Dienstvereinbarung über die Nutzung der informationstechnischen Systeme (IT-Systeme)

zwischen dem Oberbürgermeister der Stadtverwaltung Göppingen

und

dem Personalrat der Stadt Göppingen

wird die folgende Dienstvereinbarung über die Nutzung der informations-technischen Systeme (IT Systeme) abgeschlossen

Um die Lesbarkeit dieser Dienstvereinbarung zu verbessern,
wurde auf die zusätzliche Verwendung der weiblichen Form verzichtet.

1 Ziel dieser Dienstvereinbarung

Diese Dienstvereinbarung regelt den Einsatz, die Nutzung und die grundlegenden Sicherheitsmaßnahmen für **alle** bei der Stadtverwaltung Göppingen eingesetzten informationstechnischen Systeme (IT-Systeme) im Hinblick auf die geltenden Bestimmungen des Datenschutzes und die gesetzlichen und betrieblichen Anforderungen an die Datensicherheit.

Diese Dienstvereinbarung soll dazu dienen, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Maßnahmen ein Sicherheitsniveau der installierten IT-Systeme zu erreichen, um insbesondere jeden durch einen ordnungsgemäßen Umgang mit den IT-Systemen vermeidbaren Schaden fernzuhalten und zwar sowohl Schäden an den IT-Systemen selbst, als auch Schäden durch Datenverlust oder die Verletzung des Datenschutzes sowie Datenmissbrauch durch Dritte.

Die nachfolgenden Regelungen stellen für die Benutzer*Innen verbindliche Rahmenbedingungen für einen sicheren Umgang mit den ihnen überlassenen IT-Systemen an die Hand dar.

2 Geltungsbereich

Diese Dienstvereinbarung gilt für alle Beschäftigten der Stadtverwaltung Göppingen, der Eigenbetriebe der Stadt (außer Stadtwerke) und der Stiftung Kinderheim Wieseneck.

Die Regelungen dieser Dienstvereinbarung gelten nach entsprechender Unterweisung durch die IuK.

Zugriffe auf die IT-Systeme der Stadt Göppingen werden ausschließlich durch die IuK genehmigt. Wird Fremdfirmen ohne vorherige Genehmigung der IuK ein Zugriff auf IT-Systeme der *Stadt Göppingen* gewährt, so hat die Auftrag erteilende Stelle, dafür zu sorgen, dass die Regelungen dieser Dienstvereinbarung auch von Dritten eingehalten werden.

Die Dienstvereinbarung ersetzt alle voran ergangenen Dienstanweisungen und Dienstvereinbarungen.

3 Begriffsbestimmung IT-System

Unter dem Begriff **informationstechnisches System** (abgekürzt IT-System) wird jegliche Art elektronischer, datenverarbeitender Systeme und Programme verstanden. Hierunter fallen:

- alle IT-Systeme, die im Bereich der Stadtverwaltung Göppingen in Verbindung mit der ITEOS eingesetzt werden
- alle sonstigen IT-Systeme, die im Bereich der Stadtverwaltung Göppingen unabhängig (autonom) bzw. sowohl unabhängig als auch in Verbindung (teilautonom) mit anderen Netzen und zur ITEOS eingesetzt werden
- alle mobilen Endgeräte die aufgrund ihrer Größe und ihres Gewichts ohne größere körperliche Anstrengung tragbar und somit mobil einsetzbar sind. Dies umfasst insbesondere alle städtischen Mobiltelefone, Tablets und Notebooks
- alle weiteren IT-Systeme der Stadtverwaltung Göppingen die der Informationsverarbeitung dienen. Hierzu zählen insbesondere Serversysteme, Datenbanksysteme, digitale Anrufbeantworter, Videokonferenzsysteme und diverse Kommunikationssysteme
- alle Hilfsgeräte (Peripherie), die an o.g. Systemen angeschlossen werden können, wie z. B., Drucker, Übertragungseinrichtungen, GPS Tracking, Gebäudeleittechnik, Schließanlagen, Alarmanlagen, AV Übertragungstechnik
- alle Software als Sammelbegriff für Programme und die dazugehörigen Daten sowie alle Verfahren, die entweder durch Mitarbeiter der Stadtverwaltung Göppingen oder von Dritten erstellt wurden und in IT-Systemen zur Be-/Verarbeitung von Daten/Informationen eingesetzt werden
- Auch das Internet wird in seiner Gesamtheit als informationstechnisches System definiert

4 Zuständigkeiten und Verantwortungsbereiche

4.1 Oberbürgermeister

Der Oberbürgermeister ist verantwortlich für die Festlegung der Grundsätze der Informationsverarbeitung und die Freigabe von Verfahren.

4.2 Referat IuK

Für die Organisation des Einsatzes aller IT-Systeme ist grundsätzlich das Referat IuK zuständig.
Die Administration wird zentral in der Hauptverwaltung durch die Mitarbeiter des Referats IuK wahrgenommen oder durch das Referat IuK an Dritte vergeben. Die Mitarbeiter des Referates IuK sind für das Funktionieren und die Sicherung der zum dienstlichen Zweck erforderlichen IT-Systeme der Stadt Göppingen sowie für die Verbindung zu Rechnern des ITEOS und darüber hinaus zu weiteren Rechnern und Netzen (Landesverwaltungsnetz, Intranet und Internet) verantwortlich.
Die sich durch die private Nutzung ergebenden Aufgabenstellungen fallen nicht in den Verantwortungsbereich des Referates IuK (z.B. Sicherung privater Dateien).

4.3 Datenschutzbeauftragter

Der behördlich bestellte Datenschutzbeauftragte hat die Aufgabe, die Mitarbeiter der Organisation in Datenschutzangelegenheiten zu beraten und die Einhaltung der Datenschutzvorschriften in der öffentlichen Stelle zu überwachen. Er ist bei der Erfüllung seiner Aufgaben dem Oberbürgermeister direkt unterstellt und weisungsfrei.
Die einzelnen Aufgaben des behördlichen Datenschutzbeauftragten ergeben sich aus § 10 LDSG.
Anfragen an den Datenschutzbeauftragten können über die E-Mail datenschutz@goeppingen.de direkt, ohne Einhaltung des Dienstweges gestellt werden.

