

	Informationssicherheitsleitlinie für die Freie und Hansestadt Hamburg	IS-LL Version 1.0
---	--	--

1 Zielsetzung

Mit dieser Informationssicherheitsleitlinie (IS-LL) legt der Senat allgemeinverbindliche Grundsätze für die Informationssicherheit in der Hamburgischen Verwaltung fest. Die IS-LL ist übergeordnete Leitlinie für die Richtlinien des IT-Handbuches und dient dem Ziel, alle Informationen in der Hamburgischen Verwaltung vollständig, korrekt und verfügbar zu machen, aber sie vor unbefugtem Zugriff zu schützen. Zu diesem Zweck beschreibt die Leitlinie organisatorische und personelle Maßnahmen für ein Sicherheitsniveau, das sich an die Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnologie anlehnt.

2 Geltungsbereich

Die IS-LL gilt für alle Dienststellen der Freien und Hansestadt Hamburg (FHH), Organe der Rechtspflege sowie die sonstigen öffentlichen Stellen der FHH, soweit diese im staatlichen Auftrag tätig werden. Für andere Stellen und Einrichtungen der FHH (z. B. Bürgerschaftskanzlei, Rechnungshof) gilt diese Leitlinie und die daraus folgenden Vorgaben nach Maßgabe gesondert abzuschließender Vereinbarungen für die gemeinsame Nutzung der IT-Infrastruktur. Soweit andere Regelwerke strengere Vorschriften zur Informationssicherheit beinhalten (z. B. bei der Polizei oder dem Landesamt für Verfassungsschutz), so gelten diese zusätzlich.

3 Sicherheitskonzept

Das zentrale Informationssicherheitsmanagement in der für die Informationstechnik zuständigen Behörde erstellt in Abstimmung mit den anderen Behörden ein zentrales Sicherheitskonzept, das behördenübergreifende Maßnahmen, Rahmenvorgaben für die Behörden und Vorgaben für den zentralen IT-Dienstleister umfasst. Dazu erfolgen eine Bestandsaufnahme der Informationsprozesse, die Feststellung des Schutzbedarfs, die daraus abzuleitenden grundsätzlichen Maßnahmen und die Konkretisierung der Ziele.

Behördenübergreifende Maßnahmen werden von der für die Informationstechnik zuständigen Behörde umgesetzt. Die Behörden setzen die Rahmenvorgaben für ihre jeweiligen Informationsprozesse um. Sofern einzelne Informationsprozesse von den Rahmenvorgaben und dem zentralen Sicherheitskonzept nicht erfasst werden, legen die jeweils zuständigen Behörden hierfür entsprechende Vorgaben und Sicherheitsmaßnahmen fest und setzen diese um. Unter Mitwirkung der für die Informationstechnik zuständigen Behörde wird ein zentrales IT-Sicherheitsvorfallteam (CERT Computer Emer-

gency Response Team) beim IT-Dienstleister eingerichtet sowie ein Notfall- und Krisenmanagement geplant.

Alle Maßnahmen der Informationssicherheit müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen stehen.

4 Zuständigkeiten

Alle Beschäftigten haben die Informationssicherheit durch ihr verantwortliches Handeln zu gewährleisten und die für die Informationssicherheit relevanten Regelwerke (Gesetze, Verordnungen, Richtlinien, personalvertretungsrechtliche Vereinbarungen, organisatorische Regelungen, vertragliche Verpflichtungen u. ä.) einzuhalten.

Die für die Informationstechnik zuständige Behörde richtet ein zentrales Informationssicherheitsmanagement (InSiMa) ein. Die Behörden benennen für ihren Verantwortungsbereich Informationssicherheitsbeauftragte. Die Führungskräfte der Verwaltung ermöglichen den Beschäftigten ihrer Organisationseinheit Schulungsmaßnahmen auf dem Gebiet der Datensicherheit bzw. setzen sie in Abstimmung mit der/dem Informationssicherheitsbeauftragten in Dienstbesprechungen oder auf andere geeignete Weise über die Belange der Informationssicherheit in Kenntnis.

Die Verantwortung für die Informationssicherheit bei Datenverarbeitung im Auftrag trägt der Auftraggeber gemäß HmbDSG.

5 Zentrales Informationssicherheitsmanagement

Das zentrale Informationssicherheitsmanagement (InSiMa) besteht aus der Leitung (Verantwortliche oder Verantwortlicher für Informationssicherheit in der FHH) und dem Sicherheitsteam (Beschäftigte aus den Bereichen IT-Technik, Datenschutz und Datensicherheit). Es wird in technischen Fragen vom zentralen IT-Dienstleister beraten bzw. unterstützt. Zu den wesentlichen Aufgaben gehören:

- Bestimmung der Informationssicherheitsziele und Fortschreibung der IS-LL,
- Entwicklung und Fortschreibung eines zentralen Sicherheitskonzepts,
- Prüfung, ob die IS-LL bzw. das zentrale Sicherheitskonzept und die darin vorgegebenen Maßnahmen umgesetzt werden und wirksam sind,
- Auslegung der IS-LL in Zweifelsfällen,
- Umsetzung der behördenübergreifenden Maßnahmen des zentralen Sicherheitskonzepts,
- Organisation und Durchführung von Schulungen zur Informationssicherheit,
- Untersuchung von Vorfällen, die die Informationssicherheit beeinträchtigen, und Festlegung geeigneter Maßnahmen zur Vermeidung solcher Vorfälle,
- Beratung des IT-Architektur-Boards und anderer Stellen der FHH in Informationssicherheitsfragen,

- Dokumentation der durchgeführten Maßnahmen und Prozessveränderungen im Informationssicherheitsmanagement.

