Informationssicherheits-Leitlinie

Stadt Ettlingen

Version:	1.0-01
Bearbeitungsstatus:	In Bearbeitung
Letztes Bearbeitungsdatum:	14.04.2014 08:43
Verantwortlicher Autor:	O. Hermann

Änderungsnachweis

Versions-nummer	Bearbeitungs-status	Datum	Bearbeiter	Änderung / Bemerkung
1.0		14.04.2014	ISMT	

Ergänzende Dokumente / Mitgeltende Unterlagen *

Dokument-nummer	Dokumentenklasse und Titel des Dokuments	Version	Datum letzte Bearbeitung	Verantwortlicher Autor

** In der Tabelle sind alle Dokumente einzutragen, die für dieses Dokument Gültigkeit besitzen, die aber im Dokument nicht explizit genannt werden (beispielsweise Namenskonventionen). Einzutragen sind auch alle Dokumente, auf die im nachfolgenden Dokument explizit verwiesen wird.*

Inhalt

1 Vorwort

Die Informationssicherheitspolitik ist ein elementarer Bestandteil der Politik der Stadt Ettlingen. Sie ist ein unentbehrlicher Baustein im Informationsmanagementsystem der Stadt und ist als solche eine wesentliche Leitlinie für die Realisierung und kontinuierliche Verbesserung der Geschäftsprozesse der Dienststellen in der täglichen Abwicklung der Anforderungen der Bürger.

Diese Geschäftsprozesse hängen zunehmend von Informationen und Informationssystemen ab. Die Sicherheit der Informationen und der Informationssysteme ist mehr als nur eine Absicherung der technischen Infrastruktur, sondern bedeutet Kontrolle und Steuerung des Informationsflusses. Dies erfordert ein angemessenes Bewusstsein bzgl. der Informationssicherheit bei allen Mitarbeiterinnen und Mitarbeitern (nachfolgend zusammengefasst „Mitarbeiter“ genannt) sowie eine Einbettung der Informationssicherheit in die Geschäftsprozesse, den Aufbau von Infrastruktur und die Entwicklung und Implementierung von Informationssystemen.

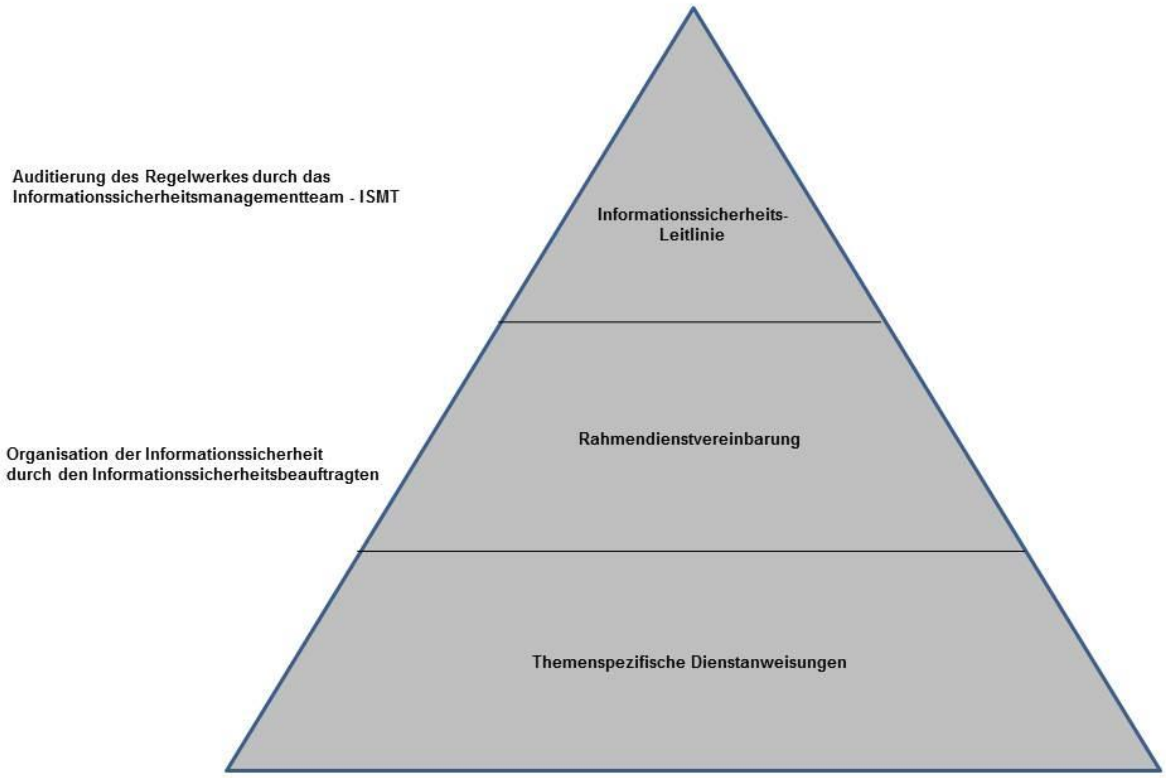
Die Informationssicherheitspolitik dient als Basis für die Erstellung weiterführender Regelungen für die Informationssicherheit. Sie stellt damit eine Regelung dar, die allen Mitarbeitern zu einem eindeutigen und klaren Verständnis der Verantwortlichkeiten innerhalb der Informationssicherheit verhelfen und sie zu einem sicheren Umgang mit Informationen der Behörden anleiten soll.
Mit dieser Informationssicherheitspolitik verpflichtet sich der Oberbürgermeister, die Führungskräfte, sowie die Mitarbeiter, die durch das Managementsystem getroffenen Festlegungen entsprechend auszuführen und tatkräftig an der kontinuierlichen Weiterentwicklung des Managementsystems für Informationssicherheit mitzuwirken.
Der Oberbürgermeister genehmigt das auf der Basis der Informationssicherheitspolitik erstellte Regelwerk. Damit sind alle im Zusammenhang mit dem Managementsystem getroffenen Festlegungen für alle Funktionsbereiche und Mitarbeiter verbindlich.

