Durchführungsrichtlinie zur IKT-Sicherheit
Version 1.0

Für die Unternehmung Wiener Krankenanstaltenverbund (KAV) sind auf Grundlage dieser Richtlinie die für diesen Bereich erforderlichen organisatorischen Anordnungen von der Generaldirektorin bzw. vom Generaldirektor sinngemäß zu treffen.

1. Begriffsbestimmungen

Die Begriffsbestimmungen des Erlasses „Sicherheit in der Informations- und Kommunikationstechnologie“ gelten sinngemäß. Darüber hinaus gelten folgende Begriffsbestimmungen:

Informationen und Daten
bilden den Inhalt und den Bedeutungsgehalt einer Nachricht ab. Informationen können in verschiedenen Formen vorliegen:

- ausgedruckt auf Papier
- elektronisch gespeichert
- auf dem Postweg oder elektronisch übertragen
- in Filmen oder Bildern gezeigt
- in Gesprächen mündlich weitergegeben

Daten im Sinne dieser Richtlinie sind Informationen, die in elektronischer Form vorliegen.

IKT-Dienstleisterin bzw. IKT-Dienstleister
ist eine von der IKT-Dienststelle beauftragte externe Stelle.

Externe Stelle (in der Folge auch Externe genannt)
Darunter sind Dienstleisterinnen bzw. Dienstleister zu verstehen, die sowohl juristische als auch natürliche Personen sein können. Z.B. IKT-Dienstleisterinnen bzw. IKT-Dienstleister, Entwicklerinnen bzw. Entwickler, Lieferantinnen bzw. Lieferanten, z.B. von Softwareprodukten und IKT-Systemen, sowie vorübergehend beschäftigte Mitarbeiterinnen und Mitarbeiter, Studentinnen und Studenten, Zivildienerinnen und Zivildiener und andere zeitlich befristete Praktikantinnen und Praktikanten.

IKT-Sicherheit
bezeichnet die Sicherheit von technischen Systemen der Informations- und Kommunikationstechnologie und damit die Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen im Bereich der Informations- und Kommunikationstechnologie.

IKT-Risikomanagement
sind koordinierte Aktivitäten zur Führung und Kontrolle einer Organisation in Bezug auf IKT-Risiken (siehe Pkt. 3.1.1).

Selfassessment
Periodische, dienststelleninterne Überprüfung und Bewertung der IKT-Sicherheit auf Basis von Checklisten (siehe Pkt. 3.1.1 IKT-Sicherheitscheckliste).

Smartphones
sind Multifunktionsgeräte, die über das Telefonieren hinaus Funktionen ähnlich eines Personal Computers aufweisen. Sie verfügen über ein eigenes Betriebssystem, das es den Benutzerinnen und Benutzern ermöglicht, zusätzliche Programme (Applikationen) zu installieren.

Smartphone-Applikationen („Apps“)
sind zusätzliche Programme, die auf Smartphones installiert werden können, um deren Funktionsumfang zu erweitern.

2. WienCERT

Das WienCERT befasst sich mit technischen und organisatorischen Fragen der IKT-Sicherheit.
Informationen unter http://www.intern.magwien.gv.at/wiencert/wiencert.html

3. Verantwortlichkeiten

3.1 Verantwortlichkeiten der Leiterinnen und Leiter der auftraggebenden Stellen

3.1.1 IKT-Risikomanagement

Die Leiterinnen und Leiter der auftraggebenden Stellen (in weiterer Folge Leiterinnen und Leiter) haben für ihren Verantwortungsbereich IKT-Risikomanagement zu betreiben. Aktivitäten im Zuge des IKT-Risikomanagements haben insbesondere darauf abzuzielen, Bedrohungen der IKT-Sicherheit zu erkennen, zu bewerten und Maßnahmen zur Beseitigung der Bedrohungssituation zu setzen. Ist die Beseitigung nicht möglich, sind Maßnahmen zu setzen, um das Risiko auf ein akzeptables Maß zu reduzieren (= Restrisiko). Insbesondere beinhaltet das IKT-Risikomanagement die IKT-Risikoidentifikation, IKT-Risikobewertung, das Setzen von Maßnahmen (z.B. Erarbeitung von Notfallplänen) und das IKT-Risikocontrolling. Gegenseitige Abhängigkeiten sind festzustellen, da diese Einfluss auf die Bewertung des Risikos haben können (z.B. ist die Funktionsfähigkeit der Hardware von der Funktionsfähigkeit der Stromversorgung abhängig). Missstände sind unverzüglich an die IKT-Dienststelle zu melden und zu beheben. Ist eine sofortige Behebung nicht möglich, sind erforderlichenfalls mit Unterstützung der zuständigen Dienststelle (IKT-Dienststelle oder andere) Maßnahmen zu erarbeiten und umzusetzen, die das durch den entdeckten Missstand auftretende Sicherheitsrisiko beheben oder zumindest auf ein akzeptables Maß herabsetzen.

IKT-Sicherheitscheckliste
Zur Darstellung der Risikosituation haben alle Leiterinnen und Leiter in ihrem Verantwortungsbereich jährlich eine Überprüfung und Bewertung der IKT-Sicherheit in Form von Selfassessments durchzuführen und nachvollziehbar zu dokumentieren, dafür steht eine Checkliste unter http://www.intern.magwien.gv.at/mir/iks/checklisten/checkliste_ikt_sicherheit.pdf zur Verfügung.

3.1.2 IKT-Sicherheitsbewusstsein

Die Leiterinnen und Leiter haben dafür zu sorgen, dass sich bei Personen, die für die Dienststelle tätig werden (Mitarbeiterinnen und Mitarbeiter, sowie Externe) ein IKT-Sicherheitsbewusstsein bildet und dieses ständig weiterentwickelt wird (z.B. durch Schulungen). Sie haben die Benutzerinnen und Benutzer insbesondere über die in Kap. 3.3 dieser Durchführungsrichtlinie angeführten Verpflichtungen zu informieren.