4.4 EDV-Ansprechpartner (Multiplikator/ Fachadministrator)

In größeren Organisationseinheiten können in Absprache mit dem Referat IuK und dem Referat Orga zusammen mit der jeweiligen Fachbereichsleitung, EDV- Beauftragte für die Unterstützung vor Ort benannt werden. Die EDV-Beauftragten arbeiten eng mit dem Referat IuK zusammen und halten sich an die vorgegebenen Direktiven.
Den EDV-Beauftragten obliegt insbesondere die Erledigung der folgenden Aufgaben:

- Zusammenarbeit mit dem Referat IuK
- Ansprechpartner für die Mitarbeiter vor Ort
- Behebung einfacher Störungen (Quick Support)
    - Z.B. Austausch von Tonerkassetten
- Qualifizierte Meldung von Störungen an den Benutzerservice

5 Benutzungsbestimmungen

5.1 Grundsätze

Für die Nutzung der IT-Systeme gelten grundsätzlich folgende Bestimmungen:

(1) Die eingesetzten IT-Systeme sind für den dienstlichen Gebrauch vorgesehen. Die private Nutzung ist unter dem Vorbehalt des Widerrufs zulässig, soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit der IT-Systeme für dienstliche Zwecke nicht beeinträchtigt werden und die private Nutzung keine negativen Auswirkungen auf die Bewältigung der Arbeitsaufgaben hat.
(2) Unzulässig ist jede Nutzung, die geeignet ist, der Behörde oder deren Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Gesetze und Verordnungen, insbesondere gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstößt.
(3) Die Benutzer sind für den Einsatz und den ordnungsgemäßen Gebrauch der ihnen überlassenen IT-Systeme verantwortlich
(4) Im Rahmen der Nutzung ist zu gewährleisten, dass die IT-Systeme vor unbefugter, unsachgemäßer und missbräuchlicher Benutzung geschützt sind und auf Betriebsunterlagen und Programme nicht unberechtigt zugegriffen werden kann.
(5) Bei der Verarbeitung personenbezogener Daten sowie Dienst- und Geschäftsgeheimnissen ist zu verhindern, dass Unbefugte Einblick in die laufende Datenverarbeitung haben.
(6) Personenbezogene oder schützenswerte Daten auf elektronischen Datenträgern (z. B. PCs, Notebooks oder mobilen Datenträgern) sind durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, beispielsweise durch

Verschlüsselung. Anfragen hierzu bitte an hotline-it@goeppingen.de.

(7) Alle sicherheitsrelevanten Ereignisse, wie z. B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verdacht auf Missbrauch der eigenen Benutzerkennung sind unverzüglich dem Referat IuK zu melden

(8) Für die Durchführung dienstlicher Aufgaben dürfen nur zugelassene und vom Referat IuK installierte Soft,- und Hardware verwendet werden.

(9) Der Anschluss privater Systeme an dienstliche IT-Systeme ist verboten.

(10) IT-Systeme dürfen außerhalb der Dienstgebäude nur eingesetzt werden, wenn diese für diesen Zweck vorgesehen sind (z. B. mobile Endgeräte)

(11) Bei Arbeitsunterbrechungen und beim Verlassen des Arbeitsplatzes ist eine Bildschirmsperre mit Passwortschutz zu aktivieren.

(12) Nach Abschluss der Arbeiten sind alle Ausdrucke aus dem Drucker, Fax und zentralem Kopiersystem zu entfernen.

5.2 Zugangs- und Zugriffsberechtigungen

(1) Jeder Benutzerzugang zu IT-Systemen muss durch ein Passwort, das nur dem jeweiligen Nutzer bekannt ist, geschützt werden. Bei Ausscheiden des Mitarbeiters wird dessen Zugang und Passwort gelöscht.

(2) Die Weitergabe und das Zur-Verfügung-stellen von personenbezogenen Benutzerkennungen (Accounts) und der dazugehörigen Authentifizierungshilfsmittel (z. B. Passwort) an andere Personen (auch Administratoren) ist verboten.

(3) Das Ausspionieren von Zugangsdaten als auch das Ausprobieren, ob weitere Dienste und Zugriffsrechte genutzt werden können, ist verboten.

(4) Für Abwesenheiten ist im Bedarfsfall eine Abwesenheitsnotiz einzurichten. Sollte dies nicht durch den Nutzer selbst möglich sein, ist ein Auftrag hierzu über den Vorgesetzten an hotline-it@goeppingen.de zu richten. Ausgenommen hiervon sind die Postfächer des Personalrats.

(5) Zu Räumen, in denen zentrale IT-Systeme (z.B. Server, Netzwerkkomponenten) installiert sind, dürfen nur Mitarbeiter der IuK und deren beauftragte Dritte Zugang erhalten.

(6) Unbesetzte Räume mit IT-Systemen sind zu verschließen.

(7) Außenstehende Personen, die Zugriff auf IT-Systeme haben dürfen sich nicht ohne Begleitung oder Beaufsichtigung eines verantwortlichen Mitarbeiters in Büroräumen aufhalten, außer es liegt eine zweckgebundene Freigabe durch das Referat IuK vor.

(8) Die Einrichtung und der Betrieb eines nicht durch die Stadtverwaltung Göppingen bereitgestellten Anschlusses an ein öffentliches Netz (z. B. durch Modem-, DSL- oder drahtlose Netzwerkverbindungen) ist nicht zulässig.

5.3 Einsatz von Software

(1) Vor Beschaffung von neuer Software muss ein durch das Referat IuK vorgegebenes Freigabeverfahren durchgeführt werden.

(2) Nicht freigegebene Software darf nicht eingesetzt werden.

(3) Software darf nur durch Mitarbeiter des Referates IuK oder von diesen autorisierten Personen unter Beachtung der lizenzrechtlichen Bestimmungen installiert werden. Das eigenmächtige Einspielen von Software oder die Beauftragung von

Dritten ohne Genehmigung des Referates IuK ist verboten.

(4) Die Nutzung von der Stadt Göppingen lizenzierter Software ist nur im Rahmen der unter Kapitel 5.1 Absatz (1) definierter Grundsätze gestattet.

(5) Das Kopieren von dienstlich zur Verfügung gestellten Programmen auf private IT-Systeme und die Weitergabe von Software an Dritte ist grundsätzlich unzulässig. Ausnahmen bedürfen der Zustimmung des Referates IuK und Zentrale Dienste

(6) Die Originaldatenträger und Dokumentationen von Software werden vom Referat IuK zentral verwahrt. Benutzerhandbücher und Handbücher auf CD-ROM können bei den Fachämtern verbleiben.

5.4 Internet und E-Mail

Die Stadtverwaltung Göppingen nutzt die elektronischen Medien wie z.B. Internet und E-Mail zum Austausch von Nachrichten und Dokumenten sowohl im verwaltungsinternen als auch im externen Verkehr.
Um bei der Nutzung der o. g. Kommunikationsdienste einen reibungslosen Betrieb und einen ordnungsgemäßen Verwaltungsablauf sicher zu stellen, werden nicht zuletzt wegen der damit verbundenen datenschutzrechtlichen und sicherheitsrelevanten Aspekte in der vorliegenden Dienstvereinbarung entsprechende innerdienstliche Regelungen getroffen. Bei einer privaten Nutzung des dienstlichen E-Mail-Kontos ist die in der Anlage 1 beigefügte Erklärung zu unterschreiben.

