STADT BADEN

150.101

Verordnung über die Benutzung von Informatikmitteln und die Überwachung der Informationssicherheit

vom 27. März 2017

Kurzbezeichnung:

Informatik und Informationssicherheit

Zuständig:

Informatik

Stand: 1. November 2017

Baden ist.

Verordnung über die Benutzung von Informatikmitteln und die Überwachung der Informationssicherheit

vom 27. März 2017

Der Stadtrat der Stadt Baden,

gestützt auf § 12 des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006[1], die §§ 4 und 5 der Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG) vom 26. September 2007[2] sowie die §§ 18 und 20 der kommunalen Verordnung über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDA) vom 22. Dezember 2008,

beschliesst:

I. Allgemeine Bestimmungen

§ 1 Zweck

1 Diese Verordnung regelt die Benützung von Informatikmitteln und in diesem Zusammenhang den Schutz von Informationen der Stadt Baden. Die definierten Regeln auf organisatorischer Ebene sollen die Informationssicherheit als integraler Bestandteil von Geschäftsprozessen und damit die Verfügbarkeit, Vertraulichkeit und Integrität von Informationen gewährleisten.

2 Sie soll sicherstellen, dass beim Einsatz der Informatikmittel

a) die technischen Möglichkeiten zur Erfüllung der dienstlichen Aufgaben gemäss den definierten Sicherheitsanforderungen[3] zweckmässig genutzt werden;

b) die Datenbestände und insbesondere die vertrauenswürdigen Informationen geschützt sowie Schäden und Missbräuche verhindert werden;

c) der Schaden infolge Störungen und Problemen minimiert wird;

d) die Persönlichkeitsrechte gewahrt werden.

---

[1] SAR 150.700

[2] SAR 150.711

[3] Siehe Betriebsorganisation

§ 2 Geltungsbereich

Diese Verordnung gilt für die Mitglieder der Behörden und Gremien sowie die Mitarbeitenden der Verwaltung der Stadt Baden (nachfolgend "IT-Benutzende").

§ 3 Persönliche Verantwortung

1 Alle IT-Benutzenden sind für die Verwendung der ihnen zur Verfügung gestellten Informatikmittel und den zugänglichen dienstlichen Informationen im Rahmen der geltenden Rechtsordnung und dieser Verordnung persönlich verantwortlich.

2 Feststellungen über technische Mängel und sicherheitsrelevante Vorkommnisse sind umgehend den direkten Vorgesetzten sowie der Fachabteilung Informatik (nachfolgen "Informatik") zu melden.

§ 4 Dritte

1 Unbefugten Dritten ist weder der Zutritt zu den Räumlichkeiten der Stadt Baden ausserhalb der Publikumsbereiche noch der Zugang zu Informatiksystemen zu gewähren.

2 Dritte in den nicht öffentlichen Räumlichkeiten der Stadt Baden sind anzusprechen und falls nötig zum Ausgang zu begleiten.

3 Dritte, die aufgrund ihres Aufgabenbereichs Zugang zu Informatiksystemen der Stadt Baden erhalten sollen, sind mittels Unterzeichnung einer Vertraulichkeits-/Sicherheitsvereinbarung schriftlich zur Einhaltung von Sicherheitsvorgaben zu verpflichten.

II. Ein- und Austritt von IT-Benutzenden

§ 5 Mitglieder der Behörden und Gremien

1 Die Informatik regelt zusammen mit den Behördendiensten die formellen Vorgänge in Zusammenhang mit dem Ein- und Austritt der Mitglieder der Behörden und Gremien.

2 Benutzerzugänge und E-Mail-Adressen für neu eintretende Mitglieder der Behörden und Gremien sind bei der Informatik zu bestellen.

§ 6 Mitarbeitende

1 Die Informatik regelt zusammen mit der Fachabteilung Personal die formellen Vorgänge in Zusammenhang mit dem Ein- und Austritt von Mitarbeitenden.[1]

2 Benutzerzugänge und E-Mail-Konten für neu eintretende Mitarbeitende sind durch die (Fach-)Abteilung bei der Informatik zu bestellen.[1]

---

[1] Geändert durch Stadtratsentscheid vom 23. Oktober 2017, in Kraft seit 1. November 2017

§ 7 Austrittsformalitäten

1 Die Behördendienste erstatten der Informatik eine Meldung eines bevorstehenden Austritts von Mitgliedern von Behörden und Gremien.

