährdet.

Diese Benutzerrichtlinien ergänzen die geltenden sonstigen Regelungen und Vorschriften bezüglich Datenschutz und Datensicherheit.

2. Regelungen

2.1 Verantwortung

Jede/r berechtigte/r Mitarbeiter/in ist in seinem/ihrem Zuständigkeitsbereich verantwortlich für die vollständige und korrekte Anwendung der jeweils geltenden Regelungen, Anweisungen und Vorschriften zur Gewährleistung von Datenschutz und Datensicherheit.

Jede/r berechtigte/r Mitarbeiter/in ist insbesondere zuständig und verantwortlich für die in seinem/ihrem Zuständigkeitsbereich liegende Anwendung der vorgesehenen und vorhandenen Zugangskontrolleinrichtungen, Zugriffseinrichtungen und Maßnahmen entsprechend der Dienstanweisung für Datenschutz und Datensicherheit in der jeweils aktuellen Fassung.

2.2 Nutzung des/r Internet (-dienste)

Das Einbringen von privater Hard- und/oder Software in das Datennetz der .....(Firmenname einsetzen).....ist nicht zulässig.

Die Einrichtung und der Betrieb eines nicht durch das Team .....(Name des Dienstleisters einsetzen)..... bereitgestellten Anschlusses an ein öffentlich zugängliches Netz (mittels Datenübertragungseinrichtungen wie Modem, ISDN-Einbaukarten usw.) ist nicht zulässig, weil dadurch weitere, unkontrollierbare und ungesicherte Übergänge in das lokale Netz geschaffen werden.

Die Nutzung des/r Internets (-dienste) ist ausschließlich zu dienstlichen Zwecken und lediglich in demjenigen Umfang erlaubt, der zur Erledigung der Aufgaben der/des jeweiligen Mitarbeiters/in erforderlich ist. Die Nutzung der Dienste zu privaten Zwecken ist untersagt.

Das Laden (Downloaden) und Ausführen von Programmen (dies betrifft auch so genannte Bildschirmschoner – Screensaver -), die aus den oder über die Internet-Dienste beschafft wurden, ist ohne vorherige Prüfung und Freigabe durch .....(Abteilung oder Person einsetzen)..... untersagt, um insbesondere das Risiko des Einschleppens von Computerviren im lokalen Netzwerk zu reduzieren und Lizenzverstöße auszuschließen.

Unzulässig ist jede Nutzung, die geeignet erscheint, den Interessen, dem Ansehen in der Öffentlichkeit der.....(Firmenname einsetzen)..... zu schaden oder die gegen geltende Gesetze oder Verordnungen verstößt.

Verboten ist das Abrufen und Ins-Netz-Stellen

- von Dateien, die gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,

- von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen oder pornografischen Äußerungen oder Abbildungen.

Das Ausprobieren, das Ausforschen und die unberechtigte Benutzung fremder Zugriffsberechtigungen (wie z. B. Benutzererkennungen, Passworte) und sonstiger Authentifizierungsmittel (wie z. B. Chipkarten, Magnetkarten) ist unzulässig.

Die Weitergabe und das Zurverfügungstellen von eigenen Benutzererkennungen und sonstigen Authentifizierungshilfsmitteln für eine Benutzung durch Dritte ist unzulässig. Es wird ausdrücklich darauf hingewiesen, dass in einem derartigen Fall aus den Protokolldaten die Identität des/der jeweiligen Mitarbeiters/in hervorgeht. Jegliche Aktivität – auch unzulässige – durch diesen Dritten wird also dem/der jeweiligen verantwortlichen Mitarbeiter/in zugeschrieben.

3. Nutzung des E-Mail-Dienstes

Für die Netze der.....(Firmenname einsetzen).....ist ein E-Mail-Dienst eingerichtet worden. Über diesen Dienst können alle Teilnehmer des E-Mail-Verbundes direkt kontaktiert werden (globales Adressbuch), mittels so genannter Internet-Mail-Adressen können aber auch alle aktiven E-Mail-Adressen weltweit über das Internet erreicht werden. Ebenso können auf diesem Wege alle E-Mail-Empfänger innerhalb der .....(Firmenname einsetzen).....von außen erreicht werden, hierzu muss allerdings die jeweilige Internet-Mail-Adresse des Empfängers bekannt sein.

