STADT GRAZ MAGISTRATSDIREKTION

Bericht an den Gemeinderat

BearbeiterIn: DI Josef Robert Zeiler

BerichterstatterIn: ……..

GZ: 024399/2014/11

Graz, 15. Mai 2014

Stand der Maßnahmen zur Datensicherheit und zum Datenschutz im Haus Graz

Motivenbericht

1. Zusammenfassung

Das Thema Informationssicherheit/Datensicherheit/Datenschutz spielt in der öffentlichen Verwaltung generell und so auch im Magistrat Graz und im Haus Graz seit jeher eine große Rolle. Es wurden bisher schon wesentliche Anstrengungen unternommen, um die Datensicherheit und den Datenschutz zu gewährleisten.

So wurde beispielsweise im Frühjahr 2013, mit dem Beschluss der „Informationssicherheitspolitik Haus Graz V3.0“ (ISP 3.0) durch den ITG-KundInnenbeirat, eine Haus-Graz-weite Organisation zur strukturierten Planung und Umsetzung von Maßnahmen zur Informationssicherheit geschaffen, welche die bisherige Organisation des bereits seit 2005 geltenden Informationssicherheitsmanagements abgelöst hat.

In dieser ISP 3.0 sind die Zielsetzungen, die Aufbauorganisation und die Verantwortlichkeiten für das Informationssicherheitsmanagement im Haus Graz festgelegt. So wurde beispielsweise das sog. Informationssicherheits-Kompetenzteam (ISKT) als interdisziplinäres ExpertInnenteam geschaffen, welches die Aufgabe hat, Informationssicherheitsthemen zu sammeln, zu priorisieren, in entsprechende Maßnahmen „zu gießen“ und deren Umsetzung zu initiieren und zu überwachen. Die Leitung des ISKT obliegt dabei den InformationssicherheitsmanagerInnen des Magistrat Graz und der Holding Graz.

Im Herbst 2013 nahm das ISKT seine Arbeit auf und begann die wichtigsten Haus-Graz-weit relevanten IS-Themen zu sammeln, zu strukturieren und zu priorisieren. Ende 2013 war somit eine Liste von zu planenden IS-Projekten entstanden, von welchen bis März 2014 vier konkrete und relativ umfangreiche Informationssicherheits-Projekte im Detail ausgearbeitet und am 2. April 2014 durch den ITG-Beirat in Auftrag gegeben wurden.

Der Inhalt dieser Projekte befasst sich im Wesentlichen mit der Aktualisierung bzw. Ausarbeitung und Haus-Graz-weiten Veröffentlichung der unter Punkt 3 näher dargestellten Informationssicherheits-Richtlinien (IS-Richtlinien) und der Umsetzung konkreter Maßnahmen bis ins Jahr 2015.

Abgesehen von der Neustrukturierung des Informationssicherheitsmanagements im Haus Graz und den geplanten Projekten wird das Thema Datensicherheit und Datenschutz in den einzelnen Organisationen des Hauses Graz sehr ernst genommen.

Verantwortlich für die **technische** Informationssicherheit im Haus Graz ist die ITG GmbH, zu deren Hauptaufgaben es gehört, elektronische Informationen technisch gegen fremden Zugriff abzusichern. Für die **organisatorische** Informationssicherheit zeichnen die einzelnen

Abteilungsleitungen und Geschäftsführungen des Hauses Graz verantwortlich. Im Magistrat Graz gibt es derzeit keine/n zentrale/n „Datenschutzbeauftragte/n“, da diese Funktion gesetzlich nicht verpflichtend ist. Sehr wohl aber ist die Präsidialabteilung für die Rechtsberatung zum Thema Datenschutz für die Fachabteilungen zuständig.

Nur durch das optimale Ineinandergreifen von technischen und organisatorischen Maßnahmen können Risiken, die in der Informationsverarbeitung auftreten wirksam vermindert werden.

Die wesentlichen Grundbedrohungen in der Informationsverarbeitung sind:

Die Bedrohung der Vertraulichkeit …	betrifft vor allem Daten. Es ist daher alles Notwendige zu unternehmen, um zu verhindern, dass Daten in unbefugte Hände geraten.
Die Bedrohung der Integrität …	betrifft ebenfalls Daten, Programme, Hardware und alle sonstigen für die Verarbeitung notwendigen Mittel. Es ist daher alles Notwendige zu unternehmen, um zu verhindern, dass Daten verfälscht werden oder falsche Daten verarbeitet werden.
Die Bedrohung der Verfügbarkeit …	betrifft Daten, Programme, Hardware und alle sonstigen für die Verarbeitung notwendigen Mittel. Es ist daher alles Notwendige zu unternehmen, um zu verhindern, dass Daten verschwinden oder nicht verfügbar sind, wenn sie gebraucht werden.
Die Bedrohung der Authentizität …	betrifft vor allem Daten, insbesondere Dokumente und Urkunden, die elektronisch übertragen werden. Es ist daher möglichst alles zu unternehmen, dass die Herkunft solcher Daten und die Urheber dieser Daten korrekt authentifiziert werden können.