2 Die Fachabteilung Personal erstatten der Informatik Meldung eines bevorstehenden Austritts von Mitarbeitenden. [1]

3 Austretende IT-Benutzende

a) räumen ihre persönliche Datenablage und ihr E-Mail-Konto @baden.ch auf;

b) übergeben alle geschäftsrelevanten Daten sowie wichtige und nicht erledigte E-Mails an die definierte Stellvertretung;

c) aktivieren den Abwesenheitsassistenten im Outlook mit einer Austrittsmeldung und Angabe der Adresse der Stellvertretung.

4 Die Informatik inaktiviert per Austrittsdatum das Benutzer- und das E-Mail-Konto sowie allfällige Mailweiterleitungen. Benutzerkonten werden frühestens einen Monat nach dem Austrittsdatum endgültig gelöscht.

III. Gebrauch von Informatikmitteln

§ 8 Dienstliche / Private Informatikmittel

1 Der Begriff "dienstliche Informatikmittel" erfasst alle Sachmittel der Informations- und Telekommunikationstechnologie (Hard- und Software), die

a) von der Informatik zur Benutzung bereitgestellt werden,

b) im Eigentum der Stadt Baden sind,

c) durch die Stadt Baden offiziell beschafft beziehungsweise zur Installation oder Nutzung freigegeben worden sind.

2 Der Einsatz privater Informatikmittel ist unter Einhaltung der geltenden Installations- sowie Sicherheitsbestimmungen zulässig.

§ 9 Fremdanschlüsse, Fremdprogramme

1 Nicht-städtische Informatikmittel dürfen nur mit Bewilligung der Informatik mit der städtischen Netzwerkinfrastruktur verbunden oder an städtische Informatikmittel angeschlossen werden. Davon ausgenommen ist die Nutzung des öffentlichen WLAN-Netzwerks der Stadt Baden.

2 Die Installation von Softwareprogrammen oder Treibern jeglicher Art auf dienstlichen Informatikmitteln durch die IT-Benutzenden ist untersagt.

---

[1] Geändert durch Stadtratsentscheid vom 23. Oktober 2017, in Kraft seit 1. November 2017

§ 10 Nutzung von dienstlichen Informatikmitteln

1 Die zur Verfügung gestellten dienstlichen Informatikmittel dürfen nur zur Erfüllung geschäftlicher Aufgaben benutzt werden. Dienstliche Informatikmittel dürfen unter Einhaltung dieser Vorschriften ausnahmesweise zu nicht kommerziellen privaten Zwecken verwendet werden.

2 Dienstliche Informatikmittel dürfen – mit Ausnahme der speziell für den mobilen Einsatz vorgesehenen Sachmittel – nicht mit nach Hause genommen werden.

§ 11 Zugangs- und Zugriffsschutz

1 Die von der Informatik bereitgestellten Informatikmittel werden durch folgende Massnahmen vor unberechtigtem Gebrauch geschützt:

a) Verwendung von Benutzernamen und starken Passwörtern (Benutzeridentifikation),

b) Verwendung von alternativen oder zusätzlichen Identifikationselementen (Chipkarte, Sicherheitszertifikat, Token, o.ä.),

c) Geheimhaltung von Zugangsdaten jeglicher Art (insbesondere der persönlichen Benutzeridentifikationsmerkmale),

d) zwingende Änderung des Initialpassworts bei der ersten Anmeldung oder nach Rücksetzung des Passworts,

e) periodische Änderung der Passwörter für die Anmeldung im Netzwerk,

f) Sperren oder Beenden des Zugriffs auf Anwendungen und Daten beziehungsweise das Abschliessen des Büros beim Verlassen des Arbeitsplatzes.

2 In ausserordentlichen Situationen (beispielsweise bei unvorhersehbaren längeren Abwesenheiten) kann durch die vorgesetzte Stelle bei der Informatik ein vorübergehender Zugriff auf das Benutzer- oder E-Mail-Konto von IT-Benutzenden beantragt werden. Ein entsprechender Antrag setzt, sofern möglich, das schriftliche Einverständnis der betroffenen Mitarbeitenden voraus und muss in jedem Fall durch die Personaldienste genehmigt werden.