5.4.1 Allgemeine Hinweise Internetzugang

IT-Systeme, die an das LAN der Stadtverwaltung Göppingen angeschlossen sind, haben ausschließlich über den Provider der Stadtverwaltung Göppingen Zugang zum Internet. Dieser Zugang bietet ein Höchstmaß an Sicherheit gegen Angriffe von außen. Andere Zugangsarten sind nicht erlaubt.

Aus Wirtschaftlichkeits- oder IT-Sicherheitsgründen kann die Internetnutzung beschränkt werden. Dies kann beispielsweise folgendes beinhalten:

- Sperrung bestimmter Dienste der Internetnutzung (unter Berücksichtigung von 5.1 (1) sowie 5.7.2 Nr.2)
- Reduzierung auf bestimmte Internetanschlüsse,
- Beschränkung des Massendatentransfers oder des Speicherplatzes

Die bei der Nutzung der Internetdienste anfallenden personenbezogenen Daten dürfen nicht zur Leistungs- und Verhaltenskontrolle verwendet werden. Sie dürfen nur zu den in 5.7.2 Nr.2 genannten Zwecken unter Berücksichtigung der einschlägigen datenschutzrechtlichen Vorschriften verwendet werden.

5.4.2 Nutzungsbeschränkungen des Internetzugangs

Die Nutzung des Internets ist nur im Rahmen der unter Kapitel 5.1 Absatz (1) definierter Grundsätze gestattet. Unzulässig ist insbesondere:

(1) Das Abrufen, die Übertragung, Verbreitung und Speicherung von Daten, die gegen Gesetze (z.B. datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen) verstoßen

(2) die Übertragung, Verbreitung und Speicherung von beleidigenden, verleumderi-

schen, verfassungsfeindlichen, rassistischen, gewaltverherrlichenden oder pornographischen Inhalten oder Abbildungen soweit dies nicht aus dienstlichen Gründen erforderlich ist.

(3) Das Abrufen von für die Stadtverwaltung Göppingen kostenverursachenden, dienstlichen Informationen oder Inhalten aus dem Internet ist bei der zuständigen Behörde / Dienststelle zu beantragen und bedarf der Genehmigung durch den jeweiligen Dienststellen- oder Fachbereichsleiter

(4) Das Abrufen von Informationen oder Inhalten, die für die Stadtverwaltung Göppingen Kosten verursachen, ist für den Privatgebrauch unzulässig.

(5) Im Rahmen der privaten Nutzung dürfen keine kommerziellen oder sonstigen geschäftliche Zwecke verfolgt werden

(6) Das Speichern von privaten Filmen, Bild-, Spiel- und Musikdateien. Werden derartige Dateien empfangen, sind diese sofort vom Mitarbeiter zu löschen. Dies gilt nicht für Endgeräte, die gemäß 5.5.2 c) genutzt werden.

(7) die Abwicklung privater Rechtsgeschäfte, insbesondere die Nutzung von Zahlungsfunktionen (Onlinebanking, Internetversandhandel, eBay o.ä.) über einen dienstlichen Account oder

(8) die Nutzung von Onlinespieleplattformen

(9) Der Versuch, Beschränkungen zu verändern oder zu umgehen oder sich höhere Sicherheitsprivilegien zu verschaffen sowie Jegliche Maßnahmen die die Sicherheit des Stadtverwaltungsnetzes beeinträchtigen

(10) Die Manipulation von Sicherheitsmechanismen der Stadtverwaltung Göppingen

(11) Urheberrechtlich geschützte Dateien, für die keine Lizenz vorhanden ist, dürfen nicht abgerufen und gespeichert werden.

(12) Das Abrufen und die Installation von Treibern, Setup-Programmen oder ähnlicher systemeingreifender Software, die von der IuK zentral verwaltet werden.

(13) Das sorglose Ausführen von aktiven Inhalten (z.B. Makros) in heruntergeladenen Dokumenten.

(14) Die ferngesteuerten Zugriffe oder Steuerungen von IT-Systeme über sogenannte Remote-Anwendungen. Der dienstliche Bedarf für Remote-Zugriffe muss beim Referat 14 IuK unter Angabe der Gründe beantragt werden.

(15) Die Internet-Telefonie und Bildtelefonie (z.B. Skype). Ausnahmen für den dienstlichen Gebrauch sind beim Referat 14 IuK zu beantragen und nur mit der dafür zur Verfügung gestellten Software zulässig. Dies gilt nicht für Endgeräte, die gemäß 5.5.2 c) genutzt werden.

5.4.3 Allgemeine Hinweise E-Maildienst

Über die dienstlichen E-Mail-Adressen eingehende private E-Mails sind wie private schriftliche Post zu behandeln. Eingehende private, aber fälschlich als Dienstpost behandelte E-Mails sind den betreffenden Benutzern unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben. Private E-Mails sind umgehend aus dem dienstlichen Postfach zu löschen.

Jedes dienstliche E-Mail muss mindestens eine Signatur mit folgendem Aufbau in Schriftgröße 12pt Arial enthalten:

Freundliche Grüße

[Vorname] [Nachname]

Stadtverwaltung Göppingen
[Stellenbezeichnung] (z.B. Leiter Referat IuK-Technik und Zentrale Dienste)

z.B. Hauptstr. 1
z.B. 73033 Göppingen

Tel.: 07161 650-Durchwahl
Fax: 07161 650-Durchwahl
E-Mail: Emailname@goeppingen.de
www.goeppingen.de

Diese Nachricht enthält vertrauliche und/oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind oder diese Nachricht irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese Nachricht. Das unerlaubte Kopieren sowie die unbefugte Weitergabe dieser Nachricht ist nicht gestattet.

Die Dienststelle regelt insbesondere den Einsatz des Abwesenheitsagenten:

Guten Tag, vielen Dank für Ihre Nachricht.
Leider kann ich ihre Nachricht nicht direkt beantworten. Ich bin ab dem xxxx wieder erreichbar und werde dann Ihre Nachricht umgehend bearbeiten.

In dringenden Fällen wenden Sie sich bitte an ….

freundliche Grüße
Vorname Nachname

Mit Beendigung des Beschäftigungsverhältnisses steht die E-Mail-Adresse der jeweiligen Benutzer nicht mehr für diesen zur weiteren Nutzung zur Verfügung. Die Benutzer sind angehalten, ihre außerbetrieblichen Kommunikationspartner über diesen Umstand zu informieren.

Dienstliche E-Mails werden an, einen durch den fachlichen Vorgesetzten benannten Mitarbeiter, weitergeleitet. Ist ein privater Charakter des Inhaltes dieser weitergeleiteten E-Mail ersichtlich, ist die E-Mail ohne weitere Kenntnisnahme des Inhaltes durch diesen Benutzer zu löschen.