2. Derzeit im Haus Graz umgesetzte Maßnahmen zum Datenschutz und zur Datensicherheit

2.1. Derzeit im Magistrat Graz in Anwendung befindliche **organisatorische** Maßnahmen zur Informationssicherheit sind:

- Gültige Richtlinien/Erlässe zum Thema Informationssicherheit im Magistrat sind (Links siehe Beilage):
  - Informationssicherheitspolitik Haus Graz V3.0
  - IS-Richtlinie zur „BenutzerInnenverwaltung in IT-Strukturen“
  - IS-Richtlinie „Kennwort-Richtlinie“
  - IS-Richtlinie „Benutzung und Behandlung von elektronischer Post“ (Email-Richtlinie)
  - IS-Richtlinie zur „Benutzung des Internets“

- Präsidialerlass 25/2005 zu IS-Richtlinien und Informationssicherheits-management
- Präsidialerlass 34/2002 Allgemeine Datenschutzvorschriften
- Präsidialerlass 36/2002 Datensicherheitsvorschrift für das ZMR
- Präsidialerlass 22/2012 Registerabfragen gem. E-GovG
- Präsidialerlass 20990/2003-1 Ablage- und Skartierungsordnung (ASO)

- Im Rahmen der Umsetzung des Projektes zur Einführung eines Internen Kontrollsystems (IKS) im Magistrat Graz wird derzeit eine neuerliche Erhebung aller im Einsatz befindlichen IT-Fachanwendungen und eine Risikoanalyse dieser Anwendungen durchgeführt.
  Ziel ist die Entdeckung von Risiken bzw. Sicherheitslücken in der Verwendung dieser IT-Systeme und der darin gespeicherten Daten und das Ergreifen entsprechender Sicherungsmaßnahmen. Die Risikoanalyse von Fachanwendungen ist ein stetig wiederkehrender Prozess, da sich einerseits Risiken aber auch die Fachanwendungen selbst mit der Zeit verändern können.

- Um der Bestimmung des § 14 Abs 2 Z 3 DSG Rechnung zu tragen, wird zusätzlich zu den bis dato schon durchgeführten Datenschutzschulungen für bestehende MitarbeiterInnen, seit Herbst 2013 jedem/jeder neu in den Magistrat eintretenden Mitarbeiter/Mitarbeiterin durch das Personalamt ein Merkblatt nachweislich zur Kenntnis gebracht, welches zur Unterweisung betreffend Datenschutz dient.

- Die Beantragung von Zugriffsberechtigungen auf jegliche IT-Systeme ist geregelt, unterliegt generell einem abteilungsinternen 4-Augen-Prinzip und wird technisch über ein Intranetformular (Anforderung von Berechtigungen in IT-Strukturen an die ITG) abgewickelt. Jede Anforderung wird seitens der ITG dokumentiert.

- Für Zugriffe von Fachabteilungen auf zentrale Register, wie zB auf ZMR über das Portal Austria, wird vorab durch die Präsidialabteilung geprüft, ob eine entsprechende rechtliche Grundlage für die gewünschten Zugriffe besteht. Wenn diese gegeben ist, erhält die Fachabteilung durch die Präsidialabteilung pauschal die Bestätigung, dass die Zugriffe rechtlich gedeckt sind. Die Fachabteilungsleitung entscheidet daraufhin selbst, für welche/n Mitarbeiter/in ein Zugriff beantragt werden soll. Die Präsidialabteilung führt eine Liste aller für die jeweiligen Fachabteilungen genehmigten, zentralen Registeranwendungen.

- Für die ca. 560 BenutzerInnen des ZMR im Magistrat wurde seitens der zuständigen Fachabteilung BürgerInnenamt ein Schulungshandbuch, welches die wesentlichsten Hinweise in Bezug auf Datenschutz beinhaltet, über das e-learning-Portal verfügbar gemacht. Durch diese Verfahrensweise ist die nachweisliche Unterweisung von ZMR-Usern betreffend Datenschutz sichergestellt.

- Sämtliche PCs sind passwortgeschützt. Die geltende IS-Richtlinie zur Verwendung von Kennwörtern (Kennwortrichtlinie) wurde 2013 an den Stand der Technik angepasst. Vorgeschrieben sind seither die Verwendung ausreichend langer Kennwörter und deren Änderung alle 90 Tage.