Sämtlichen neu eintretenden Mitarbeiterinnen und Mitarbeitern sind der IKT-Sicherheitserlass und die entsprechenden Verpflichtungserklärungen jedenfalls nachweislich zur Kenntnis zu bringen. Bestehende Verpflichtungserklärungen sind in regelmäßigen Intervallen zu aktualisieren und allen Mitarbeiterinnen und Mitarbeitern zur Kenntnis zu bringen.

Externe Stellen bzw. Externe
Bei der Zusammenarbeit mit Externen ist sicherzustellen, dass sich Externe ihrer Verpflichtungen bewusst sind und die Verantwortlichkeiten und Haftung akzeptieren, die der Zugriff, die Verarbeitung, die Kommunikation oder die Verwaltung von Informationen und informationsverarbeitenden Einrichtungen mit sich bringen. Es müssen sich alle aus der Zusammenarbeit mit Externen oder aus den betrieblichen Kontrollen resultierenden Sicherheitsanforderungen in vertraglichen Regelungen widerspiegeln (siehe Pkt. 6 des Erlasses „Sicherheit in der Informations- und Kommunikationstechnologie“).

3.1.3 Durchführung der Klassifizierung

Informationen sollen unabhängig von der dargebotenen Form, der gemeinsamen Nutzung oder Speicherung immer angemessen geschützt werden. Darunter fallen auch Informationen, die aus IKT-Anwendungen erzeugt werden bzw. als Auswertungen zur Verfügung stehen.

Für alle elektronisch verarbeiteten Daten ist durch die auftraggebende Stelle eine Klassifizierung gemäß der unten stehenden Tabelle unter Berücksichtigung der Gesetze, Verordnungen und Erlässe durchzuführen. Darüber sind geeignete Aufzeichnungen zu führen und der IKT-Dienststelle zur Verfügung zu stellen. Die IKT-Dienststelle kann bei der Klassifizierung unterstützen.

Sicherheitsklasse	SK	Eigenschaft	Bei Zugriff erforderliche Sicherheitsanforderungen aus Sicht der Benutzerinnen und Benutzer	Bemerkung
frei verfügbar	0	Die Sicherheitsklasse 0 regelt den Zugriff auf veröffentlichte Informationen/Daten, die „jedermann“ berechtigterweise ohne Identifizierungsnotwendigkeit einsehen kann.	nicht erforderlich	z.B. Daten aus dem Internet, öffentliches Telefonbuch,…
eingeschränkt	1	Die Sicherheitsklasse 1 regelt den Zugriff auf eigene, möglicherweise personenbezogene Daten oder Daten Dritter ohne Personenbezug, die nicht „jedermann“ zur Verfügung stehen.	Anmeldung durch Wissen (z.B. Benutzerinnen- bzw. Benutzername/ Passwort)	z.B. Daten aus dem Intranet; Datenaustausch von nichtpersonenbezogenen Daten im internen E-Mail-Verkehr im Rahmen der Amtstätigkeit
vertraulich	2	Die Sicherheitsklasse 2 regelt den Zugriff auf vertrauliche Daten.	Anmeldung durch Wissen (z.B. Benutzerinnen- bzw. Benutzername/Passwort) und an einem von der IKT-Dienststelle als sicher eingestuften Netzwerk betriebenen Gerät oder durch Wissen und Besitz (z.B. Dienstkarte, Zertifikat,…)	z.B. personenbezogene Daten Dritter gemäß DSG 2000 (Abfrage, Änderungen, ...) bei internem (über internes, sicheres Netzwerk) Zugriff genügt Wissen; bei Zugriff von extern (z.B.: von zu Hause) ist Wissen und Besitz erforderlich
geheim	3	Die Sicherheitsklasse 3 regelt den Zugriff auf geheime Daten.	Anmeldung durch Wissen (z.B. Benutzerinnen- bzw. Benutzername/Passwort) und an einem von der IKT-Dienststelle als sicher einge-	z.B. sensible Daten gemäß DSG 2000 (z.B. Religionsbekenntnis,…); Vorhandensein eines umfassenden Be-

			stuften Netzwerk betriebenen Gerät oder durch Wissen und Besitz (z.B. Dienstkarte, Zertifikat,…)	rechtigungssystems notwendig
Sicherheitsklasse	SK	Eigenschaft	Bei Zugriff erforderliche Sicherheitsanforderungen aus Sicht der Benutzerinnen und Benutzer	Bemerkung
streng geheim	4	Die Sicherheitsklasse 4 regelt den Zugriff auf streng geheime Daten.	Anmeldung durch Wissen und Besitz (z.B. Dienstkarte, Zertifikat,…) an einem von der IKT-Dienststelle als sicher eingestuften Netzwerk	z.B. Verschlusssachen (siehe auch § 3 Ziff. 39, BVergVS 2012)

Die IKT-Dienststelle hat die Aufzeichnungen der auftraggebenden Stelle über die Klassifizierung der elektronisch verarbeiteten Daten zusammenzuführen und daraus die Klassifizierung der IKT-Anwendungen abzuleiten. Für bestehende IKT-Anwendungen, die in Sicherheitsklasse 3 („geheim“) eingestuft werden und die Sicherheitsanforderungen bei Zugriff technisch nicht erfüllen, können in Abstimmung mit der MD-OS/IKT Ausnahme- bzw. Übergangsregelungen getroffen werden. Über Ausnahme- bzw. Übergangslösungen sind geeignete Aufzeichnungen zu führen.

Daten (in elektronischer Form vorliegende Informationen) sind bei Weitergabe entsprechend ihrer Sicherheitsklasse zu schützen (z.B. durch Verschlüsselung). Die IKT-Dienststellen haben entsprechende Schulungen anzubieten und geeignete Maßnahmen zur Förderung des IKT-Sicherheitsbewusstseins zu setzen.

Verfügbarkeit von IKT-Anwendungen
Die auftraggebende Stelle hat die Verfügbarkeitsanforderung der jeweiligen IKT-Anwendung der IKT-Dienststelle bekannt zu geben (als Verfügbarkeit wird die Wahrscheinlichkeit bezeichnet, dass ein IKT-System innerhalb eines spezifizierten Zeitraums funktionstüchtig ist).

