	Rahmen-Sicherheitskonzept der Freien und Hansestadt Hamburg	**RaSiKo Version 1.1 19.01.2016**

Inhaltsverzeichnis

1. Vorbemerkung

Der Senat hat mit Drucksache 2014/713 am 2. April 2013 die Informationssicherheitsleitlinie der FHH (IS-LL) beschlossen. In der IS-LL ist verankert, in Abstimmung mit den übrigen Behörden, ein behördenübergreifendes, zentrales Sicherheitskonzept (im Folgenden Rahmen-Sicherheitskonzept (RaSiKo) genannt), das die behördenübergreifenden Maßnahmen, die Rahmenvorgaben für die Behörden und die Vorgaben für den zentralen IT-Dienstleister umfasst, zu erstellen.

Dabei soll dieses Konzept allen Organisationseinheiten der FHH als Vorlage dienen (siehe Geltungsbereich IS-LL lfd. Nr. 2), um ggf. eigene Sicherheitskonzepte zu erarbeiten.

Die im Konzept genannten Begrifflichkeiten werden im Anhang 1 „Begriffsbestimmungen“ beschrieben.

2. Zielsetzung

Ziel dieses Konzeptes ist es, die

- **Verfügbarkeit**

  (Gewährleistung, dass Informationen, Anwendungen und IT-Systeme für Berechtigte im vorgesehenen Umfang und in angemessener Zeit nutzbar sind),
- **Vertraulichkeit**

  (Gewährleistung, dass Informationen ausschließlich Berechtigten zugänglich sind),
- **Integrität**

  (Gewährleistung, dass die Unverfälschtheit und Vollständigkeit von Informationen, Anwendungen und IT-Systemen überprüfbar sind),

aller Informationen (digitale sowie analoge Informationen, Anwendungen und IT-Systeme) in der Hamburgischen Verwaltung unter Berücksichtigung der Aspekte des Datenschutzes in angemessener Weise zu gewährleisten.

Dabei soll mit den Vorgaben aus dem IT-Handbuch der FHH und in Anlehnung an die Standards des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) ein normales Schutzniveau erreicht werden. Sofern ein höherer Schutzbedarf für fachliche Verfahren notwendig ist, müssen weitergehende Prüfungen durch die fachlich zuständigen Stellen erfolgen.

3. Informationssicherheitsmanagement

3.1. Die Organisation der Informationssicherheit in der FHH

Beteiligte des Informationssicherheitsprozesses in der FHH sind:

- Das Zentrale Informationssicherheitsmanagement (InSiMa) der FHH in der für die Informationstechnik zuständigen Behörde,

- die behördlichen Informationssicherheitsbeauftragten (beh. InSiBe) oder die mit deren Aufgaben befassten Stellen [1],
- die IT-Stellen der Behörden, Ämter und übrigen Organisationseinheiten (OE),
- der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit sowie die behördlichen Datenschutzbeauftragten (beh. DSB),
- der IT-Dienstleister Dataport.

Mit dieser Organisationsstruktur und dem IT-Regelwerk (IT-Handbuch und weitere IT-Konzepte in Verbindung mit den Standards des BSI) soll für die FHH eine an Standards ausgerichtete Informationssicherheitsmanagement-Struktur ermöglicht bzw. sichergestellt werden. Die organisatorischen Verantwortlichkeiten und Beziehungen werden im Anhang 2 dargestellt und beschrieben).

3.2. Aufgaben und Kompetenzen des Informationssicherheitsmanagement

Das Informationssicherheitsmanagement (InSiMa) besteht aus der Leitung (Informationssicherheitsbeauftragte/r der FHH) (siehe Anhang 1) und dem Sicherheitsteam. Es koordiniert für die FHH die Aufgabe Informationssicherheit, initiiert und steuert die erforderlichen behördenübergreifenden Maßnahmen und überprüft, ob die Sicherheitsziele erreicht worden sind.
Hinsichtlich der konkreten Aufgaben und Kompetenzen des InSiMa wird auf Anhang 2 verwiesen.