5.4.4 Nutzungsbeschränkungen des E-Maildienstes

Die Nutzung des E-Maildienstes ist nur im Rahmen der unter Kapitel 5.1 Absatz (1) definierter Grundsätze gestattet. Unzulässig ist insbesondere:

(1) Die Übertragung von externen, ein- und ausgehenden E-Mails nebst Datei-

Anhängen mit einem Transfervolumen von über 20 MB. Dieses ist durch das ITEOS begrenzt.

(2) Jede Form des Verbergens, Veränderns oder der Fälschung der eigenen Identität in E-Mail Nachrichten

(3) Die Erzeugung oder die Weiterleitung von Kettenbriefen oder Briefen mit Schneeballsystem

(4) Das Öffnen unbekannter, auffälliger E-Mails. Dies umfasst insbesondere das Ausführen von Links oder das Öffnen von Dateianhängen.

(5) Das Antworten und/oder die Weiterleitung von sog. SPAM-Mails. SPAM-Mails müssen ungelesen gelöscht werden

5.5 mobile Endgeräte und mobile Datenträger

5.5.1 Beantragung

Die Beantragung und Genehmigung eines mobilen Endgerätes zum Dienstgebrauch erfolgt über die jeweilige Fachbereichsleitung. Zusätzlich ist für die Genehmigung eines Smartphones (z.B. iPhone), mit Zugriff auf Internet und E-Maildienste, die Zustimmung des Oberbürgermeisters erforderlich.

Die Beantragung erfolgt über das Formular „Beschaffungsantrag mobile Endgeräte“.

5.5.2 Gebühren

Für die Gebührenabrechnung mobiler Endgeräte werden die folgenden Nutzergruppen entsprechend der Nutzung unterschieden und entsprechend abgerechnet.

a) **Handybenutzer mit ausschließlich dienstlicher Nutzung**
Es werden keine Kosten in Rechnung gestellt

b) **Smartphone (IPhone) Benutzer oder Nutzer einer Datenflat (z.B. Surfstick, und /oder Notebook/ Tablet mit SIM) mit ausschließlich dienstlicher Nutzung**
Es werden keine Kosten in Rechnung gestellt.

c) **Smartphone (IPhone) Benutzer oder Nutzer einer Datenflat (z.B. Surfstick, und /oder Notebook/ Tablet mit SIM) mit anteiliger privater Nutzung**
Da die Nutzung vorrangig im allgemeinen betrieblichen Interesse des Arbeitgebers liegt werden keine Kosten in Rechnung gestellt.

Die Smartphone Verträge werden grundsätzlich ohne Auslandsnutzungsoption abgeschlossen. Diese kann aber auf Antrag hin mit aufgenommen werden.

Die bei der Nutzung von Sonderdiensten (Sonderrufnummern) anfallenden Gebühren werden der Dienststelle in Rechnung gestellt, welcher der Smartphone Vertrag zugeordnet ist.

5.5.3 Nutzung mobiler Endgeräte

Für die Nutzung der mobilen Endgeräte gelten grundsätzlich folgende Bestimmungen:

(1) Der Einsatz der mobilen Endgeräte mit Mobilfunkzugang ist im Ausland aus Kostengründen (Roamingkosten in ausländischen Netzen) grundsätzlich untersagt außer ein entsprechender Datentarif steht zur Verfügung.
(2) Die Weitergabe des Geräts an unbefugte Dritte ist nicht zulässig.
(3) Der Verlust eines mobilen Endgerätes ist umgehend beim Referat 14 IuK als auch bei dem jeweiligen Vorgesetzten zu melden. Aus Sicherheitsgründen wird das mobile Endgerät automatisch gesperrt.
(4) Der Benutzerzugang zu einem mobilen Endgerät muss durch eine PIN oder Passwort, der nur dem jeweiligen Nutzer bekannt ist, geschützt werden.
(5) Bei Inaktivität ist automatisch eine passwortgeschützte Sperrung zu aktivieren. Der Zeitraum der Inaktivität bis zur Sperrung sollte nicht mehr als 5 Minuten betragen
(6) Sämtliche Funk- (WLAN, Bluetooth etc.), Infrarot- und andere Kommunikationsschnittstellen werden deaktiviert, sofern diese nicht benötigt werden.
(7) Die Nutzer von mobilen Endgeräten müssen dafür sorgen, dass diese für unberechtigte Dritte unzugänglich aufbewahrt werden und nicht unkontrolliert gelagert oder transportiert werden. Dem Verlust oder Diebstahl ist mit höchstmöglicher Sorgfalt entgegenzuwirken. (Auch in verschlossenen Fahrzeugen dürfen Geräte nicht sichtbar gelagert werden).
(8) Sollten dienstliche Daten bei einer mobilen Nutzung auf den lokalen Laufwerken anfallen, müssen diese eigenverantwortlich und so früh wie möglich auf die zentralen Verzeichnisse übernommen werden.
(9) Die Datensicherung und Rücksicherung auf lokalen Datenträgern liegt in der Verantwortung der Mitarbeiter. Diese Datenbestände werden nicht von den Sicherungsroutinen des Referat IuK erfasst, so dass bei technischen Problemen oder Tausch der Hardware ein Datenverlust eintreten kann.

5.5.4 Nutzung von mobilen Datenträgern (externe Datenspeicher)

(1) Datenträger (wie z. B. USB-Sticks, Memory-Karten, CDs, DVDs) mit personenbezogenen Daten oder Programmen dürfen nur von Berechtigten befördert und benutzt werden.
(2) Datenträger, die vorübergehend nicht verwendet werden, sind einzuschließen, so dass sie vor unbefugtem Zugriff geschützt sind. Werden Datenträger auf Dauer nicht mehr benötigt, sind diese im Referat IuK abzugeben.
(3) Datenträger mit Originaldaten müssen besonders gesichert aufbewahrt werden (z. B. in einem Tresor oder einem abschließbaren Schrank).
(4) Vertrauliche Arbeitsergebnisse auf mobilen Datenträgern sind nur an den berechtigten Empfänger und gegen Nachweis auszugeben.
(5) Daten von mobilen Datenträgern dürfen erst nach Überprüfung auf Virenbefall eingespielt werden.
(6) Jeder Benutzer hat einen Datenträgernachweis zu führen. In diesem sind alle Datenträger nachzuweisen und Zu- und Abgänge mit Angaben zu den übergebenden bzw. übernehmenden Personen, zum Speicherinhalt und zum Anlass

des Datenträgertransports zu vermerken. Bei zentral verwalteten Datenträgern übernimmt dies das Referat IuK und Zentrale Dienste.

(7) Datenträger sind eindeutig zu beschriften. Die Beschriftung muss den Eigentümer, den Inhalt, den Status (Original-, Sicherungs- oder Arbeitsdaten) und das Erstellungsdatum ausweisen.

(8) Sicherungskopien sind getrennt vom Originalbestand in einem für Unbefugte unzugänglichen Raum in feuer- und wassergeschützten Sicherheitsbehältnissen aufzubewahren.