Das InSiMa legt alle Regelungen und Maßnahmen dem IT-Architektur-Board (ITAB) zur Beratung und Beschlussfassung vor. Bei Gefahr im Verzuge oder sehr dringlichen Themen kann das InSiMa entsprechende Maßnahmen direkt in Kraft setzen. Es beruft regelmäßig die behördlichen Informationssicherheitsbeauftragten zu einer Arbeitsgruppe ein, um Themen zur Informationssicherheit gemeinsam zu beraten und bei entsprechendem Handlungsbedarf dem ITAB geeignete Sicherheitsmaßnahmen zur Beschlussfassung vorzulegen.

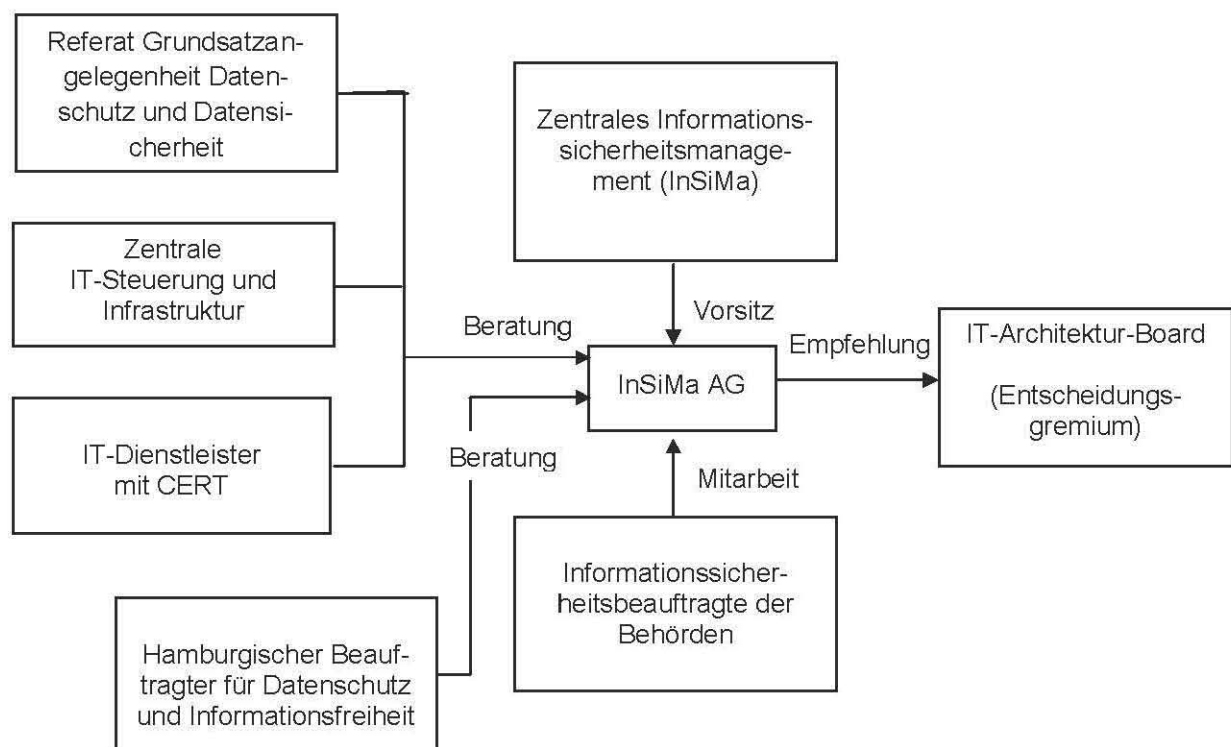
6 Behördliche Informationssicherheitsbeauftragte

Die Funktion der/des Informationssicherheitsbeauftragten kann zusätzlich zu anderen Aufgaben, sollte aber nicht von der IT-Leitung selbst wahrgenommen werden. Zu den wesentlichen Aufgaben der/des Informationssicherheitsbeauftragten gehören:

- Beratung der mit Informationsprozessen befassten Stellen der Behörde (z. B. Leitung Organisation, IT-Beauftragte oder IT-Beauftragter, IT-Leitungen) in Fragen der Informationssicherheit,
- Erstellung eines Sicherheitskonzepts, das die Rahmenvorgaben des zentralen Sicherheitskonzepts erfüllt und alle weiteren erforderlichen Maßnahmen zur Informationssicherheit in der jeweiligen Behörde beschreibt,
- Prüfung, ob in der Behörde alle vorgeschriebenen Maßnahmen zur Informationssicherheit umgesetzt werden und wirksam sind,
- Teilnahme am regelmäßigen Informationsaustausch bzw. an der Arbeitsgruppe des zentralen InSiMa,
- Unterrichtung der Beschäftigten in Fragen der Informationssicherheit.

Die Behördenleitungen, IT-Beauftragten, IT-Leitungen und fachlich zuständigen Stellen haben ihre jeweiligen Informationssicherheitsbeauftragten bei der Wahrnehmung ihrer Aufgaben zu unterstützen.

7 Organigramm zum Informationssicherheitsmanagement



8 Inkrafttreten

Diese Sicherheitsleitlinie tritt am 02.04.2013 in Kraft.