3.3. Aufgaben und Kompetenzen der/des behördlichen Informationssicherheitsbeauftragten

Die/der behördliche Informationssicherheitsbeauftragte (beh. InSiBe) koordiniert im Auftrag der Leitungsebene die Aufgabe Informationssicherheit für die OE und bringt diese voran. Dabei sind die Vorgaben des zentralen InSiMa als Grundlage einzuhalten; sie können durch eigene Sicherheitskonzepte entsprechend den jeweiligen behördlichen Anforderungen ergänzt und fortgeschrieben werden. Hinsichtlich der konkreten Aufgaben und Kompetenzen sowie der Zusammenarbeit mit weiteren Stellen der Behörde (z.B. IT-Leitungen, IT-Beauftragte) wird auf den Anhang 2 verwiesen.

3.4. IT-Stellen der Behörden, Ämter und übrigen Organisationseinheiten

Die IT-Stellen der Behörden, Ämter und übrigen OE treffen für die in ihrem Geschäftsbereich eigenständig betriebene IT-Infrastruktur (inkl. Technik- und Systemräume sowie IT-Verkabelung) die erforderlichen Maßnahmen zur Informationssicherheit. Sie stimmen sich in Bezug auf die für die übergreifend zur Verfügung gestellte Informationstechnik-Infrastruktur (Rechenzentrums- und Netzbetrieb, Endgerätesicherheit) mit der hierfür verantwortlichen Fachlichen Leitstelle der Finanzbehörde ab. Sie koordinieren auf Grundlage der Anforderungen der Fachlichen Leitstellen der Behörden ggf. gesonderte, über den BSI-Grundschutz hinausgehende, Maßnahmen zum Betrieb der Fachverfahren in der Rechenstelle (Datenverarbeitung im Auftrag).

[1] Im Dokument wird der Terminus „beh. InSiBe" verwendet, auch wenn dezentrale Strukturen innerhalb der Behörden Teile der Aufgaben der Informationssicherheit wahrnehmen

Die IT-Stellen unterstützen die beh. InSiBe bei der Durchführung von Sicherheitsprüfungen und der Dokumentation der IT-Verfahren/Anwendungen sowie der örtlichen Infrastruktur (z. B. Gebäude).

3.5. Aufgabenverteilung zwischen Datenschutz und Informationssicherheit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit wird nach den Vorgaben der „Richtlinie zur Beteiligung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit " unterrichtet und ist Ansprechstelle für das InSiMa und die beh. InSiBe in datenschutzrechtlichen Angelegenheiten.
Die/der beh.DSB hat die Aufgabe, die Daten verarbeitenden Stellen der jeweiligen OE in der Ausführung des HmbDSG sowie anderer Vorschriften über den Datenschutz zu unterstützen (siehe § 10a Abs. 5 HmbDSG). Eine konkrete Aufgabenbeschreibung findet sich im „Konzept behördliche Datenschutzbeauftragte".
Teile der Aufgaben des InSiMa bzw. des Datenschutzes sind bei personenbezogenen Prozessen deckungsgleich. Informationsverarbeitung ohne Personendatenbezug unterliegt nur den Vorgaben des InSiMa.

3.6. Aufgabe des IT-Dienstleisters Dataport

Dataport hat die Aufgabe, die öffentliche Verwaltung der FHH durch Informations- und Kommunikationstechniken zu unterstützen und nimmt damit die Rolle des zentralen IT-Dienstleisters wahr. Um einen sicheren Betrieb zu gewährleisten, hat Dataport in Zusammenarbeit mit der FHH Sicherheitskonzeptionen erarbeitet, die kontinuierlich dem jeweiligen Stand der Technik entsprechend fortzuentwickeln sind. Die daraus resultierenden Aufgaben werden im Anhang 2 beschrieben.
Im Rahmen der Datenverarbeitung im Auftrag gewährleistet Dataport einen sicheren IT-Betrieb in der FHH. Die Verantwortung verbleibt bei der Auftrag gebenden Stelle.

4. Betrieb und Verantwortungen im FHH-Netz

Die Verantwortung für das FHH-Netz (siehe Begriffsbestimmungen) trägt die für die Informationstechnik zuständige Behörde, die Dataport mit dessen Betrieb beauftragt hat. Das FHH-Netz dient als Grundlage für BASIS, Non-BASIS (siehe Begriffsbestimmungen) und weitere Dienste, z.B. Telefonie, Steuerung von Systemkomponenten, RZ-Infrastruktur (Beschreibung siehe Anhang 2).