5.5.5 Außerbetriebnahme

Vor Außerbetriebnahme sind bei Bedarf die auf dem Gerät gespeicherten Daten entsprechend zu sichern.

5.5.6 Einstellungen und Auslieferungszustände verwaltungsinterne Smartphones (iPhones) & Tablets (iPad)

Die nachfolgenden Erläuterungen zeigen die durch die IuK bei Auslieferung der Geräte vorgenommenen datenschutzkonformen Einstellungen und deren Wirkungsweise.

Der Nutzer hat die Möglichkeit das Gerät entsprechend der gewünschten Privatnutzung zu konfigurieren.

Einstellungen, Apps oder Fotos, die der Benutzer im Rahmen seiner Privatnutzung zusätzlich auf das Gerät bringt dürfen von der IuK nicht verändert, gesichert oder gesichtet werden.

Die IuK hat daher bestimmte Apps als Basis Apps vorgesehen, die zum dienstlichen Betrieb notwendig sind und die dann auch durch die IuK möglichst vollautomatisiert aktuell gehalten werden.

5.5.6.1 **Definition „betreute iPhones“**

Sie finden in den Geräteeinstellungen den Hinweis auf die Betreuung durch die IuK.

Der Hinweis bedeutet, dass die IuK während der Standardeinrichtung bei Auslieferung alle Geräte über einen zentralen Konfigurationsserver (MDM) eingerichtet und in einer Grundinstallation Basis Apps installiert hat.

Im Konfigurationsserver ist für jedes durch die IuK betreute iPhone einmalig das Gerät zum Auslieferungszustand hinterlegt. D.h. es werden Grundeinstellungen (z.B. WLAN Einstellungen), Basis Apps, und der Gerätename mit Nutzer gespeichert.

Damit sollen folgende Administrationstätigkeiten für den Nutzer vereinfacht werden:

- Regelmäßige Updates der Basis Apps
- WLAN Einstellungen für das Rathaus WLAN bleiben erhalten
- Schnelle Einrichtung eines Ersatzgerätes bei z.B. Verlust, Defekt, …

Die durch die IuK vorgegebenen Einstellungen können durch den Nutzer auf die eigenen Bedürfnisse hin angepasst und vereinzelt deaktiviert werden.

Jede neue App, die automatisiert aufgespielt werden soll wird vorher durch den Datenschutzbeauftragten geprüft und freigegeben.

5.5.6.2 **Was kann die IuK?**

Auf den durch die IuK betreuten Geräten kann die IuK:

- Apps und Updates automatisch aufspielen
- Durch die IuK verwaltete Basis Apps löschen

5.5.6.3 **Die IuK kann nicht!**

1. auf das iPhone/iPad aufschalten,
2. auf dem iPhone/iPad gespeicherte Daten lesen, verändern oder löschen,
3. den Internet- oder E-Mail-Verkehr des iPhone/iPad überwachen oder mitlesen oder
4. das iPhone/iPad orten.

Wichtig:
Auch bei Verlust des iPhones/ iPads ist es nicht möglich das Gerät zu finden und/oder aus der Ferne zu löschen.

5.6 Nutzung WLAN Hotspots Stadtverwaltung Göppingen

5.6.1 WLAN Hotspots

Es gibt zwischenzeitlich in verschiedenen Gebäuden der Stadt einen Zugriff auf das WLAN System der Stadt Göppingen in das sich die Geräte automatisch einloggen wir z.B. im Rathaus.

5.6.2 Verbindung iPhone/ iPad zum WLAN Hotspot

Bei den durch die IuK betreuten Geräten werden standardmäßig alle notwendigen Einstellungen in der Grundkonfiguration für das WLAN bereits voreingestellt.

Findet ein Gerät eine WLAN Verbindung an einem der Standorte, dann können evtl. anstehende Updates etc. automatisiert auf die Geräte übertragen werden.

Es findet keine „Fernwartung“ oder ein unbemerktes Aufschalten durch die IuK auf die Geräte statt.

Die Updates laufen vollautomatisch.

5.7 Firewall

Unter einer Firewall ist ein organisatorisches und technisches Konzept zur Trennung und Abschirmung von Netzbereichen aus Gründen der IT-Sicherheit zu verstehen. Als Schnittstelle zwischen einzelnen Netzen, kontrolliert die Firewall den Netzwerkverkehr zwischen den Netzen, um ungewünschten Verkehr zu verhindern und nur bestimmte, im Vorfeld definierte Zugriffe zu gestatten.

Zu den zentralen Aufgaben eines Firewall Systems gehören zum einen die Reglementierung von Kommunikationsbeziehungen zwischen unterschiedlichen Schutzniveaus (Beschränkung von Netzdiensten um eine Vermischung unterschiedlicher Netze zu vermeiden) und zum anderen die Überwachung der ausgetauschten Daten (Protokollierung und Analyse des Datenverkehrs 5.7.2).

Die Stadtverwaltung Göppingen setzt hierfür ein „managed Firewall“ System des Rechenzentrums ein.

5.7.1 Änderungen des Regelwerks (Webfilter)

1. Jede Änderung am Regelwerk der Firewall darf nur auf Antrag erfolgen. Der Antrag bedarf der Schriftform, wobei auch die elektronische Form durch Verwendung von E-Mails, benutzt werden kann. Der Antrag muss durch den jeweiligen fachlichen Vorgesetzten erstellt und versandt werden.

2. Ein Antrag auf Änderung des Regelwerks muss unter Angabe der fachlichen Gründe, über den jeweiligen fachlichen Vorgesetzten an die hotline-it@goeppingen.de, gerichtet werden. Der Referatsleiter der IuK entscheidet über die Durchführung der beantragten Änderung des Regelwerks.

3. In strittigen Fällen, in denen der Referatsleiter IuK und der Antragsteller über eine Lösung bezüglich einer Änderung des Regelwerks keine Einigung erzielen können, wird der Vorgang an den Datenschutzbeauftragten zur Klärung weitergeleitet. In diesem Fall leitet der Referatsleiter IuK diesen Antrag zusammen mit einer kurzen Einschätzung, inwieweit die Sicherheit des Firewall-Systems durch die gewünschte Änderung beeinflusst wird, an den Datenschutzbeauftragten und den PR zur Entscheidung weiter.

4. In begründeten Notfällen kann der Antrag auch mündlich gestellt werden. Wenn der Referatsleiter IuK keine wesentliche Beeinträchtigung der Sicherheit feststellt, kann die gewünschte Änderung vorläufig sofort vorgenommen werden. Der Antragsteller muss in diesem Fall so schnell wie möglich den Antrag in Schriftform nachreichen.