3 Für den Zugang und Zugriff kann in begründeten Ausnahmefällen ein allgemeines, personenungebundenes, aufgaben- oder funktionsbezogenes Benutzerkonto eingerichtet werden.

§ 12 Internet

1 Zugänge ins Internet werden durch die Informatik bereitgestellt oder koordiniert.

2 Handlungen im Internet oder mittels anderen digitalen Medien gemäss § 17 Abs. 3 sind aus ethischen und/oder technischen Gründen (ausser in einem expliziten Zusammenhang mit der Arbeitstätigkeit) strikt untersagt und können bei Bedarf technisch reguliert werden.

3 Die Nutzung von sozialen Medien während der Arbeitszeit und/oder unter Einbezug der dienstlichen Informatikmittel ist gemäss den geltenden Richtlinien erlaubt, wenn die Nutzung verhältnismässig und zurückhaltend erfolgt.

§ 13 E-Mail-Verkehr

1 Die Mitarbeitenden der Verwaltung der Stadt Baden erhalten zusammen mit ihrem Benutzerkonto ein persönliches E-Mail-Konto @baden.ch.

2 Für die Mitglieder von bestimmten Behörden und Gremien[1] wird eine Weiterleitung der persönlichen @baden.ch-Mailadresse auf ein privates E-Mail-Konto eingerichtet. Die Weiterleitung an eine allgemeine, personenungebundene, aufgaben- oder funktionsbezogene E-Mail-Adresse ist nicht gestattet.

3 Bei Bedarf können auf Bestellung einer Abteilung unpersönliche, aufgaben- oder funktionsbezogene E-Mail-Konten (@baden.ch) mit Zugriffsberechtigung durch definierte IT-Benutzende eingerichtet werden.

4 Vertrauliche Informationen und besonders schützenswerte Personendaten[2] dürfen ausschliesslich mit den durch die Informatik bereitgestellten vertrauenswürdigen Übermittlungs- und/oder Verschlüsselungstechniken übermittelt werden (z.B. per E-Mail).

5 Die Bekanntgabe der geschäftlichen E-Mail-Adresse, beispielsweise im Internet, ist nur für dienstliche Zwecke erlaubt.

6 Beim Gebrauch der geschäftlichen E-Mail-Adressen für den Versand von privaten Nachrichten sind diese über die entsprechende Vertraulichkeitsoption des Mailprogramms als "Privat" zu kennzeichnen.

7 Der Gebrauch privater E-Mail-Adressen durch Mitarbeitende der Verwaltung der Stadt Baden für die geschäftliche Kommunikation ist nicht zulässig.

8 Nicht vertrauenswürdige E-Mails sind umgehend und endgültig zu löschen. Potenziell virenverdächtige Anhänge (Attachments) solcher E-Mails dürfen nicht geöffnet und Weblinks oder Bilder nicht angeklickt werden. Als nicht vertrauenswürdig gelten E-Mails insbesondere, wenn

a) die Absenderadresse als dubios erscheint oder unbekannt ist,

b) der Inhalt klar nicht geschäftsrelevant ist,

c) die Nachricht so nicht erwartet wurde beziehungsweise sie keinen Sinn ergibt,

d) der Absender zur Bekanntgabe von Passwörtern oder anderen vertraulichen Angaben oder Informationen auffordert.

---

[1] Mitglieder des Einwohnerrats und der Schulpflege

[2] § 3 Abs. 1 lit. k) des Gesetzs über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24.10.2006 [SAR 150.700], § 7 der Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG) vom 26.09.2007 [SAR 150.711]

9 Auf nicht vertrauenswürdige Nachrichten (inkl. Spam-Mails) darf nicht geantwortet werden. Eine Antwort bestätigt dem Absender die Korrektheit der Empfängeradresse.

§ 14 Abwesenheitsmeldungen, Weiterleitung von E-Mails

1 Bei Abwesenheiten von mehr als einem Arbeitstag haben Mitarbeitende der Verwaltung der Stadt Baden für eintreffende E-Mails eine Abwesenheitsmeldung mit Angabe der Adresse der Stellvertretung und der Dauer der Abwesenheit einzurichten.