2 Zweck

Die in diesem Dokument beschriebene Informationssicherheitspolitik definiert die grundlegenden Ziele, Strategien und Verantwortlichkeiten zur Gewährleistung der Informationssicherheit bei der Stadt Ettlingen.
Die Informationssicherheitspolitik basiert auf der Einhaltung von internationalen Regularien und Standards (ISO 27001:2013) und zielt darauf ab, diese innerhalb der Stadt Ettlingen zu verankern.

3 Kontext

Folgende Übersicht zeigt den Aufbau der Informationssicherheitspolitik bei der Stadtverwaltung Ettlingen:



4 Geltungsbereich

Die Informationssicherheitspolitik und alle damit verbundenen Regelungen gelten für die gesamte Stadtverwaltung Ettlingen mit allen Außenstellen und sind durch konkrete IT-Regelungen im Einzelfall auszugestalten.

5 Kernaussage

Der Erfolg der Geschäftsprozesse der Stadtverwaltung Ettlingen wird entscheidend durch die Erfahrung und das Wissen der Mitarbeiter bestimmt. Unkontrollierter Abfluss und Manipulation von Daten, Kenntnissen und Informationen (nachfolgend zusammengefasst „Informationen“ genannt) können die Durchführung und damit den Erfolg nachhaltig gefährden.
Informationen und die für die Informationsverarbeitung und Kommunikation zur Verfügung gestellten Einrichtungen sind wertvolles und schützenswertes Gut. Alle Mitarbeiter sind

daher persönlich verpflichtet, Informationen und die zur Verfügung gestellten Kommunikationsmittel gegen Verlust, Verfälschung bzw. Beschädigung und Missbrauch jeglicher Art zu schützen und die eingesetzten Arbeitsmittel mit der gebotenen Sorgfalt zu behandeln.
Die Beachtung der Informationssicherheitspolitik ist ein wesentliches Mittel zur Einhaltung von Gesetzen. Die kontinuierliche Umsetzung der Informationssicherheitspolitik in die Geschäftsprozesse fördert ein positives Image bei den Bürgern und sichert Vertrauen in die Dienstleistungen der Stadtverwaltung.

6 Vision

Informationssicherheit bedeutet Vertrauen haben - Vertrauen in die Sicherheit unserer Informationen und Vertrauen in die Sicherheit unserer Prozesse. Die Schaffung und der Erhalt von Vertrauen in unsere Informationswerte bedingt die Erstellung und Umsetzung von Regelungen zum Schutz der Informationen auf der Basis einer „Kultur von Sicherheit“ bei der Stadtverwaltung Ettlingen.