Elektronischer Austausch bzw. elektronischer Transport von Daten
Bei Austausch oder Transport von Daten hat die auftraggebende Stelle in Abstimmung mit der IKT-Dienststelle nach Maßgabe der technischen Möglichkeiten, unter Berücksichtigung der Wirtschaftlichkeit und unter Einhaltung der gültigen Richtlinien, Verordnungen und Gesetze, Vorsorge zu treffen, um den Verlust oder Missbrauch von Daten zu verhindern. Dabei ist die Klassifizierung der Daten zu berücksichtigen.

3.1.4 Management der Benutzerinnen- bzw. Benutzerberechtigungen

Die Leiterinnen und Leiter haben Benutzerinnen- bzw. Benutzerberechtigungen nur in dem für die Aufgabenerfüllung erforderlichen Umfang einzuräumen. Sie haben Änderungen von Benutzerinnen- bzw. Benutzerberechtigungen schriftlich bei der IKT-Dienststelle, unter Angabe des konkreten Umfanges, zu beauftragen. Die Berechtigungen sind regelmäßig zu überprüfen. Die Benutzerinnen- bzw. Benutzerberechtigungen müssen deaktiviert oder gelöscht werden, wenn das Beschäftigungsverhältnis oder der Vertrag endet, bei Veränderungen (z.B. Versetzungen) müssen sie angepasst werden. Nicht mehr aktive Benutzerinnen- bzw. Benutzernamen dürfen für Nachfolgerinnen bzw. Nachfolger nicht reaktiviert werden. Personenbezogene Benutzerinnen- bzw. Benutzernamen dürfen nicht mehrmals vergeben werden.

Erfolgt die Vergabe von Benutzerinnen- bzw. Benutzerberechtigungen im eigenen Wirkungsbereich, d.h. durch die Dienststelle selbst, ist die Vergabe schriftlich unter Angabe des Benutzerinnen- bzw. des Benutzernamens und des konkreten Umfanges zu dokumentieren.

Externen darf der elektronische Zugang zu den Informationen des Magistrats, welche nicht als „frei verfügbar“ klassifiziert sind, erst dann bereitgestellt werden, wenn die entsprechende Geheimhaltungsverpflichtung unterzeichnet wurde. Die Vergabe der Benutzerinnen- bzw. Benutzerberechtigung auf Daten für Externe muss mit der auftraggebenden Dienststelle abgestimmt werden. Bei Beauftragung von externen Stellen hat die auftraggebende Stelle die Einhaltung dieses Erlasses durch schriftlichen Vertrag sicherzustellen.

Zugriffsberechtigungen auf Portalverbundanwendungen
Der Zugriff auf Anwendungen des Portalverbundes oder die Bereitstellung von Anwendungen über den Portalverbund für externe Stellen im Sinne der Portalverbundvereinbarung ist vorab mit der Magistratsabteilung 26 abzustimmen und erfolgt über das Stammportal des Magistrats der Stadt Wien.

3.1.5 Maßnahmen zum Schutz der IKT-Räume sowie Hard- und Software

Räume bzw. Räumlichkeiten
Die Leiterinnen und Leiter haben für die Sicherheit der IKT-Anlagen und -Geräte und sonstigen Benutzerinnen- bzw. Benutzerkomponenten zu sorgen. Sie sind auch für die Wahl des

Standortes der Hardware im Hinblick auf die Vermeidung und Verringerung potenzieller Risiken (Beschädigung, Diebstahl, unberechtigter Zugriff, etc.) verantwortlich, sofern nicht im Ausnahmefall im Einvernehmen zwischen der IKT-Dienststelle und einer Dienststelle andere Vereinbarungen getroffen wurden.

Sofern sich in Räumlichkeiten IKT-Anlagen, IKT-Infrastruktur und IKT-Geräte befinden, haben die Leiterinnen und Leiter Sicherheitszonen (erforderlichenfalls im Rahmen eines Zutrittssicherheitskonzepts) festzulegen und zu dokumentieren. Dabei ist der unbeaufsichtigte Zutritt sowie die Beschädigung und Störung der IKT-Anlagen und IKT-Geräte zu verhindern. Eine Sicherheitszone kann ein abschließbares Büro oder mehrere Räume, die innerhalb eines physikalisch abgegrenzten Bereichs liegen, sein. Für Räume mit erhöhter Schutzwürdigkeit (das sind jedenfalls Räume mit Zentraleinrichtungen der IKT) sind dementsprechend verschärfte Maßnahmen (wie z.B. Schließvorrichtung, Sperrsystem, Überwachungssystem, Zutrittsberechtigungssystem, Einbruchmeldesystem) vorzusehen. Diese Maßnahmen sollen im Einklang mit den identifizierten Risiken stehen.

Die Leiterinnen und Leiter haben für den Betrieb der zentralen IKT-Anlagen (z.B. Netzwerkkomponenten, Telekommunikationsanlage) geeignete Räume zur Verfügung zu stellen, die den Vorgaben der IKT-Dienststelle entsprechen. Sie haben den unbeaufsichtigten Zutritt sowie die Beschädigung und Störung der IKT-Anlagen und -Geräte in diesen zu verhindern. Werden Räume von auftraggebenden Stellen für Zentraleinrichtungen der IKT genutzt, ist eine Abstimmung mit allen beteiligten Dienststellen hinsichtlich Zutrittssicherheit notwendig.

Hardware

Hardware ist, sofern sich auf dieser nicht ausschließlich Daten, die ausdrücklich zur Veröffentlichung freigegeben wurden (im Sinne der Klassifizierung „frei verfügbare Informationen“) befinden, jedenfalls im Wege der oder im Einvernehmen mit der IKT-Dienststelle zu entsorgen. Allenfalls darauf befindliche Daten sind vor der Übergabe von der auftraggebenden Stelle zu löschen. Die IKT-Dienststelle hat jedenfalls für die sichere Löschung der Daten zu sorgen.