5. In bestimmten Ausnahmefällen kann für einen festgelegten Zeitraum die mündliche Antragstellung zwischen dem Referatsleiter IuK und dem Antragsteller vereinbart werden. Die Vereinbarung über den festgelegten Zeitraum muss unter Angabe der Gründe schriftlich dokumentiert und der Personalvertretung zeitnah bekannt gegeben werden. Wenn innerhalb von fünf Tagen nach Bekanntgabe die Personalvertretung nicht widerspricht, gilt die Vereinbarung als zugestimmt.

5.7.2 Protokollierung und Auswertung

Die Protokollierung erfolgt im Rahmen der unter Kapitel 6 beschriebenen Grundsätze.

1. Kommunikation, die das Regelwerk der Firewall zulässt, wird protokolliert.

2. Unzulässige Zugriffsversuche werden einer automatischen, systembedingten Protokollierung der sicherheitsrelevanten Vorgänge unterzogen. Die Protokolle werden dabei ausschließlich zu Zwecken

   - der Gewährleistung der Systemsicherheit, insbesondere der Sicherung der zu schützenden Netze vor unbefugten Zugriffen bzw. unbefugter Kommunikation,
   - der Analyse und Korrektur technischer Fehler,
   - der technischen Optimierung des Netzes und der im Netz angebotenen Dienste (optimale Kapazitätsauslegung, angemessene Wartezeiten) sowie
   - der Aufklärung bei Vorliegen eines konkreten Verdachts missbräuchlicher Nutzung der Internetdienste gemäß den in dieser Dienstvereinbarung (siehe 5.4.2) festgelegten Regelungen

   verwendet.

5.8 Nutzung Videokonferenzsystem

5.8.1 Allgemeines

Das in der Stadtverwaltung eingesetzte Videokonferenzsystem bietet unter Beachtung der Vorgaben dieser Dienstvereinbarung und dem Vorliegen entsprechender technischer Rahmenbedingungen (Internetzugang) die Möglichkeiten alle Besprechungsformate im Tagesgeschäft der Stadtverwaltung störungsfrei und ohne Abbrüche sowie datensicher durchführen zu können.

Die, durch die IuK getätigten Voreinstellungen dürfen nicht eigenständig abgeändert werden und stellen sicher, dass die Konferenzen immer im Geltungsbereich der EU-DSGVO, stattfinden. In Ergänzung dazu, setzt die datenschutzgerechte Nutzung des Systems auch die Einhaltung bestimmter Verhaltensregeln im Umgang mit dem Videokonferenzsystem voraus, die von allen Beschäftigten der Stadtverwaltung zwingend einzuhalten sind. Hinweise und Erläuterungen zur Umsetzung der Vorgaben und zur technischen Nutzung des Videokonferenzsystems erhalten Sie auch im Intranet auf den Seiten der IuK.

Wird Fremdfirmen die Durchführung einer Videokonferenz mit einer städtischen Videokonferenz Lizenz gewährt, so hat die Dienststelle, die den Auftrag erteilt, dafür zu sorgen, dass die Regelungen dieser Dienstvereinbarung auch von Dritten eingehalten werden.

5.8.2 Beschränkung des Teilnehmerkreises

Zur Wahrung der Vertraulichkeit von Wort und Bild in Veranstaltungen und Konferenzen und um Störungen bzw. Angriffe von außen zu vermeiden ist die Teilnehmer-

zahl in der Form zu begrenzen, dass nur Personen den Veranstaltungen beiwohnen können, die auch tatsächlich eingeladen wurden. Das bedeutet, dass ein Passwort mit der Einladung zu versenden ist (alternativ die „Warteraumoption“), um zu gewährleisten, dass nur berechtigte Personen teilnehmen.
Die Teilnehmenden sollten auch darauf hingewiesen werden, dass die Weitergabe der Login-Daten für eine Veranstaltung ausdrücklich verboten ist.
Die Teilnahme unerlaubter Dritter führt zum Abfluss von personenbezogenen Daten der, Teilnehmer, was von Seiten der Stadtverwaltung zwingend zu verhindern ist.

5.8.3 Einrichtung und Beantragung

Der Zugang zum Videokonferenzsystem muss über die IuK beantragt werden. Neue Mitarbeiter oder Namenswechsel werden über den bisherigen Prozess (Mitarbeiterstammdatenblatt) angezeigt und beantragt. Zur Registrierung wird ausschließlich die dienstliche E-Mail-Adresse verwendet. Mit dem Antrag wird auch der Umfang der zu nutzenden Funktionsumfang definiert. Es wird unterschieden in:

- Organisator
- Teilnehmer

Das Videokonferenzsystem wird automatisch auf den Dienstrechner installiert und aktualisiert – eigene Installationen sind gem. Kapitel 5.3 nicht zulässig.

Die private Nutzung ist im Rahmen der in Kapitel 5.1 beschriebenen Grundsätze geduldet.

5.8.4 Aufzeichnung Videokonferenz

Die Aufzeichnung einer Veranstaltung, Besprechung oder sonstiger Videokonferenz ist ohne Zustimmung aller Teilnehmer untersagt. Die Einholung der Zustimmung muss durch die die Dienststelle schriftlich im Vorfeld erfolgen, welche die Videokonferenz durchführt. Die Zustimmung der Teilnehmer ist entsprechend zu dokumentieren und zusammen mit der aufgenommenen Datei abzuspeichern.

5.8.5 Löschung von Protokollen, Chatverläufen

Nach einer Videokonferenz müssen die Chatverläufe und Protokolle einer Besprechung gelöscht werden. In einer Präsenzveranstaltung gibt es solche Protokolle nicht, weshalb dies keine Einschränkung darstellt. Zur Sicherung des Datenschutzes ist die Löschung zwingend.

5.8.6 Abschalten der Videofunktion für Teilnehmer

Bei den verwendeten Systemen kann jeder Teilnehmer für sich entscheiden, ob er ein Bild oder Ton sendet oder nicht. Wenn für die jeweilige Besprechung keine Notwendigkeit besteht, dass Teilnehmer mit Bild anwesend sind, sollen die Teilnehmer zu Beginn darauf hingewiesen werden, dass die Kamera des eigenen Endgerätes abgeschaltet werden bzw. bleiben kann.

Dies ist aus datenschutzrechtlicher Sicht, aber auch zur Minderung der verwendeten Bandbreite für die Veranstaltung sinnvoll.

5.8.7 Hintergrund & Namen der Teilnehmer

Das Videokonferenzsystem bietet die Möglichkeit, bei der Teilnahme an einer Konferenz den eigenen Hintergrund auszublenden oder ein eigenes Hintergrundbild anzuzeigen. Hierbei ist bei dienstlicher Nutzung nur die Auswahl eines Hintergrundbildes möglich, welches durch die Stadtverwaltung explizit für diesen Zweck zur Verfügung gestellt wird (dienstlicher Hintergrund).
Die offiziell zu nutzenden Hintergrundbilder werden dem User im Intranet zur Verfügung gestellt. Sollten Sie kein Bild als Hintergrund wählen, ist der Hintergrund durch Aktivieren der Funktion „Weichzeichnen“ unter dem Menüpunkt „Hintergründe & Filter“ auszublenden.
Bei dienstlicher Nutzung ist der Name nach folgendem Muster anzugeben: [Vorname] [Nachname].