2 Die automatische Weiterleitung eintreffender E-Mails ist unzulässig.

§ 15 Mobile Informatikmittel

1 IT-Benutzende, die mobile Informatikmittel (z.B. Notebooks, Tablets, private oder geschäftliche Smartphones usw.) dienstlich nutzen, sind angehalten, verantwortungsbewusst mit den verwendeten Geräten umzugehen.

2 Dienstlich genutzte, mobile Informatikmittel dürfen nicht unbeaufsichtigt an öffentlich oder leicht zugänglichen Orten zurückgelassen werden.

3 Die Verwendung von Drahtloskommunikation (2G/GSM, 3G/UMTS/HSDPA, 4G/LTE, WLAN, Bluetooth usw.) ist grundsätzlich gestattet. Zu beachten ist dabei, dass

a) keine Drahtloskommunikation zu einem öffentlichen Netzwerk hergestellt werden darf, sobald ein Gerät kabelgebunden mit dem städtischen Netzwerk verbunden ist,

b) ausschliesslich vertrauenswürdige, passwortgeschützte öffentliche Netzwerke genutzt werden und auf den mobilen Informatikmitteln stets aktuelle Betriebssystem- und Browserversionen sowie ein Virenschutz installiert sind.

§ 16 Mobile Datenträger

1 Mobile Datenträger (Speichermedien wie z.B. USB Sticks, externe Festplatten, Speicherkarten usw.) sind potenziell unsicher. IT-Benutzende sind angehalten, für den Datenaustausch auf den Einsatz mobiler Datenträger zu verzichten und auf vertrauenswürdige Technologien auszuweichen.

2 Die Informatik kann bei Bedarf die Nutzung von mobilen Datenträgern technisch beschränken.

3 Die Verwendung von unbekannten mobilen Datenträgern ist untersagt. Sie dürfen weder mit der Informatikinfrastruktur der Stadt Baden verbunden noch dürfen auf solchen Geräten geschäftliche Informationen gespeichert werden. Als unbekannt gelten insbesondere Datenträger, die

a) unbeaufsichtigt herumliegen,

b) deren Herkunft und vorherige Verwendung nicht bekannt sind,

c) ungefragt beziehungsweise unerwartet zugestellt werden (z.B. Geschenke).

§ 17 Unzulässiger Gebrauch von dienstlichen Informatikmitteln

1 Missbräuchlich ist jede Verwendung der Informatikmittel, die

a) gegen diese Verordnung verstösst,

b) gegen andere Bestimmungen der Rechtsordnung verstösst,

c) Rechte Dritter in rechtlich unzulässiger Weise verletzt.

2 Missbräuchlich sind insbesondere folgende Handlungen:

a) Anschliessen und Einrichten nicht bewilligter Informatikmittel (Hardware) und Installieren oder Nutzen nicht lizenzierter Programme (Software),

b) Versenden von E-Mails oder anderer elektronischer Nachrichten in Täuschungs-, Belästigungs- oder Beleidigungsabsicht und private Massenversendungen,

c) widerrechtliches Kopieren von Daten oder Software,

d) das Verwenden von fremden Benutzeridentifikationen (Benutzername, Passwörter oder andere Identifikationselemente),

e) der Versuch, die Sicherheitsvorkehrungen von Netzwerken, Informatikmitteln und Benutzerzugängen zu umgehen.

3 Unzulässige Handlungen im Internet oder im Bereich anderer digitaler Medien im Sinn dieser Verordnung sind:

a) der Zugriff auf oder die Verbreitung von sexistischen, rassistischen oder pornographischem Inhalten, Gewaltdarstellungen, Geldspiel- und Börsenseiten, Musik-/Video- und Softwaretauschbörsen, Internetradio/-fernsehen und dergleichen,

b) das Erstellen von Links auf Websites gemäss § 17 Abs. 3 lit. a),

d) das Downloaden von Daten oder Software für private Zwecke,

e) das Spielen von (Online-)Games.