Netzwerk

Der Anschluss von IKT-Geräten (auch mobiler IKT-Geräte) an das Netzwerk der Stadt Wien darf nur mit Zustimmung der IKT-Dienststelle erfolgen, die die Anschlussbedingungen entsprechend der gültigen Sicherheitsvorschriften vorgibt.

Die Vergabe von IP-Adressen und IP-Adressbereichen erfolgt zentral durch die IKT-Dienststelle oder durch von der IKT-Dienststelle beauftragte externe Stellen bzw. Externe.

Das Herbeiführen von Störungen oder Unterbrechungen des Netzbetriebes durch fahrlässiges Verhalten (z.B. durch Wiederholen der Fehlersituation) ist zu vermeiden. Die Belastung des Netzes durch ungezielte und übermäßige Verbreitung von Informationen, insbesondere dienstlich nicht relevanter Art (siehe § 51 der GOM) ist jedenfalls zu unterlassen.

Software
Maßnahmen und Systeme der IKT-Dienststelle zum Schutz der Software (z.B. Virenscanner, Einspielen von Patches,…) sind zu verwenden. Änderungen an von der IKT-Dienststelle vorgegebenen Sicherheitseinstellungen sind untersagt.

IKT-Anwendungen dürfen nur in Abstimmung mit der IKT-Dienststelle in der von der IKT-Dienststelle freigegebenen Version eingesetzt werden.

Jede auftraggebende Stelle hat den ordnungsgemäßen und sicheren Betrieb bei Zulieferungen durch Überwachung und Überprüfung der externen Dienstleistungen sicherzustellen. Diesbezügliche Aufträge an externe Stellen sind mit der IKT-Dienststelle abzustimmen. Die zuständigen IKT-Dienststellen können mit der Unterstützung der Überwachung und Überprüfung beauftragt werden.

3.1.6 Meldung von IKT-sicherheitsrelevanten Ereignissen bzw. Vorfällen

Die Leiterinnen und Leiter haben IKT-sicherheitsrelevante Ereignisse und Vorfälle sowie IKT-Sicherheitsrisiken unverzüglich an die IKT-Dienststelle zu melden. Im Fall von Hinweisen auf schwerwiegende Sicherheitsrisiken ist in der Dienststelle ein spezifisches IKT-Risikomanagement durchzuführen und nachvollziehbar zu dokumentieren. Die Leiterinnen und Leiter haben erforderlichenfalls unverzüglich die für Revisionen zuständige Stelle sowie die MD – Geschäftsbereich Organisation und Sicherheit, Gruppe Informations- und Kommunikationstechnologie zu informieren, die gegebenenfalls andere Dienststellen hinzuziehen kann.

3.1.7 Sicherer Umgang mit mobilen IKT-Geräten

Die Technologie von mobilen Endgeräten ist bereits auf dem Niveau eines PCs. Daten auf dem mobilen IKT-Gerät sind vor Zugriff und Manipulation Dritter zu schützen.

Die Leiterinnen und Leiter haben dafür Sorge zu tragen, dass den Mitarbeiterinnen und Mitarbeitern die speziellen Sicherheitsmaßnahmen für Handys, Smartphones und Tablets, die in Kap. 3.3.3 angeführt sind, zur Kenntnis gebracht werden und die Einhaltung dieser durch geeignete Maßnahmen (z.B. Information, Awarenessbildung) gewährleistet wird. Auf die "Verpflichtungserklärung zur dienstlichen Nutzung mobiler Endgeräte"
(http://www.intern.magwien.gv.at/ma14/ikt-sicherheit/regelungen/verpflichtungserklaerung-nutzung-mobiler-geraete.pdf)
wird hingewiesen.

Smartphone- bzw. Tablet-Applikationsmanagement („Apps“)
Um das Risiko von ungewollten Datenübermittlungen (Gerätecode, Standort, Bankdaten,…) und dadurch unkontrollierbaren Kosten zu minimieren, stellt die IKT-Dienststelle eine Liste der freigegebenen Applikationen („Whitelist“) zur Verfügung, die den IKT-Sicherheitskriterien entsprechen, sowie eine Liste der verbotenen Applikationen („Blacklist“). Alle anderen Smartphone-Applikationen werden auf eigenes Risiko der Dienststelle installiert. Auswertungen über die installierten Smartphone- bzw. Tablet-Applikationen werden im IKT-DienststellenleiterInnen-Infoportal zur Verfügung gestellt.

3.1.8 Maßnahmen zum Schutz vor dem Zugriff Unbefugter

Die Leiterinnen und Leiter haben dafür Sorge zu tragen, dass bei der Nutzung von Passwörtern, Sicherheitskarten o.ä. Authentisierungsmerkmalen und Codes, die in Kap. 3.3.4 angeführten Anforderungen durch geeignete Maßnahmen (z.B. Information, Awarenessbildung) bekannt gemacht und eingehalten werden.

3.1.9 Regelungen für die private Nutzung dienstlicher und dienstliche Nutzung privater IKT-Geräte

Die private Nutzung von IKT-Geräten der Stadt Wien ist nur im Rahmen von § 51 GOM gestattet. Auf privaten IKT-Geräten ist die Speicherung dienstlicher Daten, die nicht als frei verfügbar klassifiziert sind, verboten (z.B. E-Mails). Die Leiterinnen und Leiter haben dafür Sorge zu tragen, dass die Mitarbeiterinnen und Mitarbeiter über die speziellen Einschränkungen informiert werden und diese einhalten (siehe Kap. 3.3.5).

3.1.10 Sicherheitsrelevante Maßnahmen bei Beendigung des Beschäftigungsverhältnisses

Bei Beendigung des Beschäftigungsverhältnisses oder sonstiger Vertragsverhältnisse, die zur Nutzung von Hard- bzw. Software der Stadt Wien berechtigen, ist die gesamte zugeteilte Hard- und Software einschließlich dazugehöriger Handbücher, Dokumente, Zutrittskarten und Schlüssel etc. zurückzugeben. Benutzerinnen- bzw. Benutzerberechtigungen sind infolge des Ausscheidens einer Mitarbeiterin bzw. eines Mitarbeiters zu deaktivieren bzw. zu löschen.