5.8.8 Teilen des Bildschirms

Der Organisator (Host) einer Veranstaltung ist in der Lage, seinen Bildschirm mit allen Teilnehmern zu teilen und damit Inhalte seines PCs anzuzeigen. Hierbei hat der Teilende darauf zu achten, dass auf dem geteilten Bildschirm keine personenbezogenen Daten Dritter zu sehen sind. Sinnvoll ist es, auf dem geteilten Bildschirm nur die beabsichtigte Präsentation (o.ä.) zu öffnen und alle anderen Fenster zu schließen oder auf einem weiteren Bildschirm zu öffnen. Gegebenenfalls sollte die Freigabe auf einzelne Fenster beschränkt werden. Die Preisgabe von personenbezogenen Daten Dritter (z.B. durch das geöffnete E-Mail-Postfach) ist auszuschließen.

5.8.9 Stummschalten der übrigen Teilnehmer

Der Organisator (Host) einer Veranstaltung ist in der Lage, die Mikrofone der Teilnehmer stumm zu schalten. Dies ist sinnvoll, um eine Geräuschkulisse zu verhindern und zudem schützt es Teilnehmer vor der zufälligen Preisgabe personenbezogener Daten Dritter. Deshalb sollte der Host hiervon regelmäßig Gebrauch machen.

5.9 Datenschutz und Datensicherheit

Durch geeignete Maßnahmen ist der Schutz personenbezogener Daten unter Berücksichtigung der Vorschriften über den Datenschutz, insbesondere zur DSGVO und LDSG sicherzustellen.

5.9.1 Maßnahmen

(1) Die Zulässigkeit der Verarbeitung personenbezogener Daten richtet sich nach der DSGVO und LDSG
(2) Eine Datenerhebung und – Speicherung von personenbezogenen Daten „auf Vorrat“, d. h. für noch nicht festgelegte Zwecke, ist unzulässig.
(3) Verboten ist die Verarbeitung und Speicherung personenbezogener dienstlicher Daten auf privaten IT-Systemen.
(4) Der Nutzer ist für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich.

5.9.2 Datensicherung und Datenspeicherung

(1) Alle personenbezogenen, vertraulichen oder dienstlichen Daten müssen auf den zentralen Verzeichnissen der Stadtverwaltung Göppingen gespeichert werden soweit die infrastrukturellen, technischen Voraussetzungen für die Speicherung gegeben sind. In Ausnahmefällen kommt eine mit dem Referat 14 abgestimmte Sicherungsroutine zum Einsatz.

(2) Alle zentral verwalteten Datenbestände (Systemdaten, Anwendungsdaten, Protokolldaten, installierte Software) sowie Server und Router/ Switches, werden durch das Referat IuK regelmäßig gesichert.

(3) Die Kontrolle der Verfügbarkeit der Sicherungsdaten wird mindestens zweimal pro Jahr durch das Referat IuK geprüft.

(4) Die Datensicherung und Rücksicherung auf lokalen Datenträgern liegt in der Verantwortung der Mitarbeiter. Diese Datenbestände werden nicht von den Sicherungsroutinen des Referat IuK erfasst, so dass bei technischen Problemen oder Tausch der Hardware ein Datenverlust eintreten kann.

5.9.3 Umgang mit Passwörtern

Werden in einem IT-System Passwörter zur Authentifizierung verwendet, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, dass das Passwort korrekt gebraucht wird. Die Zeichenzusammensetzung des Passwortes muss so komplex sein, dass es nicht erraten oder durch einfaches Ausprobieren ermittelt werden kann. Folgende Regeln sind dabei zu beachten:

1. Passwörter sind nirgends zu notieren und niemandem mitzuteilen.
2. Das Passwort muss geheim gehalten werden und darf nur dem Benutzer bekannt sein.
3. Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben und Zahlen/Zeichen mit Sonderzeichen) zu gestalten.
4. Passwörter dürfen nicht leicht zu erraten sein. Vor- und Familiennamen oder Geburtstage sind beispielsweise nicht zur Bildung von Passwörtern geeignet. Es dürfen niemals Trivialpasswörter verwendet werden (z. B. 4711; 12345 oder andere nebeneinanderliegende Tasten).
5. Die Passwörter sind nach Aufforderung oder spätestens alle 90 Tage zu wechseln.
6. Sofern Gruppenpasswörter zwingend erforderlich sind, gilt: Gruppenpasswörter sind umgehend zu ändern, wenn die Zusammensetzung der Gruppe sich verändert. Gleiches gilt, wenn Passwörter unautorisierten Personen bekannt geworden sind.
7. Einmal genutzte Passwörter sind nicht wieder zu verwenden.
8. Benutzer haben den Empfang von Initial-Passwörtern immer zu bestätigen und müssen diese sofort wechseln.
9. Alle IT-Systeme sind zum Schutz vor unbefugten Personen zu sperren.
10. Passwörter dürfen nicht als Teil eines automatischen Anmeldeprozesses verwendet werden, z. B. in einer Makro- oder Funktionstaste

5.10 Entsorgung von IT-Systemen und Datenträgern

Die datenschutzkonforme Entsorgung von IT-Systemen und Datenträgern übernimmt das Referat IuK.

6 Protokollierung und Kontrollen

Protokolldaten sind personenbezogen, da sie Aufschluss über die Aktivitäten eines Benutzers geben. Sie unterliegen nach dem Datenschutzrecht einer strikten Zweckbindung (DSGVO, LDSG) und dürfen nur zum Nachweis der fehlerfreien und ordnungsgemäßen Datenverarbeitung oder zur Aufdeckung von missbräuchlichen Zugriffen oder Zugriffsversuchen, nicht jedoch für Zwecke der Verhaltens- oder Leistungskontrolle der Mitarbeiter verwendet oder ausgewertet werden. Eine pauschale, flächendeckende und „vorbeugende“ Protokollierung aller Aktivitäten der Mitarbeiter am IT-System zur Verhaltens- und Leistungskontrolle verboten.

6.1 Art und Umfang von Protokollierungen

Eine Unterscheidung von dienstlicher und privater Nutzung auf technischem Weg erfolgt nicht. Die Protokollierung und Kontrolle gemäß 5.7.2 Nr.2 erstrecken sich auch auf den Bereich der privaten Nutzung.
Die Benutzer erklären durch die Unterschrift der Anlage 1 ihre Einwilligung in die Protokollierung und Kontrolle im Sinne dieser Dienstvereinbarung.

Eine private Nutzung ohne diese Einwilligung ist verboten.