Dazu sind Maßnahmen notwendig, die

- das Bewusstsein für die Chancen und Risiken der Informationstechnologie erhöhen;
- das Verständnis für den Schutz von Informationswerten fördern;
- die Informationssicherheit in den Geschäftsprozessen verankern.

Um die obige Kernaussage nachhaltig bei den verschiedenen Dienststellen der Stadtverwaltung Ettlingen zu verankern und um die Informationssicherheitspolitik langfristig auszurichten, haben sich alle Mitarbeiter der Stadtverwaltung Ettlingen an folgenden Leitbildern zu orientieren:

- Jeder, der Informationen nutzt, ist im Rahmen von Vorgaben für deren Sicherheit verantwortlich.
- Jede Information wird bei der Verarbeitung grundsätzlich als vertraulich klassifiziert.
- Jede schützenswerte elektronische Information muss gesichert werden.
- Nur eindeutig ausgewiesene Personen mit entsprechender Befugnis erhalten Zugang zu schützenswerten Informationen.
- Jeder Zugriff auf Informationen muss eindeutig erkennbar und nachvollziehbar sein.

7 Grundsatzaussagen

Die Nutzung des Potenzials moderner Informationstechnologie ist eine wichtige Aufgabe zur Erfüllung der anfallenden Aufgaben. Daraus ergibt sich die Notwendigkeit, dass bei Planung, Entwicklung und Beschaffung von IT-Infrastruktur und IT-Systemen, ebenso wie im laufenden Betrieb, Maßnahmen für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen durchzuführen sind. Darüber hinaus müssen Handlungen innerhalb der IT nachvollziehbar sein. Sämtliche Maßnahmen sind nach wirtschaftlichen Gesichtspunkten auszurichten.

Es ist nach folgenden Grundsätzen zu verfahren:

Vertraulichkeit - Informationen, die nicht zur allgemeinen Veröffentlichung bestimmt sind, sind nur den dafür Berechtigten zugänglich zu machen.

Integrität - Eine fehlerfreie Verarbeitung der Informationen sowie der Schutz vor unberechtigter Veränderung ist zu gewährleisten.

Verfügbarkeit - Informationen sind innerhalb eines vereinbarten Zeitraums zur Verfügung zu stellen.

Nachvollziehbarkeit/Nachweisbarkeit - Der Zugriff auf schützenswerte Informationen und die Durchführung von Transaktionen muss unbestreitbar sein.

Zur Sicherstellung dieser Grundsätze sind unter anderem folgenden Sicherheitsverfahren anzuwenden:
Authentisierung - Die eindeutige Identifikation beim Zugriff auf Informationen ist sicherzustellen.

Autorisierung - Der Zugriff auf Informationen ist nur Befugten zu gewähren und auf den für die Tätigkeit notwendigen Umfang zu beschränken.

Auditierung – Die Zugriffsberechtigung wird protokolliert und überprüft.

Das entsprechende Bewusstsein für Informationssicherheit bei allen internen und externen Mitarbeitern stellt das Fundament für die Anwendung der Informationssicherheitsverfahren und die Einhaltung der Informationssicherheitsgrundsätze dar. Somit sind entsprechende Informations- und Ausbildungsmaßnahmen für Mitarbeiter durchzuführen, um Informationssicherheitsrisiken durch Unwissenheit oder Fehlbedienung zu vermindern.
Eine regelmäßige Anpassung der Informationssicherheitsanforderungen an sich ändernde Anforderungen ist erforderlich. Zum Erkennen neuer Risiken und Sicherheitsanforderungen sind Methoden und Arbeitsmittel zur regelmäßigen Analyse und Audits einzusetzen.

8 Verantwortlichkeiten

Die Informationssicherheit wird wesentlich beeinflusst durch das verantwortungsbewusste Verhalten von Führungskräften, Mitarbeitern sowie Betreibern von Informationssystemen.

Die **Führungskräfte** tragen in Ihrem Zuständigkeitsbereich die Verantwortung dafür, dass beim Umgang mit Informationen und Informationssystemen jederzeit eine angemessene Informationssicherheit gewährleistet ist. Daraus ergibt sich für alle Führungskräfte die Aufgabe, in ihrem Verantwortungsbereich für die Durchsetzung von Informationssicherheitsmaßnahmen, deren Abstimmung mit anderen tangierenden Bereichen zu sorgen und die Einhaltung der Regelungen zu kontrollieren.