- Im Rahmen der Dienstprüfungskurse für neue MitarbeiterInnen erfolgt die Behandlung des Themas Datenschutz durch die einzelnen ReferentInnen.

- Im Rahmen des Einführungstages für neue Bedienstete wird das Thema Datenschutz in Form eines kurzen Blockes abgehandelt.

2.2 Die Stellungnahme der **ITG** für die in Anwendung befindlichen **technischen** Maßnahmen zur Informationssicherheit lautet wie folgt:

Grundsätzliches:

- IT-Sicherheit ist nicht Selbstzweck: Es müssen Risikos erkannt und Maßnahmen ganz bewusst gesetzt werden mit dem einzigen Zweck diese Risiken gezielt zu verringern!
- IT-Sicherheit geschieht nicht von allein: Die zu setzenden Maßnahmen initiieren sich nicht von selbst, sie müssen ganz bewusst beauftragt werden.
- IT-Sicherheit braucht Ressourcen: Die Umsetzung beauftragter Maßnahmen ist nur durch Einsatz von Arbeitszeit, Hard- und Software möglich.
- Die ITG liefert IT-Security die den momentanen Sicherheitsstandards entsprechen und auf dem BSI-Grundschutzkatalog aufbauen.
- Aufgrund der sich ständig ändernden Entwicklungen identifizieren wir neue Risiken, die durch organisatorische und technische Maßnahmen abgefangen werden müssen.
- Um die Notwendigkeit für IT-Sicherheitsmaßnahmen zu verdeutlichen, muss bei den Verantwortlichen das dafür nötige Bewusstsein geschaffen werden.
- Dimensionen der Informationssicherheit:
    - Confidentiality – Vertraulichkeit: Informationen dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden, dies gilt sowohl beim Zugriff auf gespeicherte Daten, wie auch während der Übertragung.
    - Integrity – Integrität: Informationen dürfen nicht unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein.
    - Availability – Verfügbarkeit: Der Zugriff auf Informationen muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein.
    - Authentizität, Nichtabstreitbarkeit: Bei Überprüfung der Informationen muss eindeutig feststellbar sein, von wem sie wann erstellt wurden (elektronische Signaturen, Bürgercard).

Aktuell umgesetzte Maßnahmen:

- Netzwerkbereich:
    - Eine Firewall mit Intrusion Prevention in unsere Domain und in die Demilitarisierte Zone DMZ (e-Government-Plattform, …) überwacht den Internetverkehr und unterbricht verdächtige Verbindungen.
    - Eine weitere Firewall zwischen der Demilitarisierten Zone und unserem internen Benutzernetz verhindert verdächtige Verbindungen von unseren eigenen Webservern in unser internes Netz.
    - Eine weitere Firewall mit Intrusion Detection zwischen Benutzernetz und Servern verhindert, dass verdächtige Verbindungen zwischen unseren Webservern und unseren Arbeitsservern aufgebaut werden können.
    - Der Internetverkehr zwischen unserem internen Netz und dem Internet wird stark reglementiert und beschränkt:

        - Der gesamte HTTP-Traffic kann ausschließlich über einen Zwischenserver (Proxy-Server) abgewickelt werden, auf dem Inhalte auf Malware überprüft und gegebenenfalls geblockt werden.
        - Der Virenscan überprüft ein- und ausgehende Informationen auf bekannte Viren. Aktualisierungen auf aktuelle Virenmuster werden permanent durchgeführt.
        - Heuristic Scans ermöglichen Überprüfungen auf noch nicht bekannte aber verdächtige Muster (Tag- 0 Bedrohungen)
    - Mehrstufiger Virenscan am Mail-Server für ein- und ausgehende Mails (EXCHANGE).
    - Zugang in unser internes Netz z.B. für MitarbeiterInnen oder Partnerfirmen erfolgen ausschließlich über gesicherte und hoch sicher verschlüsselte Internettunnel (Virtual Private Network VPN). Die Identifizierung für jede Benutzerin erfolgt über individuelle Token-Passworte, die im Minutentakt neu generiert werden und dann wieder ungültig sind (RADIUS-One-Time-Passwords)
    - Interner Zugang ins Firmennetz und Rechteverwaltung über ACTIVE-DIRECTORY-Authentifizierung
    - Interne Zugänge in unser Netz und damit individuell gestaltbare Zugriffe auf interne Ressourcen sind nur über Single-Sign-On Mechanismen möglich. (ACTIVE DIRECTORY , KERBEROS)
    - Sobald neue Bedrohungen bekannt werden, arbeiten die entsprechenden Firmen an Patches und veröffentlichen diese so rasch wie möglich. Mit diesen Updates werden periodisch alle Server und Clients aktualisiert.
    - Public Key Infrastructure:
        - Die Verwendung eines Haus Graz eigenen Root-Zertifikates dient zur Identifizierung aller internen Devices und Dienste (Webserver…)
        - Intern: Für jede MitarbeiterIn und jedes Gerät existiert ein nur für sie/es und nur im Haus Graz gültiges Zertifikat. Dadurch sind nur Verbindungen für Benutzerinnen/Geräte mit einem entsprechenden Zertifikat möglich.
        - Dadurch wird durch die Verwendung dieser Zertifikate sichergestellt, dass alle internen Verbindungen im gesamten internen Netz verschlüsselt werden sowie, dass nur Geräte verwendet werden können, die durch so ein individuelles Zertifikat dafür autorisiert sind.
        - Extern: Verwendung internationaler Zertifikate für alle nach außen gehenden Dienste (Webserver…), denen von jedem Browser vertraut wird (VERISIGN), ermöglicht sicher verschlüsselte Verbindungen mit allen externen Internetservern
        - Die personalisierte, digitale Signatur ersetzt rechtlich die manuelle Unterschrift und verhindert eindeutig nachweisbar die nachträgliche Veränderung eines digital signierten Dokuments.