§ 18 Fernzugriff

Den IT-Benutzenden stehen Möglichkeiten für den Fernzugriff auf Informationen (z.B. via Internet) zur Verfügung. Alle Zugriffe müssen mit der nötigen Sorgfalt erfolgen.

IV. Umgang mit Informationen

§ 19 Grundsatz

Die Bestimmungen betreffend Umgang mit Informationen regeln den Schutz von Informationen der Stadt Baden in Ergänzung zu bestehenden Regelungen. Vorbehalten bleiben spezialgesetzliche Bestimmungen.

§ 20 Verteilung von Informationen

1 Die Verarbeitung von Informationen und personenbezogener Daten ist am allgemeinen Ziel auszurichten, so wenig Daten wie möglich zu verteilen ("Datensparsamkeit").

2 Klassifizierte Informationen ("intern", "vertraulich", "geheim") sind nur jenen Personen zugänglich zu machen, die davon Kenntnis haben müssen. Das öffentlich Zugänglichmachen von klassifizierten Informationen ist untersagt.

3 Dritte, die aufgrund ihres Aufgabenbereichs Zugang zu klassifizierten Informationen erhalten sollen, sind zur Geheimhaltung (Vertraulichkeitsvereinbarung) zu verpflichten.

§ 21 Bekanntgabe von Informationen in sozialen Medien

1 Soziale Medien sind grundsätzlich nicht vertrauenswürdig. Nichtöffentliche Bereiche innerhalb sozialer Medien (z.B. Facebook, XING, LinkedIn, usw.) sind nicht als geschützte Bereiche zu betrachten.

2 Eine Benutzerregistrierung mittels der geschäftlichen E-Mail-Adresse ist, ausser in einem expliziten Zusammenhang mit der Arbeitstätigkeit, untersagt.

3 Die Bekanntgabe des Namens der Arbeitgeberin in einem persönlichen Benutzerprofil ist zulässig, wenn das Profil den Hinweis enthält, dass

a) es sich um ein persönliches Profil handelt, das nicht die Marke der Stadt Baden repräsentiert,

b) die gemachten Aussagen die persönliche Meinung des Profilinhabers sind und nicht zwingend mit der Meinung der Stadt Baden übereinstimmen.

4 Das automatische Synchronisieren geschäftlicher Kontaktdaten mit sozialen Netzwerken ist untersagt.

5 Erhalten IT-Benutzende innerhalb von sozialen Medien Anfragen, die die Stadt Baden betreffen, sind diese an die zuständigen internen Kommunikationsverantwortlichen weiterzuleiten.

§ 22 Speicherung von Informationen

1 Alle geschäftsrelevanten Daten müssen durch die Mitarbeitenden der Verwaltung der Stadt Baden auf den dafür bestimmten Informationssystemen der Stadt Baden gespeichert werden und sind vor unberechtigtem Zugriff zu schützen.

2 Geschäftsrelevante Daten im Sinn der geltenden Richtlinien zur Informationsverarbeitung dürfen temporär auf mobilen Informatikmitteln, lokalen Laufwerken, externen Datenträgern oder nicht geschäftlichen Speichersystemen (Cloud-Speicher usw.) abgespeichert werden. Die Informationen sind so rasch wie möglich auf die geschützten, dienstlichen Informations- bzw. Speichersysteme zu transferieren.

3 Informationen auf lokalen Laufwerken von mobilen und nicht dienstlichen Informatikmitteln (z.B. Notebooks oder Tablets) werden durch die Informatik nicht gesichert. Bei Störungen oder sicherheitsrelevanten Vorfällen können entsprechende Daten ohne Vorankündigung unwiderruflich gelöscht werden. Die Wiederherstellung und Verfügbarkeit dieser Daten ist somit nicht gewährleistet.

4 Persönliche Daten der Mitarbeitenden der Verwaltung der Stadt Baden dürfen auf dem dafür bestimmten persönlichen Datenbereich gespeichert werden. Diese Daten werden regelmässig gesichert.

5 Daten, die auf Informatiksystemen der Stadt Baden gespeichert sind, stehen im Eigentum der Stadt Baden. Die Vertraulichkeit dieser Daten kann nicht grundsätzlich gewährleistet werden.