3.1.11 Personenbezogene Auswertungen

Den Leiterinnen und Leitern sind von der zuständigen IKT-Dienststelle Statistiken ohne Personenbezug betreffend die Internetnutzung bzw. über Telekommunikationsdaten zur Verfügung zu stellen. Für Auswertungen über die Bediensteten mit Personenbezug (im Falle des begründeten Verdachts auf missbräuchliche Verwendung) gelten folgende Regelungen: Hinsichtlich personenbezogener Auswertungen der Internetzugriffe über Smartphones bzw. Tablets ist der Erlass MD-OS-329/2011 „Internet und elektronische Kommunikation; offizielle Dienststellen Postfächer“ anzuwenden. Bei der personenbezogenen Auswertung von Telekommunikationsdaten kommt der Erlass MDO-150/2004 **„**Auswertung von TK-Vermittlungsdaten; Vorgehensweise“ zur Anwendung.

3.2 Zusätzliche Verantwortlichkeiten der IKT-Dienststellen

Die Leiterinnen und Leiter der IKT-Dienststellen haben über die in Kap. 3.1 angeführten Verantwortlichkeiten hinaus folgende Verpflichtungen:

Die Leiterinnen und Leiter der IKT-Dienststellen sind für den ordnungsgemäßen und sicheren Betrieb der Einrichtungen zur Informationsverarbeitung sowie für die Sicherheit der von der IKT-Dienststelle betriebenen Rechnerräume verantwortlich.

3.2.1 Betreiben eines Informationssicherheitsmanagement-Systems

Unter Management der Informationssicherheit versteht man das Aufstellen von Regeln und Verfahren, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Die IKT-Dienststellen haben ein IKT-Sicherheitskonzept zu entwickeln, welches insbesondere eine Bestandsaufnahme und Strukturanalyse der IKT-Geräte und Software, die Feststellung des Schutzbedarfes einzelner IKT-Systeme sowie die Festsetzung von Sicherheitsstandards und Schutzmaßnahmen zu umfassen hat. Die Ergebnisse des IKT-Risikomanagementprozesses und der internen und externen Audits führen zu einem kontinuierlichen Verbesserungsprozess.

Sofern andere Dienststellen einen genehmigten IKT-Betrieb führen, haben sie ein IKT-Sicherheitskonzept zu erstellen und mit der IKT-Dienststelle abzustimmen. Die zuständigen IKT-Dienststellen können von diesen Dienststellen mit der Unterstützung beauftragt werden.

Die IKT-Dienststellen haben technische Sicherheitsvorfälle oder sicherheitsrelevante Ereignisse unverzüglich dem WienCERT zu melden.

3.2.2 Ordnungsgemäßer und sicherer Betrieb von IKT-Einrichtungen

Die IKT-Dienststellen haben den ordnungsgemäßen und sicheren Betrieb von Einrichtungen zur Informationsverarbeitung sicherzustellen. Die IKT-Dienststellen haben in ihrem Verantwortungsbereich für Präventionsmaßnahmen zu sorgen, die den Schutz der Integrität von Software und Informationen vor Beschädigung durch Software mit Schadfunktion sicherstellen. Sie haben im Rahmen dessen geeignete, dem Stand der Technik entsprechende und wirtschaftlich vertretbare Schutzkonzepte gegen Viren, Spam etc. zu entwickeln, zu implementieren und zu betreiben.

Auf Basis eines Sicherungskonzeptes sind regelmäßige Sicherungskopien von Daten zu erstellen und die Wiederherstellung der Daten zu überprüfen. Art und Ausmaß der Datensicherung sind (unter Berücksichtigung der Sicherheitsklassen) in den Service-Level-Agreements zwischen den auftraggebenden Dienststellen und den IKT-Dienststellen zu vereinbaren. Bei Datenverlust darf der Aufwand für die Wiederherstellung der Daten nicht unverhältnismäßig sein.

Betriebskontinuitätsmanagement
Die IKT-Dienststellen haben den Verfügbarkeitsanspruch von IKT-Anwendungen in entsprechenden Verfügbarkeitsklassen zu dokumentieren. Sie haben ein Notfall-Handbuch (Disaster Recovery Handbuch) zu führen, in dem alle Maßnahmen, die nach Eintritt eines notfallauslösenden Ereignisses zu ergreifen sind, und alle dazu erforderlichen Informationen dokumentiert sind.

3.2.3 Maßnahmen zum Schutz der IKT-Infrastruktur - Netzwerke der Stadt Wien sowie der Hard- und Software

Die IKT-Dienststellen haben dem Stand der Technik entsprechende Maßnahmen zur Gewährleistung der Sicherheit der IKT-Infrastruktur (Netzwerke der Stadt Wien sowie der Hard- und Software) zu treffen. Sie haben darüber hinaus dem Stand der Technik entsprechende Maßnahmen zu ergreifen, um den Verlust oder Missbrauch von Daten bei deren Austausch oder Transport zu verhindern.

IKT-Anwendungen (IKT-Applikationen)
IKT-Anwendungen dürfen nur in Abstimmung mit der IKT-Dienststelle in der von der IKT-Dienststelle freigegebenen Version eingesetzt werden. Dafür haben die IKT-Dienststellen geeignete Methoden anzuwenden, um ein Höchstmaß der Sicherheit der eingesetzten IKT-Anwendungen zu erreichen (z.B. automatisiertes Einspielen von Sicherheitspatches). Sie haben eine entsprechende Information über die freigegebenen IKT-Anwendungen und deren Version für die Benutzerinnen und Benutzer bereitzustellen.

Patchmanagement
Die IKT-Dienststellen haben ein entsprechendes Patchmanagement zu implementieren, mit der Möglichkeit, die auf den IKT-Geräten eingesetzte Software und ihre Versionen auf Aktualität zu überprüfen.