Die behördenübergreifenden Infrastrukturen (siehe Begriffsbestimmungen) werden durch die für die Informationstechnik zuständige Behörde verantwortet.

Grundsätzlich ist im BASIS-Umfeld vereinbart, dass Dataport das LAN wie auch die Clients administriert. Sofern die Behörden vom Grundsatz im BASIS-Umfeld abweichen, trägt die betreibende Behörde/Organisationseinheit die Verantwortung für das LAN bzw. die Clients. Dies ist im jeweiligen Sicherheitskonzept der Behörde darzustellen. In diesem Fall endet die Zuständigkeit beim Übergabepunkt am jeweiligen Router, so dass die Behörde die LAN-Administration selbst verantwortet; dies gilt auch für Non-BASIS-Clients. Separate Netze der Behörden, etwa mit eigenem Internet-Zugang, liegen ganz in deren Verantwortung und dürfen nur aufgrund gesonderter Vereinbarungen mit der für die Informationstechnik zuständigen Behörde an das FHH-Netz angeschlossen werden.

Wie sich im Einzelnen die Verantwortlichkeiten und Beziehungen im Netzbereich darstellen, zeigt die Abbildung in Anhang 3.

5. Prozesse in der Informationssicherheit

Das InSiMa verantwortet im Rahmen seiner Aufgaben die Prozesse Sicherheitsvorfälle und Abwicklung im IT-Notfall.

Die Sicherheitsprozesse (Sicherheitsvorfälle und Abwicklung im IT-Notfall) und dazugehörigen Dokumente sind einer regelmäßigen Überprüfung zu unterziehen, die mindestens alle fünf Jahre stattfinden soll, wenn nichts anderes festgelegt worden ist. Dasselbe gilt auch für Dokumente oder Vorgaben der dezentralen Sicherheitsorganisation in den Behörden. Grundsätzlich sind kürzere Review-Zyklen anzustreben. Das Informationssicherheitsmanagement-System (siehe Begriffsbestimmung) unterliegt selbst einer regelmäßigen Überprüfung nach dem PDCA-Modell (Plan, Do, Check, Act) siehe (Begriffsbestimmungen).

5.1. Sicherheitsvorfälle

Werden Ereignisse, die unmittelbar auf die Sicherheit der IT-Systeme abzielen, oder Bedrohungen der Informationssicherheit von Beschäftigten erkannt, müssen sie unverzüglich die nach dem behördlichem Informationssicherheitskonzept zuständige Stelle (in der Regel die/der beh. InSiBe, IT-Leitung, UHD, siehe hierzu PC-RL, Ziffer 6.2) informieren, die das weitere Vorgehen, wenn nötig in Absprache mit dem IT-Dienstleister und/oder dem InSiMa, zu veranlassen hat. Sind personenbezogene Daten betroffen, sind auch die Leitungen der betroffenen Bereiche sowie die/der beh. DSB zu informieren.

Grundsätzlich werden Ereignisse beim UHD gemeldet. Die daran anschließende Bearbeitung durch den Second/Third Level Support bindet das IT-Sicherheitsmanagement von Dataport ein. Je nach Sachlage kann das Ereignis durch InSiMa, beh. InSiBe, oder Sicherheitsmanagement von Dataport zu einem Sicherheitsvorfall (SV) erklärt werden. Für den Fall, dass Dataport nicht involviert ist (Non-BASIS), kann die Behörde ggf. gemeinsam mit dem InSiMa das Ereignis zu einem SV erklären.

Die Klassifizierung von Sicherheitsvorfällen ist anhand eines Priorisierungsschemas vorzunehmen. Die Priorisierung eines Vorfalles leitet sich aus der Bewertung der zu erwartenden Auswirkungen (Schadenshöhe) und der Dringlichkeit der Beseitigung (Einsatzmöglichkeiten für Ersatzlösungen) des Vorfalles ab. Welche Priorität aus Auswirkung und Dringlichkeit resultiert, ist Anhang 4 zu entnehmen.