§ 23 Unzulässige Nutzung von Informationen

1 Unzulässig ist jede unberechtigte Bearbeitung, Veröffentlichung oder Speicherung von Informationen, die

a) gegen diese Verordnung verstösst,

b) gegen das Urheberrecht, das Geschäftsgeheimnis, patentgeschützte oder weitere geschützte Rechte Dritter verstösst.

2 Missbräuchlich sind insbesondere folgende Nutzungen:

a) der eigenmächtige sowie gezielte effektive Zugriff auf Informationen, für die man nicht berechtigt ist,

b) widerrechtliches Kopieren, Verändern und Löschen von Daten und Informationen,

c) das dauerhafte Speichern von vertraulichen Informationen und besonders schützenswerten Personendaten auf Notebooks, Tablets, Smartphones, externen Datenträgern oder nicht geschäftlichen Speichersystemen (Cloud-Speicher usw.).[1]

3 Unzulässige Nutzungen im Internet sind:

a) das Verwenden von Elementen der Dachmarke (Logos, Claim usw.) der Stadt Baden in persönlichen Benutzerprofilen oder auf nicht offiziellen Webseiten,

b) das Verbreiten persönlicher Meinungsäusserungen, die dem Ansehen der Stadt Baden und ihren Mitarbeitenden oder der Mitglieder ihrer Behörden und Gremien schaden könnten,

c) das Publizieren von Aufnahmen (Bilder, Videos) in persönlichen Benutzerprofilen oder auf nicht offiziellen Webseiten, die teilweise oder gänzlich nichtöffentliche Räumlichkeiten der Stadt Baden zeigen.

---

[1] Die nebenamtlichen Mitglieder des Stadtrats sind von der Geltung dieser Bestimmung vorderhand ausgenommen.

V. Kontroll- und Überwachungsmassnahmen

§ 24 Zweck

Kontroll- und Überwachungsmassnahmen dienen in erster Linie der Überprüfung und Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit und der Verfügbarkeit der dienstlichen Informatikmittel.

§ 25 Zuständigkeit

1 Die vorgesetzten Stellen kontrollieren in Zusammenarbeit mit der Informatik die Einhaltung der vorstehenden Bestimmungen über den Gebrauch von Informatikmitteln der Mitarbeitenden.

2 Die Informatik ist zuständig für Kontroll- und Überwachungsmassnahmen zur Überprüfung und Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit und der Verfügbarkeit der dienstlichen Informatikmittel sowie das Durchführen entsprechender Auswertungen.

§ 26 Allgemein

1 Die Informatik betreibt Einrichtungen zur Durchführung der Kontroll- und Überwachungsmassnahmen sowie zur Optimierung der Netzwerkinfrastruktur. Diese ermöglichen, den Verkehr im Netzwerk systematisch zu untersuchen und auszuwerten.

2 Die Internetzugriffe und der E-Mail-Verkehr der IT-Benutzenden werden aufgezeichnet (protokolliert). Diese Protokolldaten können im Rahmen von § 29 zur Überprüfung des Vollzugs dieser Verordnung verwendet werden.

3 Die Informatik hat dafür zu sorgen, dass Auswertungen nur von den dazu autorisierten Systemverantwortlichen durchgeführt und vertraulich behandelt werden.

§ 27 Verhinderung von Missbrauch

1 Es können Netzwerküberwachungs- oder Netzwerkanalysewerkzeuge eingesetzt werden. Der Einsatz von Spionageprogrammen ist nicht gestattet.

2 Folgende Daten werden protokolliert:

a) Internetzugriffe: Benutzername, aufgerufene Internet-Adressen, Zugriffszeit, Zugriffsdauer, Grösse der heruntergeladenen Files.

b) E-Mail-Verkehr: Absenderadresse, Empfängeradresse, Betreffzeile, Datum, Zeit, Grösse des E-Mails und allfällige Attachments.

3 Protokolldaten gemäss § 27 Abs. 2 dieser Verordnung werden spätestens nach sechs Monaten vernichtet. Zu den Protokolldaten dürfen ausschliesslich die Systemverantwortlichen der Informatik Zugang haben. § 5 Abs. 2 VIDAG[1] bleibt vorbehalten.

