

83 Geschäftsanweisung zur Organisation der IT-Sicherheit bei der Landeshauptstadt Düsseldorf

01
10/2

01.09.2011

Inhalt

1 Allgemeines

- 1.1 Zweck
- 1.2 Regelungsbereich
- 1.3 Geltungsbereich
- 1.4 Begriffsbestimmungen/Ziele

2 Regelungen

- 2.1 Dezentrale Gewährleistung der IT-Sicherheit
- 2.2 Zentrale Gewährleistung der IT-Sicherheit
 - 2.2.1 Funktion der/des IT-Sicherheitsbeauftragten
 - 2.2.2 Besondere Befugnisse
 - 2.2.3 Pflicht zur Beteiligung der/des IT-Sicherheitsbeauftragten
 - 2.2.4 Organisatorische und fachliche Anbindung
- 2.3 Zusammenarbeit mit der/dem Datenschutzbeauftragten

3 Inkrafttreten

1 Allgemeines

1.1 Zweck

Zweck dieser Geschäftsanweisung ist es, die sichere Verarbeitung von Daten durch IT-Systeme und Anwendungen zu gewährleisten. Hierzu sind im Rahmen von IT-Sicherheitskonzepten Maßnahmen aufzuzeigen, durch die ein angemessener Schutz der IT-Systeme und Anwendungen erreicht werden kann. Die Maßnahmen sind unter Berücksichtigung des Schutzbedarfs der Daten, des verbleibenden Restrisikos und des Grundsatzes der Verhältnismäßigkeit festzulegen und umzusetzen.

1.2 Regelungsbereich

Diese Geschäftsanweisung regelt die Zuständigkeiten und Aufgaben im Bereich der IT-Sicherheit.

1.3 Geltungsbereich

Diese Geschäftsanweisung gilt für alle städtischen Organisationseinheiten (Büros, Ämter und Institute) sowie für die städtischen Eigenbetriebe und die wie ein Eigenbetrieb geführten Einrichtungen. Sie gilt auch für städtische IT-Systeme, die außerhalb der Dienstgebäude betrieben werden.

1.4 Begriffsbestimmungen/Ziele

IT-Sicherheit umfasst die Summe aller organisatorischen, personellen und technischen Maßnahmen, die geeignet sind, die nachfolgend genannten Ziele zu erreichen:

Vertraulichkeit

Es ist sicherzustellen, dass nur Befugte Daten zur Kenntnis nehmen können.

Integrität

Es ist sicherzustellen, dass Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben.

Verfügbarkeit

Es ist sicherzustellen, dass Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.

Als IT-System wird die Hard- und Systemsoftware bezeichnet, die dazu geeignet ist, Daten durch Anwendungen zu verarbeiten, zu speichern oder zu übermitteln. Zu den IT-Systemen zählen auch die Komponenten der Kommunikationsinfrastruktur.

2 Regelungen

2.1 Dezentrale Gewährleistung der IT-Sicherheit

Jede Mitarbeiterin, jeder Mitarbeiter und jede Führungskraft ist dafür verantwortlich, dass mit den IT-Systemen, Anwendungen und Daten verantwortungsvoll umgegangen wird. Die in diesem Zusammenhang aufgezeigten Maßnahmen sind an jedem Arbeitsplatz zu beachten. Hierbei werden die Mitarbeiterinnen und Mitarbeiter durch die IT-Koordinatoren unterstützt.

2.2 Zentrale Gewährleistung der IT-Sicherheit

2.2.1 Funktion der/des IT-Sicherheitsbeauftragten

Der Oberbürgermeister überträgt einer Mitarbeiterin oder einem Mitarbeiter die Funktion der/des IT-Sicherheitsbeauftragten für den Geltungsbereich dieser Geschäftsanweisung (Ziffer 1.3). Die Funktion ist mit der Aufgabe verbunden, im Rahmen einer ganzheitlichen Konzeption für einen angemessenen Schutz der IT-Systeme, Anwendungen und Daten zu sorgen. Zu ihren/seinen Aufgaben zählt insbesondere:

- die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit zu unterstützen, deren Umsetzung zu steuern und zu koordinieren,
- die Erstellung des IT-Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte,

- die System-Sicherheitsrichtlinien zu koordinieren sowie weitere Richtlinien und Regelungen zur Informationssicherheit zu erlassen,
- den Realisierungsplan für Sicherheitsmaßnahmen zu erstellen und ihre Umsetzung zu initiieren und zu überprüfen,
- sicherheitsrelevante Projekte zu koordinieren,
- sicherheitsrelevante Zwischenfälle zu untersuchen,
- der Leitungsebene über den Status der Informationssicherheit zu berichten,
- Kontrollen der Effektivität von Sicherheitsmaßnahmen zu initiieren,
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren,
- die Personalvertretung in Fragen der IT-Sicherheit zu beraten.

Für die Erstellung und Umsetzung von IT-Sicherheitskonzepten im Bereich des Anwendungs- und Systemmanagements ist die ITK Rheinland zuständig und verantwortlich. Die/der IT-Sicherheitsbeauftragte ist hierbei zu beteiligen.

2.2.2 Besondere Befugnisse

Die/Der IT-Sicherheitsbeauftragte ist befugt, IT-Systeme ganz oder teilweise außer Betrieb nehmen zu lassen, wenn die unter Ziffer 1.4 genannten Ziele gefährdet sind. Hierüber informiert sie/er unverzüglich die Leiterin bzw. den Leiter seiner Organisationseinheit sowie die durch den Systemausfall betroffenen Organisationseinheiten der Verwaltung.

2.2.3 Pflicht zur Beteiligung der/des IT-Sicherheitsbeauftragten

Die/Der IT-Sicherheitsbeauftragte ist zu beteiligen, sofern die unter Ziffer 1.4 genannten Ziele betroffen sind. Dies ist insbesondere der Fall, wenn IT-Systeme bzw. Anwendungen geplant, ausgewählt, entwickelt oder wesentlich geändert werden.

Die/Der IT-Sicherheitsbeauftragte ist von der zuständigen Organisationseinheit (Ziffer 1.3) unaufgefordert und umfassend zu informieren.

Die/Der IT-Sicherheitsbeauftragte ist unverzüglich zu unterrichten, wenn ein IT-System oder eine Anwendung in einer Weise benutzt wurde, die den unter Ziffer 1.4 genannten Zielen der IT-Sicherheit nicht entspricht. Für die Benachrichtigung ist die Stelle verantwortlich, die das IT-System oder die Anwendung betreut.

2.2.4 Organisatorische und fachliche Anbindung

Die/Der IT-Sicherheitsbeauftragte ist organisatorisch dem Hauptamt zugeordnet.

2.3 Zusammenarbeit mit der/dem Datenschutzbeauftragten

Die bzw. der Datenschutzbeauftragte und die bzw. der IT-Sicherheitsbeauftragte arbeiten vertrauensvoll zusammen.

3 Inkrafttreten

Diese Geschäftsanweisung tritt am 01. 09. 2011 in Kraft. Sie gilt längstens für die Dauer von fünf Jahren und ist bei Bedarf zu verlängern.

Sie ersetzt die Geschäftsordnung über die Organisation der IT-Sicherheit bei der Landeshauptstadt Düsseldorf vom 01.09.2006.

Dirk Elbers
Oberbürgermeister