- Serverbereich:

    - Durch periodische Aktualisierung der Patchlevel werden alle bekannten Bedrohungen ausgeschlossen.
    - Die Verwendung eines Infrastruktur -Monitoring-Systems alarmiert bei kritischen Vorfällen die für das jeweilige Service zuständige Person, um sofortige Interventionen durchführen zu können (NAGIOS).
    - Redundante Serverarchitekturen an zwei getrennten Standorten ermöglichen bei Ausfall die sofortige Übernahme jedes Services am jeweils anderen Standort.
    - Durch Zutrittsberechtigungen zu beiden Serverräumen wird die physische Manipulation an den Servern verhindert.

- Alle Clients
    - Ein eindeutiges Zertifikat stellt sicher, dass nur autorisierte Geräte im internen Netz arbeiten können (802.1x)
    - Alle Windows Geräte werden zentral durch den System Center Configuration Manager SCCM verwaltet und überwacht. Dadurch werden folgende Punkte sichergestellt:
        - Stetig aktualisierter Virenschutz
        - Periodische Aktualisierung der Patchlevel
        - Möglichkeit zur Plattenverschlüsselung auf mobilen Endgeräten (BITLOCKER)
    - Möglichkeit zur Zentralen Verwaltung und Überwachung von Geräten mit IOS, Android (MOBILEIRON)

- Organisatorische Maßnahmen
    - Das Risiko-Management-System behandelt bekannte Bedrohungen und wird zumindest einmal jährlich um neue Bedrohungen aktualisiert.
    - Ein periodisch revisionierter ITG interner Prozess dient zur Identifizierung und Bewertung bestehender und möglicher zukünftiger Risiken.
    - Unser Informations-Sicherheits-Management-System (ISMS) wird ebenfalls jährlich durch externe Audits geprüft und dient dazu, den erkannten Bedrohungen Maßnahmen gegenüberzustellen.
    - Sämtliche periodische Überprüfungen aller sicherheitsrelevanten vordefinierten Prozesse werden durch ein internes Kontrollsystem (IKS) in Zukunft automatisiert angestoßen.
    - Für alle sicherheitsrelevanten Maßnahmen sind periodische Zeiträume definiert, in denen sie durchgeführt, auf Aktualität überprüft und überarbeitet werden müssen.
    - Für Katastrophenszenarien wurde ein Desaster-Recovery-Plan DRP erstellt, der die möglichst rasche Wieder-Inbetriebnahme aller relevanten Services in priorisierter Reihenfolge sicherstellt. Dieser DRP wird jährlich überarbeitet und durch Testszenarien überprüft.
    - Periodische Security Audits durch wechselnde externe Firmen garantieren eine möglichst umfassende IT-Sicherheit und sollen ein Übersehen bestimmter Bereiche durch Betriebsblindheit verhindern.
    - Die Informationssicherheitspolitik regelt die Basis aller sicherheitstechnischen Prozesse.
    - Durch die Verwaltung aller Assets (Hardware, Software, Services) in einem zentralen Tool (OMNITRACKER) und aller damit zusammenhängenden

Metadaten, wird sichergestellt, dass alle relevanten Informationen zur Servicierung, Wartung und Wiederherstellung verfügbar sind.