Räume bzw. Räumlichkeiten
Die IKT-Dienststellen haben Sicherheitszonen (erforderlichenfalls im Rahmen eines Zutrittssicherheitskonzepts) für Räumlichkeiten, in denen sich IKT-Anlagen, IKT-Infrastruktur und IKT-Geräte befinden, festzulegen und zu dokumentieren. Dabei ist der unbeaufsichtigte Zutritt sowie die Beschädigung und Störung der IKT-Anlagen und IKT-Geräte zu verhindern.

Ersatzgeräte und Datensicherungsmedien sind in sicherer Entfernung von der Sicherheitszone unterzubringen, um zu verhindern, dass diese bei einem Schaden am primären Standort mitbetroffen sind.

Entsorgen von Hardware
Die IKT-Dienststellen haben entsprechende Services für die sichere Entsorgung von auszuscheidenden Datenträgern anzubieten. Bei sämtlichen IKT-Geräten bzw. IKT-Anlagen, welche Speichermedien enthalten, muss vor der Entsorgung überprüft werden, ob alle Daten und die lizenzierte Software unwiederbringlich entfernt oder sicher überschrieben wurden. Dabei sollen anstelle der Standard-Lösch- und Formatierfunktionen, Techniken angewendet werden, die sicherstellen, dass die ursprünglichen Informationen nicht mehr zurückgewonnen werden können.

Netzwerksicherheit
Die IKT-Dienststellen sind verpflichtet, dem Stand der Technik entsprechende Netzwerkmanagementsysteme einzusetzen (Netzwerkkontrollen und -maßnahmen zu implementieren), um die Sicherheit in den IKT-Netzwerken der Stadt Wien zu gewährleisten.

Die IKT-Dienststelle hat - wenn technisch möglich und wirtschaftlich vertretbar - Versuche,

- sich ohne Autorisierung Zugang zu Informationen und Netzdiensten - welcher Art auch immer - zu verschaffen,
- in interne/externe Netze/Geräte einzudringen,
- unbefugt Informationen zu verändern, die über die Netze verfügbar sind,

zu unterbinden.

Um sicherzustellen, dass keine Programme mit unerwünschten Auswirkungen eingebracht werden und das System nicht über den festgelegten Funktionsumfang hinaus unkontrolliert genutzt wird, ist das Einspielen nichtfreigegebener Software in Produktionssysteme bzw. ihre Nutzung verboten und soweit technisch möglich zu verhindern.

3.2.4 Einsatz von Berechtigungsverwaltungssystemen

Die IKT-Dienststellen haben dem Stand der Technik entsprechende Berechtigungsverwaltungssysteme einzusetzen. Dem Benutzerinnen- bzw. Benutzernamen ist als Berechtigungsnachweis der Benutzerin oder des Benutzers (Authentifikation) ein persönliches, selbst zu wählendes und geheim zu haltendes Passwort, biometrisches Sicherheitsmerkmal, Sicherheitskarte o.ä. Authentisierungsmerkmal zuzuordnen. Die IKT-Dienststelle hat der auftraggebenden Stelle geeignete Auswertungen über die Benutzerinnen- bzw. Benutzerberechtigungen zur Verfügung zu stellen.

Portalverbundzugriffe

Der Zugriff auf Anwendungen des Portalverbundes oder die Bereitstellung von Anwendungen über den Portalverbund für externe Stellen im Sinne der Portalverbundvereinbarung ist vorab mit der Magistratsabteilung 26 abzustimmen und erfolgt über das Stammportal des Magistrats der Stadt Wien.

Administratorinnen- bzw. Administratorenrechte

Administratorinnen bzw. Administratoren von IKT-Systemen und ihre Vertreterinnen und Vertreter haben – in Abhängigkeit vom eingesetzten System – weit gehende und oftmals allumfassende Berechtigungen. Das hierfür eingesetzte Personal muss sorgfältig ausgewählt werden. Es soll regelmäßig darüber belehrt werden, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen. Eine regelmäßige Kontrolle der Zugriffe von Administratorinnen bzw. Administratoren – etwa durch Auswertung von Protokollen – ist vorzusehen. Die Vergabe von Administratorinnen- bzw. Administratorenberechtigungen hat in einem Mehraugenprinzip zu erfolgen. Die Berechtigungen von Administratorinnen bzw. Administratoren sind durch technische Maßnahmen – etwa die Verschlüsselung von ausgewählten Daten oder Zugriffsbeschränkungen zu Protokollfiles – nur so weit einzuschränken, dass deren Aufgabenerfüllung nicht beeinträchtigt wird.

3.2.5 Dokumentation von sicherheitsrelevanten IKT-Ereignissen und IKT-Vorfällen

Die IKT-Dienststellen haben dem Stand der Technik entsprechende Ereignisprotokolle zu führen, in denen außerordentliche Vorfälle und andere sicherheitsrelevante Vorfälle verzeichnet werden. Die Protokolle sind drei Jahre ab Erstellungsdatum aufzubewahren.

Die IKT-Dienststellen haben geeignete Sicherheitsauswertungen für die auftraggebenden Stellen bereit zu stellen. Die Dienststellen haben die von der IKT-Dienststelle zur Verfügung gestellten Sicherheitsauswertungen zu überprüfen und erforderlichenfalls geeignete Maßnahmen zu treffen. Die zuständigen IKT-Dienststellen können mit der Unterstützung beauftragt werden.

3.3 Verantwortlichkeiten der Benutzerinnen und Benutzer

Die Benutzerinnen und Benutzer sind für die ordnungsgemäße und sicherheitsbewusste Verwendung der ihnen übertragenen IKT-Geräte verantwortlich und haben die von der IKT-Dienststelle zur Verfügung gestellten Schutzmaßnahmen anzuwenden. Jede bzw. jeder Bedienstete ist für die unter ihrem bzw. seinem Benutzerinnennamen bzw. Benutzernamen erfolgten Aktivitäten verantwortlich.

Sie haben Daten bei Weitergabe entsprechend ihrer Sicherheitsklasse zu schützen oder die von der IKT-Dienststelle zur Verfügung gestellten Schutzmaßnahmen anzuwenden.