Die **Informationssicherheitsorganisation** unterstützt dabei die Führungskräfte und sorgt für eine effiziente Verwirklichung von Informationssicherheitsmaßnahmen sowie für einen einheitlichen Wissensstand in Informationssicherheitsfragen bei der Stadtverwaltung Ettlingen und fördert das sicherheitsbewusste Denken in den Dienststellen.

Jeder, der Informationen nutzt, ist verpflichtet mit Informationen und Informationssystemen sorgfältig umzugehen sowie diese ausschließlich im Sinne der zugewiesenen Aufgaben und im Rahmen der gültigen Regelungen zu nutzen. Das gilt auch für externe Mitarbeiter.

9 Verstöße

Als Verstöße gelten vorsätzliche oder grob fahrlässige Handlungen, die insbesondere

- den Ruf der Stadtverwaltung Ettlingen schädigen;
- die Sicherheit der Mitarbeiter, Vertragspartner oder der Bürger gefährden;
- der Behörde tatsächlichen oder potentiellen finanziellen Verlust einbringen;
- den unberechtigten Zugriff auf Informationen, deren unberechtigte Weitergabe und/oder unberechtigte Änderung beinhalten oder ermöglichen;
- die Nutzung von Bürgerinformationen für illegale Zwecke beinhalten.

Verstöße gegen das Informationssicherheitsregelwerk werden individuell nach den einschlägigen gesetzlichen, vertraglichen und dienstlichen Bestimmungen in ihrer jeweils gültigen Fassung geprüft und entsprechend geahndet.

10 Informationssicherheitsorganisation der Stadt Ettlingen

Die Stadt Ettlingen hat eine Informationssicherheitsorganisation etabliert, mit der die technisch-operative Umsetzung der Maßnahmen, aber auch die Durchsetzung der Regelungen bis hin zum einzelnen IT- Anwender sichergestellt wird.

Diese Informationssicherheitsorganisation (Information Security Management Team - ISMT) stellt die Entwicklung, Fortschreibung und Veröffentlichung der Informationssicherheitspolitik, der damit verbundenen Informationssicherheitshandlungsleitlinien, Informationssicherheitsstandards, Informationssicherheitsumsetzungsvorgaben und der technischen Anweisungen und Verfahrensanweisungen sicher. Sie ist für die Einführung von Sicherheitsprogrammen entsprechend den geschäftlichen Bedürfnissen verantwortlich.
Dazu zählen auch das Informationssicherheitsbewusstsein der Mitarbeiter, IT-Sicherheitsanalysen und – falls erforderlich – die technische Überwachung.

Die Informationssicherheitsorganisation (Informationssicherheitsmanagement-Team - ISMT) setzt sich aus Mitarbeitern aus verschiedenen Bereichen der Verwaltung zusammen.

Es legt geeignete Maßnahmen und Informationssicherheitsstandards bezüglich Informationssicherheit fest, passt sie laufend an neue Anforderungen an und achtet auf ihre Einhaltung. Dies gliedert sich wie folgt:

- Definition von strategischen Zielen der Informationssicherheit.
- Festlegung und Weiterentwicklung der Informationssicherheitsstandards auf Behördenebene.
- Einrichtung von Mechanismen, um für die Einhaltung der Informationssicherheitsstandards zu sorgen.

- Initiierung und Überwachung von Maßnahmen und Projekten zur Informationssicherheit.
- Erhöhung des Informationssicherheitsbewusstseins bei den Mitarbeitern durch Erarbeitung und Pflege entsprechender Maßnahmen.
- Vorbereitung von Berichten zur Informationssicherheit an den Oberbürgermeister der Stadt Ettlingen
- Analyse der Anforderungen und Probleme aus den Fachbereichen
- Unterstützung der Fachbereichsleiter bei der Planung und Realisierung der ausgewählten Informationssicherheitsmaßnahmen und Unterstützung bei der Einhaltung von Beschlüssen und Anweisungen.

Die Zusammensetzung und der Berichtsweg des Informationssicherheitsteams sind in der Geschäftsordnung des Informationssicherheitsteams geregelt.

Das Information Security Management Team (ISMT) können Sie per Mail an ISMT@ettlingen.de erreichen.

11 Inkrafttreten

Diese Leitlinie tritt am Tag nach Ihrer Veröffentlichung in Kraft.

Ettlingen, den 17.04.2014

gez. Johannes Arnold
Oberbürgermeister