Geplante Maßnahmen

- Vermeidung von fahrlässigem Verhalten jeder einzelnen MitarbeiterIn durch Übernahme von Verantwortung für ihren Tätigkeitsbereich in Form einer unterschriebenen diesbezüglichen Erklärung.
- Verbindliche und regelmäßige Teilnahme an IT-Sicherheits-Schulungen mit Erfolgsüberprüfung.
- Erarbeitung von ISKT-Richtlinien: Haus-Graz weit abgestimmte Richtlinien berücksichtigen aktuelle Bedrohungen und regeln den harmonisierten Umgang zu folgenden Themenschwerpunkten:
  - RL Mobile Devices
    - Obligatorische Plattenverschlüsselung auf mobilen Endgeräten
  - RL Fileserverstruktur
    - Zentrale B Berechtigungsorganisation aller Fileshares
  - RL Datenschutz
  - RL Mitarbeiter Eintritt, - Austritt und -Wechsel
    - Initiale und periodische Maßnahmen zur
    - Bewusstseinsbildung und Schulung der MA auf sicherheitsrelevante Themen
    - Revisionssichere Verwaltung der MA-Berechtigungen (IAM)

Beispiele weiterer möglicher Maßnahmen zur Verbesserung der IT-Sicherheit

- Verschärfung der PW-Richtlinie:
  - Zusätzliche Verwendung von Sonderzeichen
  - Mindestlänge von 12 Zeichen
  - Zurverfügungstellung eines Passwort-Stores
- 2 Faktor Sign on (Fingerprint + Passwort)
- Nutzung von Mail-Einzelzertifikaten für jeden einzelnen Adressaten zur Verschlüsselung des Mailinhalts zB mit PGP,GPG oder SMIME. Die Mailadresse muss per Definition immer unverschlüsselt übertragen werden.
- Versendung amtlicher Mails durch ausschließliche Nutzung von Zustelldiensten

2.3 **Die Stellungnahme** der **Holding Graz** für die in Anwendung befindlichen **organisatorischen** Maßnahmen zur Gewährleistung der Informationssicherheit lautet wie folgt:

In der Holding Graz GmbH hat man sich schon frühzeitig mit dem gewissenhaften Umgang mit Daten beschäftigt.

Bereits 1978 wurde eine Dienstanweisung, die die Behandlung, das Genehmigungsverfahren von EDV-Auswertungen und Statistiken, im speziellen mit personenbezogenen Daten, beschreibt, erlassen. Dienstanweisungen mit den Themen: Zeichnungsbefugnisse von Schriftstücken mit Außenwirkung, Internet- und E-Mail-Nutzung, Benutzerkennwortregelung etc. folgten.

Im Rahmen des Datenschutzgesetzes 2000 wurden die Bestimmungen betreffend personenbezogene Daten näher beschrieben und den MitarbeiterInnen in Form einer Dienstanweisung zur Kenntnis gebracht.

Im Jahr 2006 erfolgte eine IT-Sicherheitsüberprüfung im Geschäftsbereich Informationstechnik. Als logische Weiterentwicklung führte der Geschäftsbereich Informationstechnik ein IT-Risikomanagement (inkl. der IT-Sicherheitspolitik) ein. Das IT-Risikomanagement erfolgte in Abstimmung mit dem Konzern-Risikomanagement (Genehmigung der Konzern-Risikomanagementrichtlinien 2007).

Im Jahre 2012 wurden die Konzernrichtlinien mit dem Ziel, grundlegende Regeln unter einer einheitlichen fachlichen, organisatorischen und EDV-technischen Systematik festzulegen, verabschiedet. Berücksichtigt werden alle Standards und Vorgaben, die für den Konzernbetrieb maßgeblich sind.

In Zusammenarbeit mit dem Magistrat Graz erfolgte im Jahr 2011 der Start einer gemeinsamen Informationssicherheitspolitik für das Haus Graz, welche im März 2013 in Kraft gesetzt wurde.

In der Holding Graz GmbH wurde Anfang 2013 mit dem Informationssicherheitsprojekt gestartet. Als erster Schritt erfolgte die Bestandsaufnahme aller informationssicherheitsrelevanter Anweisungen und Richtlinien. Ziel ist es, den Informationssicherheitsstand der Holding entsprechend den Vorgaben des Österreichischen Informationssicherheitshandbuches zu aktualisieren bzw. adaptieren und allen MitarbeiterInnen zur Verfügung zu stellen.