4 Der Inhalt privater E-Mails, die als solche gekennzeichnet und somit erkennbar sind, darf ohne Zustimmung der betroffenen IT-Benutzenden nicht gelesen werden.

5 Die Stadt Baden behält sich vor, Zugriffe auf bestimmte Webseiten oder -Inhalte generell zu sperren.

§ 28 Sicherheit, Funktionsfähigkeit und Verfügbarkeit der dienstlichen Informatikmittel

1 Die Protokolldaten der Kontroll- und Überwachungsmassnahmen zur Überprüfung und Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit und der Verfügbarkeit der Informatikmittel sind in anonymisierter Form auszuwerten. Rückschlüsse auf bestimmte IT-Benutzende dürfen nicht möglich sein.

2 Werden Störungen festgestellt, die die Sicherheit, die Funktionsfähigkeit oder die Verfügbarkeit der Informatikmittel erheblich gefährden, dürfen die Protokolldaten ausnahmsweise personenbezogen ausgewertet werden, sofern dies zur Störungsbehebung unumgänglich ist. Die betroffenen IT-Benutzenden sind darüber zu informieren.

3 Für personenbezogene Auswertungen ist vorgängig die Einwilligung der Leitung Informatik einzuholen. Die Informatik erstattet der Verwaltungsleitung sowie der beauftragten Person für Öffentlichkeit und Datenschutz nachträglich Bericht über die durchgeführte Untersuchung und die allenfalls getroffenen Massnahmen.

4 Kann eine Information bzw. die Einwilligung vorgängig nicht sichergestellt werden, darf die Auswertung durchgeführt werden, sofern die Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit oder Verfügbarkeit der Informatikmittel keinen Aufschub erlaubt.

§ 29 Vollzug

1 Die Leitung Informatik kann nach vorgängiger Information der Verwaltungsleitung mittels der erwähnten Protokolldaten anonyme Plausibilitätskontrollen (Stichproben) über eine jeweils beschränkte Nutzungsdauer durchführen lassen, um den Vollzug dieser Verordnung zu überprüfen.

2 Besteht aufgrund von Überwachungs- und Analyseergebnissen oder gestützt auf den Antrag einer vorgesetzten Stelle ein erheblicher Verdacht auf Missbrauch der Informatikmittel, kann die Verwaltungsleitung gegenüber einem begrenzten Personenkreis eine zeitlich befristete Überwachung durchführen lassen.

3 Angeordnete Kontrollen sind den Betroffenen vorgängig schriftlich anzukündigen.

---

[1] Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG) vom 26. September 2007 [SAR 150.711]

4 Angeordnete Kontrollen sind unter Aufsicht der Leitung Informatik durchzuführen. Die beauftragte Person für Öffentlichkeit und Datenschutz ist vorgängig zu informieren. Über die durchgeführte Untersuchung und die allfällig getroffenen Massnahmen ist nachträglich ein Bericht zu verfassen.

5 Der Bericht (inkl. Auswertungsresultate) wird der Verwaltungsleitung und, sofern nötig, den direkt vorgesetzten Stellen der betroffenen Personen mitgeteilt.

VI. Sanktionen

§ 30 Disziplinar- und strafrechtliche Massnahmen

1 Bei Zuwiderhandlungen gegen die Bestimmungen dieser Verordnung kann der Arbeitgeber nach vorgängig erfolgloser Mahnung Disziplinarmassnahmen gemäss Personalreglement der Stadt Baden anordnen.

2 Die Strafverfolgung bei Erfüllung eines Straftatbestands bleibt vorbehalten.

VII. Schlussbestimmungen

§ 31 Inkrafttreten

1 Diese Verordnung tritt am 1. August 2017 in Kraft.

2 Sie ist allen IT-Benutzenden zugänglich zu machen.

§ 32 Aufhebung bisherigen Rechts

Diese Verordnung ersetzt die gleichnamige Verordnung vom 2. August 2011 und alle im Zeitpunkt ihres Inkrafttretens bestehenden Weisungen.

Baden, 27. März 2017

STADTRAT BADEN

Stadtammann
MÜLLER

Stadtschreiber
KUBLI

Anhang 1

der Verordnung über die Benutzung von Informatikmitteln und die Überwachung der Informationssicherheit vom 27. März 2017, gültig ab 1. August 2017, ersetzt bisherige Regelungen oder Erklärungen.