Insbesondere ergeben sich folgende Verpflichtungen:

3.3.1 Maßnahmen zum Schutz der Hard- und Software

Der Einbau privater Komponenten in IKT-Geräte der Stadt Wien ist verboten. Ebenso ist es unzulässig, Reparaturen bzw. Upgrades und sonstige Hardwareveränderungen vorzunehmen. Derartige Maßnahmen dürfen ausschließlich von

- der IKT-Dienststelle,
- Stellen, die von der IKT-Dienststelle beauftragt wurden,

durchgeführt werden.

Das Herbeiführen von Störungen oder Unterbrechungen des Netzbetriebes durch fahrlässiges Verhalten (z.B. durch Wiederholen der Fehlersituation) ist zu vermeiden. Die Belastung des Netzes durch ungezielte und übermäßige Verbreitung von Informationen, insbesondere dienstlich nicht relevanter Art (siehe § 51 der GOM) ist zu unterlassen.

Versuche,

- sich ohne Autorisierung Zugang zu Informationen und Netzdiensten zu verschaffen,
- in interne/externe Netze/Geräte einzudringen,
- unbefugt Informationen zu verändern, die über die Netze verfügbar sind,

sind verboten.

Maßnahmen und Systeme der IKT-Dienststelle zum Schutz der Software (z.B. Virenscanner, ADV-Installer, Einspielen von Patches,…) sind zu verwenden bzw. dürfen nicht abgeschaltet werden. Änderungen an von der IKT-Dienststelle vorgegebenen Sicherheitseinstellungen sind untersagt. IKT-Anwendungen dürfen nur in Abstimmung mit der IKT-Dienststelle in der von der IKT-Dienststelle freigegebenen Version eingesetzt werden. Die Verwendung privater Software auf IKT-Geräten der Stadt Wien ist grundsätzlich verboten. Ausnahmen können in

Abstimmung mit der IKT-Dienststelle genehmigt werden. Darunter fällt auch selbst beschaffte bzw. aus dem Internet geladene Software (Freeware, Shareware, Demoversionen, etc.).

Für Smartphone- und Tablettapplikationen gelten die in Kap. 3.3.3 beschriebenen Regelungen.

Die Datenablage von Daten ab der Sicherheitsklasse 1 („eingeschränkt“) hat grundsätzlich auf den von der IKT-Dienststelle zur Verfügung gestellten zentralen Speichermedien zu erfolgen (z.B. Fileservices).

3.3.2 Meldung von IKT-sicherheitsrelevanten Ereignissen bzw. Vorfällen

IKT-sicherheitsrelevante Ereignisse und Vorfälle sowie IKT-Sicherheitsrisiken sind unverzüglich im Wege der IKT-Sicherheitsbeauftragten bzw. des IKT-Sicherheitsbeauftragten der Dienststelle an die IKT-Dienststelle zu melden.

3.3.3 Sicherer Umgang mit mobilen IKT-Geräten

Mobile IKT-Geräte (Handy, Smartphone, Tablet, Notebook, etc.) sind vor dem Zugriff Dritter durch ein Passwort oder ein biometrisches Sicherheitsmerkmal oder eine Sicherheitskarte oder durch ein ähnliches Authentisierungsmerkmal abzusichern, das nur den berechtigten Personen bekannt bzw. verfügbar sein darf.

Die Datenspeicherung auf mobilen IKT-Geräten ist auf das unbedingt erforderliche Maß zu beschränken. Daten, die nicht als frei verfügbar klassifiziert sind (siehe Kap. 3.1.3), sind, wenn technisch möglich und wirtschaftlich vertretbar, zu verschlüsseln (Festplatten- bzw. Dateiverschlüsselung), wenn sie auf einem mobilen IKT-Gerät gespeichert oder verarbeitet werden. Unbeaufsichtigte mobile IKT-Geräte sind versperrt zu verwahren. Auf die "Verpflichtungserklärung zur dienstlichen Nutzung mobiler Endgeräte"
(http://www.intern.magwien.gv.at/ma14/ikt-sicherheit/regelungen/verpflichtungserklaerung-nutzung-mobiler-geraete.pdf)
wird hingewiesen.

Spezielle Sicherheitsmaßnahmen für Handys (Funktion: mobiles Telefonieren):

- Der PIN- und Gerätesperrcode ist zwingend zu verwenden.
- Die Verwendung von Verbindungsmethoden wie Bluetooth, WLAN und Infrarot sind nur im Bedarfsfall zu aktivieren und bei Beendigung wieder zu deaktivieren.
- Die Benutzung von Bluetooth ist so einzustellen, dass das Gerät für andere „unsichtbar“ ist. Der Name ist so zu wählen, dass keine Rückschlüsse auf das Gerät, den Arbeitsplatz oder die Person möglich sind. Es findet keine Datensynchronisation mit der E-Mail-Infrastruktur statt.
- Die Verwendung des Handys als Massenspeicher (analog zum USB-Stick) ist nur für Daten, die als frei verfügbar klassifiziert sind, erlaubt.

Über die Sicherheitsmaßnahmen für Handys (Funktion: mobiles Telefonieren) hinausgehende Sicherheitsmaßnahmen für Smartphones:

- Im Gegensatz zum Handy findet eine Datensynchronisation statt. Diese erfolgt kabellos im Rahmen einer sicheren Verbindung.
- Die IKT-Dienststelle kann mit Hilfe eines Fernzugriffs auf Smartphone-Funktionen zugreifen und bei Bedarf auch Änderungen (z.B. Löschen von Daten bei Verlust oder Diebstahl) vornehmen. Das Fernlöschen von Daten ist nur möglich, wenn das Smartphone bzw. Tablet in Betrieb ist.