Im ITG-KundInnenbeirat wurden u.a. folgende Richtlinien bzw. Projekte beauftragt:

- Richtlinie zum Umgang mit mobilen Geräten und Datengeräten
- Richtlinie zur Vergabe und Verwaltung von Berechtigungen
- Richtlinie zur Definition der Daten und Dokumentenklassen
- Richtlinie für digitale und analoge Datenhaltung
- Richtlinie zur Ersten Hilfe bei sicherheitskritischen Ereignissen
- Richtlinie zur E-Mailnutzung
- IS-Projekt „mobile Devices“
- IS-Projekt „Datenschutz“
- IS-Projekt „Eintritt, Austritt und Wechsel von MitarbeiterInnen“
- IS-Projekt „Fileserverstrukturen und –berechtigungen“

Diese Projekte werden in Zusammenarbeit mit dem Magistrat Graz, der ITG und Holding Graz umgesetzt.

2.4 **Die Stellungnahme** der **GBG** für die in Anwendung befindlichen **organisatorischen** Maßnahmen Informationssicherheit lautet wie folgt:

Im November 2012 wurde in der GBG die Position einer Datenschutzbeauftragten besetzt.

Die GBG verwendet ausschließlich Standardanwendungen iSd. § 17 Abs 2 Z 6 DSG.

Bereits durchgeführte Maßnahmen:

- In den jeweils relevanten SLAs wurden datenschutzrechtliche Bestimmungen aufgenommen, so beispielsweise in den wechselseitigen SLAs zwischen ITG und GBG. (Der technische Datenschutz wird von der ITG im Rahmen des SLAs sichergestellt)
- Sämtliche PCs sind passwortgeschützt. Die Passwörter müssen in regelmäßigen Abständen erneuert werden.
- Die Dienstverträge sämtlicher Kollektivvertragsbediensteten enthalten die folgende datenschutzrechtliche Bestimmung:

Der Treuepflicht entsprechend hat die Dienstnehmerin unter anderem streng die Betriebs- und Geschäftsgeheimnisse zu wahren und zwar auch nach Ende des Dienstverhältnisses. Gleiches gilt für sonstige Daten und Umstände, die ihrer Art nach einer vertraulichen Behandlung bedürfen. Auch das Datengeheimnis gemäß Datenschutzgesetz ist zu wahren.

Weiters wurde eine eigene Dienstanweisung (8/2013) für alle MitarbeiterInnen erstellt, in der auf die generelle Verpflichtung zur Einhaltung sämtlicher datenschutzrechtlicher Bestimmungen hingewiesen wurde.

- Sämtliche MitarbeiterInnen, die mit Personalstammdaten arbeiten, verfügen über versperrbare Kästen, um den Schutz der Personalunterlagen zu gewährleisten. Weiters wurde für diese MitarbeiterInnen ein Datenschutzblatt erstellt, um verstärkt auf die Verpflichtung zur Einhaltung des Datenschutzes hinzuweisen.
- Sämtliche Email-Signaturen enthalten den folgenden datenschutzrechtlichen Hinweis, der an sämtliche MitarbeiterInnen kommuniziert wurde:

Dieses Email und alle damit verbundenen Anlagen sind vertraulich und ausschließlich für den benannten Adressaten bestimmt. Sollten Sie dieses Email irrtümlich erhalten haben, bitten wir Sie, uns umgehend zu benachrichtigen, sämtliche Ausdrucke zu vernichten und dieses Email sowie sämtliche Anhänge zu löschen.

- Für Aufsichtsräte der GBG Gebäude- und Baumanagement Graz GmbH wurde ein eigenes Sharepoint-Portal aufgebaut, in dem sämtliche relevanten Dokumente abrufbar sind. Bevor ein Zugriffsrecht vergeben wird, ist jede/r NutzerIn verpflichtet, eine datenschutzrechtliche Erklärung zu unterfertigen.
- Weiters wurde bei den MitarbeiterInnen die Zustimmung zur Verwendung der Fotos im Internetauftritt der GBG sowie im Intranet des Hauses Graz bis auf Widerruf eingeholt.
- Der Zugang zu den Büroräumlichkeiten ist durch ein Sicherheitsschloss geschützt.

Geplante Maßnahmen:

- Momentan wird an der Erstellung eines eigenen Datenschutzhandbuches für alle MitarbeiterInnen der GBG gearbeitet. Dieses soll bis Mitte des Jahres 2015 fertig gestellt werden.
- Aktuell wurde beim Datenverarbeitungsregister um Registrierung einer Wildkamera angesucht. Sobald das Verfahren abgeschlossen ist, sind umfassende Schulungen für die betroffenen MitarbeiterInnen geplant.
- Weiters sind Schulungen für alle MitarbeiterInnen geplant, um für das immer wichtiger werdende Thema „Datenschutz" zu sensibilisieren.