(1) Alle eingehenden E-Mails werden durch eine Firewall, einen Spam-Filter sowie lokal installierte Virenscanner geprüft.

(2) Die Verkehrsdaten für den Internetzugang werden mit Angaben von
- Datum / Uhrzeit, Adressen von Absender und Empfänger (z.B. IP-Adressen)
- Benutzeridentifikation (z.B. bei der Verwendung eines Proxy-Servers)
- der aufgerufenen Webseiten und
- übertragener Datenmenge protokolliert.

(3) Auswertungen der Protokolle nach Absatz (2) werden ausschließlich zu Zwecken der
- Analyse und Korrektur technischer Fehler
- Gewährleistung der Systemsicherheit
- Optimierung des Netzes
- statistischen Feststellung des Gesamtnutzungsvolumens
- Stichprobenkontrollen gemäß Absatz (4) gemacht.

(4) Die Protokolle werden durch einen durch die Referatsleitung bestimmten Mitarbeiter des Referats IuK bei Vorliegen eines Verdachtes des Befalls durch Schadsoftware stichprobenhaft hinsichtlich der aufgerufenen Internetseiten, aber nicht personenbezogen, gesichtet und in aggregierter Form, also ohne Nennung von Namen und anderen Identifizierungsmerkmalen, ausgewertet. Die

Auswertung der Übersicht des Gesamtdatenvolumens erfolgt monatlich ebenfalls durch diesen Mitarbeiter. Der Datenschutzbeauftragte und der Personalrat werden immer beteiligt.

(6) Die Protokolldaten werden nach 30 Tagen automatisch gelöscht.

Kontrolle und Auswertung von personenbezogenen Protokollen können sich auch auf die private Kommunikation erstrecken. Deshalb muss jeder Beschäftigte, der Internetdienste für private Zwecke nutzen möchte, eine persönliche Erklärung unterschreiben, mit der er in mögliche Eingriffe in das Fernmeldegeheimnis einwilligt, die mit den in Satz 1 genannten Maßnahmen verbunden sind, und die weiteren Rahmenbedingungen der Privatnutzung anerkennt. Einen entsprechenden Formulierungsvorschlag enthält die Anlage 1 dieser Dienstanweisung.

Maßgeblich ist die "Erforderlichkeit zur Aufgabenerfüllung". Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine datenschutzrechtliche Löschungspflicht.

7 Maßnahmen bei Verstößen

(1) Bei einem konkreten Verdacht auf missbräuchliche oder unerlaubte Nutzung des Internetzugangs (hervorgerufen beispielsweise durch ein erhöhtes Gesamtdatenvolumen oder auch die Kenntnisnahme nicht zulässiger im Internet angebotener Inhalte) gemäß Kapitel 5.4 dieser Vereinbarung durch einen Benutzer, erfolgt unter Beteiligung des Datenschutzbeauftragten, des Referat Recht und des Personalrats eine Überprüfung des Datenverkehrs durch den nach Kapitel 6.1 Abs. 4 bestimmten Mitarbeiter des Referats IuK.

(2) Sind weitere Untersuchungsmaßnahmen (z.B. Offenlegung der IP-Adresse des benutzten Arbeitsplatzes oder weitere Überprüfungen) notwendig, ist der betreffende Mitarbeiter sofort durch Referat IuK über die weiteren Untersuchungsmaßnahmen zu informieren. Auf der Basis dieser Untersuchung wird ein Bericht erstellt, der dem Betroffenen unter Beteiligung des Referats Personal ausgehändigt wird.

8 Inkrafttreten

(1) Diese Vereinbarung tritt mit Unterzeichnung in Kraft
(2) Die Vereinbarung kann von jedem Vertragspartner unter Einhaltung einer Frist von 3 Monaten gekündigt werden.
(3) Nach Eingang der Kündigung müssen unverzüglich Verhandlungen über eine neue Dienstvereinbarung aufgenommen werden.
(4) Bis zum Abschluss einer neuen Vereinbarung bleiben die Bestimmungen dieser Vereinbarung gültig.
(5) Sollten einzelne Bestimmungen dieser Dienstvereinbarung ungültig oder unwirksam sein, so bleiben die übrigen Teile dieser Dienstvereinbarung hiervon unberührt. Die unwirksame Bestimmung wird durch eine andere ersetzt, die dem Zweck der unwirksamen Regelung am nächsten kommt und ihrerseits wirksam ist.

Für die Dienststelle
Der Oberbürgermeister

gez.
Alex Maier

Für den Personalrat
Vorsitzender

gez.
Jürgen Horst

Anlage 1

Erklärung zur Nutzung der dienstlichen E-Mail-Adresse und des dienstlichen Internetzugangs

- ☐ **Ich habe die Dienstvereinbarung über die Nutzung der IT-Systeme zur Kenntnis genommen, wurde durch das Referat IuK unterwiesen und habe die Dienstvereinbarung verstanden.**

- ☐ **Ich möchte den Internetzugang und E-Maildienst in dem von der Dienstvereinbarung erlaubten Umfang auch privat nutzen.**

- ☐ **Ich habe Kenntnis, dass die Verfügbarkeit und Integrität der genannten Systeme nicht gesichert sind, also ausnahmsweise die Möglichkeit besteht, dass E-Mails nicht oder verspätet zugestellt werden.**

- ☐ **Mir ist bekannt, dass ich im Falle einer privaten Nutzung der dienstlichen E-Mail-Adresse meine Kommunikationspartner darauf hinzuweisen habe, dass es sich um ein dienstliches E-Mail-Postfach handelt und auch bei einer privaten Nutzung die Bedingungen nach Nr. 6 und 7 (Protokollierung, Missbrauchsregelung) der Dienstvereinbarung gelten.**

.....

Name, Vorname

.....

Ort, Datum

.....

Unterschrift Beschäftigte/ Beschäftigter

Erklärung zur Nutzung
eines mobilen Endgerätes

☐ **Ich nutze nachfolgend markierte(s) mobile(s) Endgerät(e):**

		Nutzung EU Ausland
☐	**Mobiltelefon**	☐
☐	**Smartphone (iPhone)**	☐
☐	**Notebook mit SIM**	☐
☐	**Tablet (Microsoft) mit SIM**	☐
☐	**Datenstick (UMTS Stick)**	☐
☐	**Datenoption Ausland**	☐

☐ **Ich habe die „Dienstvereinbarung über die Nutzung IT-Systeme" zur Kenntnis genommen und verstanden.**

☐ **Ich möchte das mobile Endgerät in dem von der Dienstanweisung erlaubten Umfang auch privat nutzen.**
Da die Nutzung vorrangig im allgemeinen betrieblichen Interesse des Arbeitgebers liegt werden keine Kosten in Rechnung gestellt.

.....
Name, Vorname

.....
Ort, Datum

.....
Unterschrift Beschäftigte/ Beschäftigter