Smartphone- und Tablet-Applikationsmanagement („Apps“)
Um das Risiko von ungewollten Datenübermittlungen (Gerätecode, Standort, Bankdaten…) und dadurch unkontrollierbaren Datenverlust und Kosten zu minimieren, dürfen Applikationen der „Whitelist“ (eine Liste der von der IKT-Dienststelle freigegebenen Applikationen) grundsätzlich installiert werden. Von der IKT-Dienststelle verbotene Applikationen werden auf einer „Blacklist“ geführt und dürfen nicht installiert werden. Alle anderen Smartphone-Applikationen können auf eigenes Risiko der Dienststelle installiert werden. Auswertungen über die installierten Smartphone-Applikationen werden im IKT-DienststellenleiterInnen-Infoportal zur Verfügung gestellt.

Spezielle Sicherheitsmaßnahmen für die Verwendung von USB (Universal Serial Bus)-Speichergeräten:
Ist die Speicherung von Daten ab der Sicherheitsklasse 2 („vertraulich“ dh. die nicht als „frei verfügbar“ bzw. „eingeschränkt“ klassifiziert sind), auf einem USB-Speichermedium unumgänglich, so ist eine Verschlüsselung der Daten durchzuführen. Die IKT-Dienststelle hat zu diesem Zweck USB-Speichermedien bzw. entsprechende Software mit der Möglichkeit der Verschlüsselung anzubieten.

3.3.4 Maßnahmen zum Schutz vor dem Zugriff Unbefugter

Passwörter, Sicherheitskarten o.ä. Authentisierungsmerkmale und Codes sind geheim zu halten und dürfen nicht weitergegeben werden.

Bei der Nutzung von Passwörtern, Sicherheitskarten o.ä. Authentisierungsmerkmalen und Codes müssen folgende Anforderungen eingehalten werden, sofern dies technisch möglich ist:

- Sie dürfen nicht zu einfach sein (z.B. 1234, Geburtsdatum, Vornamen, Monatsnamen, abcdef,…), müssen geheim gehalten werden und dürfen nicht weitergegeben werden. Die Eingabe muss daher unbeobachtet stattfinden.
- Sie müssen mindestens 8 Zeichen lang sein, wenn technisch möglich.
- Sie müssen mindestens ein Zeichen enthalten, das kein Buchstabe ist (Sonderzeichen oder Zahl).
- Passwörter für interne Anwendungen (z.B. LAN-User Passwort) dürfen nicht auch bei externen Anwendungen (z.B. externe Webseiten) verwendet werden.
- Dienstlich verwendete Passwörter dürfen nicht als Passwörter in privaten Anwendungen verwendet werden.

- Voreingestellte Passwörter (z.B. bei Auslieferung von Systemen) müssen umgehend durch individuelle Passwörter ersetzt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Das Passwort muss regelmäßig geändert werden, mindestens alle 90 Tage.
- Wird vermutet, dass das Passwort anderen Personen bekannt geworden ist, so ist ein sofortiger Passwortwechsel durchzuführen.
- Passworthinterlegungen (z.B. in Kuverts, bei Vorgesetzten,…) sind verboten.

Bei Verlassen des Arbeitsplatzes bzw. bei Überlassung an andere Personen ist der Benutzerinnen- bzw. Benutzername abzumelden. Bei kurzfristiger Abwesenheit ist das IKT-Gerät durch Sicherheitsvorkehrungen gegen unbefugte Benutzung zu sichern (z.B. „Computer sperren“).

Datenträger, ausgedruckte Daten sowie am Bildschirm wiedergegebene Daten sind vor der Einschau bzw. dem Zugriff Unbefugter zu schützen, dabei ist die Klassifizierung der Daten (siehe Kap. 3.1.3) zu berücksichtigen.

Datenablage
Die Datenablage hat auf den von der IKT-Dienststelle betriebenen bzw. unterstützten zentralen Speichersystemen zu erfolgen. Dabei ist die Klassifizierung der Daten zu berücksichtigen.

3.3.5 Regelungen für die private Nutzung dienstlicher und dienstliche Nutzung privater IKT-Geräte

Die private Nutzung von IKT-Geräten der Stadt Wien ist im Rahmen von § 51 GOM zulässig. Für die dienstliche Nutzung privater IKT-Geräte gelten Einschränkungen. Auf privaten IKT-Geräten ist die Speicherung dienstlicher Daten, die nicht als frei verfügbar klassifiziert sind, verboten (z.B. E-Mails). Daraus ergibt sich im Speziellen:

- Die Nutzung der dienstlichen SIM-Karte, auch wenn sie über kein Datenpaket verfügt, ist in privaten IKT-Geräten verboten.
- Dienstliche E-Mails sind auf privaten Endgeräten verboten.
- Dienstliche Kontakte und dienstliche Kalenderdaten sind auf privaten Endgeräten grundsätzlich erlaubt (besondere Vorsicht ist bei Speicherung von „VIP-Nummern“ gegeben).

Der Anschluss von privaten IKT-Geräten an das Netzwerk der Stadt Wien ist verboten. Das gilt auch für die Netzanbindung über drahtlose Schnittstellen.

3.3.6 Sicherheitsrelevante Maßnahmen bei Beendigung des Beschäftigungsverhältnisses

Bei Beendigung des Beschäftigungsverhältnisses oder sonstiger Vertragsverhältnisse, die zur Nutzung von Hard- bzw. Software der Stadt Wien berechtigen, ist die gesamte zugeteilte Hard- und Software einschließlich dazugehöriger Handbücher, Dokumente, Zutrittskarten und Schlüssel etc. zurückzugeben. Benutzerinnen- bzw. Benutzerberechtigungen sind infolge des Ausscheidens einer Mitarbeiterin bzw. eines Mitarbeiters zu deaktivieren bzw. zu löschen.

Informationen zur Signatur

StaDt+Wien	**Unterzeichner**	CN=Mag. Wolfgang Mueller MBA, OU=MD-OS, O=Stadt Wien, C=AT
	Datum/Zeit	Mon Jan 28 09:07:41 CET 2013
	Austeller-Zertifikat	CN=Stadt Wien CA Benutzer, O=Stadt Wien, C=AT
	Serien-Nr.	341
	Methode	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signatur)
Hinweis	Diese Signatur kann überprüft werden, wenn Sie das Dokument mit dem Adobe Reader öffnen!	