3. seitens des ITG-KundInnenbeirates beauftragte Maßnahmen zum Datenschutz und zur Datensicherheit im Haus Graz

3.1 Informationssicherheits-Richtlinien

Folgende IS-Richtlinien werden im Lauf des kommenden Jahres überarbeitet bzw. erarbeitet:

- Richtlinie zur Fileserverstruktur
- Richtlinie zum Umgang mit mobilen Geräten und Datenträgern
- Richtlinie zur Vergabe und Verwaltung von Berechtigungen
- Richtlinie zur Definition der Daten und Dokumentenklassen
- Richtlinie für digitale und analoge Datenhaltung
- Richtlinie zur Benutzung zentraler Register (nur MG)
- Richtlinie zur Ersten Hilfe bei sicherheitskritischen Ereignissen
- Richtlinie zur Emailnutzung
- Richtlinie zur IT-Equipment-Entsorgung und Vernichtung von personenbezogenen Daten
- Richtlinie zur Datensicherheit/Datenschutz

Die o. a. IS-Richtlinien, welche im Magistrat den Stellenwert eines Präsidialerlasses und in der Holding den Stellenwert eines Vorstandsbeschlusses haben, sind die Grundlage für die Umsetzung konkreter Informationssicherheitsmaßnahmen durch die ITG und die anderen Organisationen im Haus Graz.

3.2 kurz vor der Umsetzung befinden sich folgende sonstige Informationssicherheits-maßnahmen

<u>IS-Projekt „mobile devices"</u>

- Erstellung von allgemeinen Informationen zur Benutzung von mobilen Geräten seitens der Auftraggeberorganisationen, die BenutzerInnen bei der Ausgabe der Geräte nachweislich erhalten und welche auch online im Haus Graz verfügbar sind
- Überarbeitung des Prozesses „Ausgabe von Mobilgeräten" durch die ITG
- Überarbeitung des Prozesses „Entsorgung von Mobilgeräten" durch die ITG
- Zentrale Verwaltung der im Haus Graz im Einsatz befindlichen mobilen Geräte (Telefone, Tablets, Laptops) durch die ITG mit einer technischen Lösung.
  Die effiziente Verschlüsselung und zentrale Verwaltung von Smartphones, Tablets

etc. wird nur durch den Einsatz einer entsprechenden Verwaltungssoftware in der ITG sichergestellt. Es wird dadurch auch eine sofortige Löschung der am Gerät gespeicherten Daten im Falle eines Verlustes möglich (über ITG-Serviceline oder auch Self-Service-Tool für User).

IS-Projekt „Datenschutz“

- Einrichtung eines e-learning Tools zum Thema Datenschutz, welches für MitarbeiterInnen verpflichtend zu absolvieren ist
- Einrichtung eines e-learning Tools zum Thema Informationssicherheit, welches für MitarbeiterInnen verpflichtend zu absolvieren ist
- Konzeption der Vermittlung der Informationen zu Datenschutz und Informationssicherheit auch an jene MitarbeiterInnen, welche keinen Zugriff auf einen PC haben
- Einrichtung einer Intranetseite zum Thema Datenschutz

IS-Projekt „Eintritt, Austritt und Wechsel von MitarbeiterInnen“

- Anpassung/Vereinheitlichung des Prozesses des **Eintritts von MitarbeiterInnen** in das Haus Graz
- Anpassung/Vereinheitlichung des Prozesses des **Austritts von MitarbeiterInnen** aus dem Haus Graz
- Anpassung/Vereinheitlichung des Prozesses des **Wechsels von MitarbeiterInnen** innerhalb des Hauses Graz
- Erarbeitung einer Strategie zur künftigen elektronischen Verwaltung von Organisationsstrukturen und Berechtigungen
- Erarbeitung der Inhalte einer allgemeinen Grundeinschulung/-einführung für neue MitarbeiterInnen im Haus Graz und Festlegung der Vermittlung von Pflichtinhalten zum Thema Datenschutz und Informationssicherheit

IS-Projekt „Fileserverstrukturen und -berechtigungen“

- Neustrukturierung des Fileservers und der Berechtigungsverwaltung im Magistrat

Nach Umsetzung oben angeführter Informationssicherheitsmaßnahmen erfolgt die Detailplanung und Beauftragung weiterer Maßnahmen, welche im ISKT gesammelt wurden.

Fazit: Die verantwortlichen Stellen im Haus Graz sind sich der stetig zunehmenden Komplexität in der Informationsverarbeitung und den damit verbundenen, stetig steigenden Risiken in Bezug auf Datensicherheit und Datenschutz absolut bewusst.

Eine konsequente Abwehr dieser Gefahren kann allerdings nur gelingen, wenn auch künftig ausreichend Ressourcen dafür bereitgestellt werden.