E-Mail wird zum Empfang und zur Versendung von elektronischer Post genutzt. Sie kann zur Weitergabe von Dateien und Vorgängen benutzt werden. Dokumente mit vertraulichem Inhalt dürfen ohne Verschlüsselung nicht per E-Mail versandt werden.

Jede Abteilung hat sicherzustellen, dass das E-Mail im Falle von Abwesenheit (z. B. Urlaub, Dienstreise, Krankheit) durch entsprechend berechtigte Mitarbeiter/innen geöffnet werden kann (Aufstellen und Aktivieren einer Regel, die eine Weiterleitung an berechtigte Mitarbeiter sicherstellt).

Das E-Mail dient dem Verschicken kurzer Nachrichten. Es dürfen keine E-Mails größer als derzeit ..... MByte versandt werden, dieser Wert kann auf Grund technischer Erfordernisse geändert werden. Die Größe der Nachrichten kann unter anderem im Explorer/Dateimanager überprüft werden. Gegebenenfalls sind die anzufügenden Dateien mit geeigneter Software zu komprimieren.

Für die Verwaltung des E-Mail-Systems ist der Netzwerkadministrator (...Name...) zuständig. Er muss mit den Bestimmungen des Fernmeldegeheimnisses im TKG und den Vorschriften des Hessischen Datenschutzgesetzes vertraut sein. Über alle Informationen, die sie durch ihre Tätigkeit erhalten, haben sie Stillschweigen zu bewahren.

So weit die E-Mail dienstliche Hinweise betrifft, kann der Vorgesetzte verlangen, dass der/die Beschäftigte ihm die E-Mail bereitstellt.

4. Sicherheitsrelevante Ereignisse

Alle sicherheitsrelevanten Ereignisse (z. B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste, Verdacht auf Missbrauch der eigenen Benutzererkennung usw.) sind sofort .....(Name oder Abteilung einsetzen)..... zu melden. Dort wird der Angelegenheit nachgegangen.

Auch bei verdächtigen E-Mails ist umgehend ....(Name oder Abteilung einsetzen)....zu informieren. Vorhandene Anlagen sind nicht zu öffnen.

Verdächtige E-Mails sind u. a.:

– unbekannter Absender mit nicht angeforderten Anlagen
– bekannter Absender mit nicht angeforderten Anlagen, die nicht näher beschrieben sind oder in einer ausländischen Sprache beschrieben werden.
– Anlagen mit Dateikennungen, z. B. exe, com, bin, vbs, vbe, bat, cmd, js, jse, wsf, wsh, inf.

Hierbei handelt es sich um Dateien (Programme), die Befehle ausführen. Diese Programme sollten nur dann gestartet werden, wenn zweifelsfrei die Herkunft geklärt ist und der Zweck des Programms über das Team .....(Name einsetzen)..... geklärt ist.

Es sind keine eigenen Aufklärungsversuche vorzunehmen, da eventuell wertvolle Hinweise und Spuren verwischt werden oder verloren gehen könnten.

5. Protokollierung und Kontrollen

Jeder Datenverkehr mit den Internet-Diensten unterliegt einer automatischen Protokollierung bei dem Provider der .....(Firmenname einsetzen).....; das ist derzeit die .....(Name des Providers/Dienstleisters einsetzen)..... .

Die Protokolldaten dienen ausschließlich zu Zwecken der Datenschutzkontrolle und zur Sicherstellung eines ordnungsgemäßen Betriebes. Sie werden nicht für Zwecke der Leistungskontrolle verwandt.

Die Einhaltung dieser Richtlinien kann durch den Datenschutzbeauftragten, den Netzwerkadministrator und einen Vertreter des Personalrates gemeinsam stichprobenartig oder anlassbezogen kontrolliert werden.

6. Verstöße

Der Datenschutzbeauftragte und das Team .....(Name einsetzen)..... sind unverzüglich über Missbrauch und Missbrauchversuche der Internet-Dienste und des E-Mail-Systems zu informieren. Diese informieren .....(Name des/der Personalleiters/Vorgesetztenstelle einsetzen)..... .

7. Sanktionen

Verstöße gegen diese Benutzerrichtlinien und die sonstigen Regelungen und Vorschriften bezüglich der Anwendung der Informationstechnik und bezüglich des Umgangs mit personenbezogenen Daten können arbeitsrechtliche sowie strafrechtliche Konsequenzen (siehe Punkt 2.2) haben.