Sicherheitsvorgaben für den Zugriff auf interne Informationen und Systeme der Stadt Baden für Geschäftspartner und Lieferanten

1. Grundsatz

Informationen jeglicher Art (z.B. Dokumente, Bilder, Zeichnungen, Daten und Programme auf Papier oder magnetischen, elektronischen, optischen oder anderen Informationsträgern) stellen für die Stadt Baden verwaltungsinternes Know-how dar oder können sensitive Informationen enthalten. Diese Informationen sind zusammen mit den zu ihrer Verarbeitung und Übertragung eingesetzten Informationssystemen ein schützenswertes Eigentum der Stadt Baden.

2. Geheimhaltungsverpflichtung

Mitarbeitende von Geschäftspartnern und Lieferanten verpflichten sich, alle Informationen, von denen sie Kenntnisse erlangen, weder selbst zu verwerten noch anderen mitzuteilen. Diese Pflicht zu strikter Geheimhaltung gilt sowohl während eines Auftragsverhältnisses als auch nach dessen Beendigung.

Informationen dürfen nur für geschäftliche Zwecke kopiert und niemals an Dritte weitergegeben werden, weder im Original noch als Kopie noch sonstwie.

Die Geheimhaltungspflicht gilt auch für mündliche oder sonstwie zur Kenntnis gelangte Tatsachen.

3. Zutritts- und Zugangsberechtigungen

Soweit Mitarbeitende von Geschäftspartnern/Lieferanten Zutritts- und Zugangsberechtigen erhalten, sind diese nur im Rahmen der vereinbarten Aufgaben oder Tätigkeiten persönlich zu verwenden.

Diei Verletzung der Geheimhaltungspflicht kann zur Sperrung von Zutrittsberechtigungen zu Räumlichkeiten der Stadt Baden bzw. von Zugangsberechtigungen zu Informationen und Systemen führen sowie rechtliche Konsequenzen und Schadenersatzforderungen nach sich ziehen.

Ort und Datum	Unterschrift Geschäftspartner/Lieferant
……	……

© STADT BADEN, Informatik, 2017

Anhang 2

der Verordnung über die Benutzung von Informatikmitteln und die Überwachung der Informationssicherheit vom 27. März 2017, gültig ab 1. August 2017, ersetzt bisherige Regelungen oder Erklärungen.

Sicherheitsvorgaben für die Nutzung der papierlosen elektronischen Sitzungsführung (PES) durch Mitglieder der Behörden und Gremien

1. Grundsatz

Die Stadt Baden legt grossen Wert auf die Gewährleistung der Invormationssicherheit und der Einhaltung des Datenschutzes. Sie trifft alle ihr möglichen technischen und organisatorischen Massnahmen, um diese Anforderungen sicherzustellen.

Mit der Bereitstellung von Informationen in den Anwendungen für die papierlose elektronische Sitzungsführung (PES) geht eine entsprechende Sorgfalts- und Verantwortungpflicht an die Nutzenden dieser Lösungen über.

2. Bestimmungen

Die Nutzenden der papierlosen elektronischen Sitzungsführung (PES) der Behörden und Gremien der Stadt Baden sind sich bewusst, dass die publizierten Informationen teilweise vertraulich sind und treffen alle zumutbaren Vorkehrungen, damit Datenschutz und Informationssicherheit gewährleistet werden kann.

Die Nutzenden stellen im Einzelnen sicher, dass

- die für den Zugang zur papierlosen elektronischen Sitzungsführung (PES) genutzten privaten Informatikmittel mittels Passwortschutz für den unberechtigten Zugriff durch Dritte geschützt sind,
- die persönlichen Benutzeridentifikationen (Loginangaben bzw. insbesondere Passwörter / Pincode) geheim gehalten werden,
- die publizierten Dokumente mit vertraulichen Daten weder durch unberechtigte Dritte eingesehen noch weitergegeben werden können (z.B. per E-Mail),
- nach jedem Besuch eine korrekte Abmeldung erfolgt und die genutzten Anwendungen (Web-Browser und/oder Mobile App) wieder geschlossen werden.

© STADT BADEN, Informatik, 2017