Dennoch verbleiben, wie der jüngste Fall, welcher weltweit für Aufregung gesorgt hat („Heartbeed“- Sicherheitslücke in OpenSSL), zeigt, trotz optimalem Einsatz von Ressourcen

gewisse technische aber auch menschliche Restrisiken im Umgang mit elektronischen Informationen.

Der Ausschuss für Verfassung und Organisation

stellt daher gemäß § 45 Abs 6 Statut

den

A n t r a g,

der Gemeinderat wolle vorliegenden Informationsbericht zur Kenntnis nehmen:

Der Bearbeiter:

Der Magistratsdirektor: Der Bürgermeister:

Vorberaten und einstimmig/mehrheitlich/mit …… Stimmen angenommen/abgelehnt/ unterbrochen in der Sitzung des

Ausschusses für Verfassung und Organisation am ……..

Der/die Schriftführerin Der/die Vorsitzende:

Abänderungs-/Zusatzantrag:

Der Antrag wurde in der heutigen	☐	öffentlichen	☐	nicht **öffentlichen Gemeinderatssitzung**

☐	**bei Anwesenheit von …… GemeinderätInnen**		
☐	einstimmig	☐	mehrheitlich (mit …… Stimmen /…… Gegenstimmen) angenommen.
☐	Beschlussdetails siehe Beiblatt		
Graz, am ……..		Der/die Schriftführerin:	

Beilage/n:

- LINK: Informationssicherheitspolitik Haus Graz V3.0
  https://mitarbeiter.graz.at/amt/Interne%20Vorschriften/IS-Politik.pdf
- LINK: IS-Richtlinie zur „BenutzerInnenverwaltung in IT-Strukturen“
  https://mitarbeiter.graz.at/amt/Interne%20Vorschriften/ISRichtlinieBenutzerverwaltung.pdf
- LINK: IS-Richtlinie „Kennwort-Richtlinie“
  https://mitarbeiter.graz.at/amt/Interne%20Vorschriften/956139_3.1_IS-RICHTLINIE-KENNWORT_V2_0_ENDVERSION.pdf
- LINK: IS-Richtlinie „Benutzung und Behandlung von elektronischer Post“ (Email-Richtlinie)
  https://mitarbeiter.graz.at/amt/Interne%20Vorschriften/IS-Richtlinie_E-Mailnutzung.pdf
- LINK: IS-Richtlinie zur „Benutzung des Internets“
  https://mitarbeiter.graz.at/amt/Interne%20Vorschriften/IS-Richtlinie_Internetnutzung.pdf
- LINK: Präsidialerlass 25/2005 zu IS-Richtlinien und Informationssicherheitsmanagement
  https://mitarbeiter.graz.at/amt/Praesidialerlaesse/Präs. 25 - IS-Richtlinien.doc
- LINK: Präsidialerlass 34/2002 Allgemeine Datenschutzvorschriften
  https://mitarbeiter.graz.at/amt/Praesidialerlaesse/Präs. 34 - Allgemeine Datenschutzvorschriften.pdf
- LINK: Präsidialerlass 36/2002 Datensicherheitsvorschrift für das ZMR
  https://mitarbeiter.graz.at/amt/Praesidialerlaesse/Präs.%2036%20-%20Datensicherheitsvorschriften%20für%20das%20ZMR.pdf
- LINK: Präsidialerlass 22/2012 Registerabfragen gem. E-GovG
  https://mitarbeiter.graz.at/amt/Praesidialerlaesse/Präs.22%20-%20Registerabfragen%20gem.%20%20E-GovG.pdf
- LINK: Präsidialerlass 20990/2003-1 Ablage- und Skartierungsordnung (ASO)
  https://mitarbeiter.graz.at/amt/Interne Vorschriften/Ablage- und Skartierungsordnung.pdf

GRAZ DIGITALE SIGNATUR	**Signiert von**	Zeiler Josef
	Zertifikat	CN=Zeiler Josef,O=Magistrat Graz,L=Graz,ST=Styria,C=AT
	Datum/Zeit	2014-05-05T17:11:43+02:00
	Hinweis	Dieses Dokument wurde digital signiert und kann unter: http://egov2.graz.gv.at/pdf-as verifiziert werden.

GRAZ DIGITALE SIGNATUR	**Signiert von**	Haidvogl Martin
	Zertifikat	CN=Haidvogl Martin,O=Magistrat Graz,L=Graz,ST=Styria,C=AT
	Datum/Zeit	2014-05-07T10:44:04+02:00
	Hinweis	Dieses Dokument wurde digital signiert und kann unter: http://egov2.graz.gv.at/pdf-as verifiziert werden.