Eine auf den Einzelfall bezogene Einschätzung

- wie kritisch der Vorfall für die FHH (Dringlichkeit) ist,
- welche finanziellen Folgen sich ergeben können,
- welche Konsequenzen (z.B. Abschaltung Netz/Netzsegmente) sich ergeben können,
- welche Prüfung von schadensminimierenden Maßnahmen durchgeführt werden müssen,
- und mit einer Darstellung möglicher Lösungsansätze,

muss durch das InSiMa oder den beh. InSiBe ggf. in Zusammenarbeit mit dem IT-Sicherheitsmanagement von Dataport vorgenommen werden.

In der Folge eines Sicherheitsvorfalles kann es zur eingeschränkten Nutzung oder Abschaltung der vorhandenen Systeme kommen. Ziel ist es, die Verfügbarkeit der geschäftskritische Verfahren oder kritischen Geschäftsprozesse so lange wie möglich zu gewährleisten oder nach einem Ausfall der Systeme den Zugriff auf diese Verfahren schnellstmöglich wieder zu ermöglichen.

5.2. Abwicklung im IT-Notfall

IT-Notfälle (Begriffsbestimmungen) sind grundsätzlich in Zusammenarbeit mit Dataport abzuwickeln. Für diese Fälle steht bei Dataport ein IT-Notfallkonzept zur Verfügung. Sofern sich ein Notfall auf Prozesse oder Ressourcen bezieht, in denen Dataport nicht involviert ist, muss die entsprechende OE einen eigenen Notfallprozess festlegen.

6. IT-Grundschutz in der FHH

6.1. Grundsätzliches

„IT-Grundschutz“ ist die vom BSI entwickelte Vorgehensweise zum Identifizieren und Umsetzen von Informationssicherheitsmaßnahmen. Die FHH richtet ihre Informationssicherheit in Anlehnung an diese Vorgehensweise aus. Verbindlich dabei sind

- eine Risikoanalyse und die Bewertung dieser Risiken in Anlehnung an IT-Grundschutz, bzw.die FHH-Richtlinien,
- Umfang und Bewertung der erforderlichen Maßnahmen unter Kosten-Nutzen-Aspekten unter der Voraussetzung, dass Restrisiken bei Nichtumsetzung von Maßnahmen übernommen werden,
- Umsetzung und Prüfung auf Wirksamkeit der umzusetzenden Maßnahmen.

Das konkrete Vorgehen ist im „Konzept Einführung IT-Grundschutz in der FHH“ beschrieben. Eine grundsätzliche Vorgehensweise nach diesem Konzept wird empfohlen.

Hierbei ist das in Anlage 1 dargestellte Schichtenmodell der IT-Grundschutzkataloge des BSI als Basis der IS-LL anzuwenden.

6.2. Der Basis-Sicherheits-Check in der FHH

Das InSiMa und die beh. InSiBe haben die oben beschriebene IT-Grundschutz-Vorgehensweise auf den verantworteten Informationsverbund anzuwenden. Dabei ist durch einen Basis-Sicherheits-Check zu prüfen, welche Standard-Sicherheitsmaßnahmen, die in der Modellierung (Aufnahme des IT-Verbundes) als erforderlich identifiziert wurden, bereits umgesetzt worden sind und wo noch Defizite bestehen.

Sofern der Basis-Sicherheits-Check für die standardisierten Maßnahmen Lücken aufzeigt, ist die Umsetzung ergänzender Maßnahmen zu prüfen, um das angestrebte Schutzziel zu erreichen. Bei der Umsetzung muss darauf geachtet werden, dass diese unter wirtschaftlichen Gesichtspunkten zu realisieren ist. Sofern unter diesem As-

pekt eine Umsetzung unwirtschaftlich erscheint, sind die Risiken – nach deren Bewertung - durch die zuständige Behörde zu verantworten. Für die nicht standardisierten Maßnahmen wird die gleiche Vorgehensweise empfohlen.

6.3. Ergänzende Risikoanalyse

Die Standardmaßnahmen nach IT-Grundschutz bieten für den Schutzbedarf „normal" einen angemessenen und ausreichenden Schutz. Sofern ein höherer Schutzbedarf identifiziert wurde, ist eine ergänzende Sicherheits- bzw. Risikoanalyse zu erstellen. Die daraus resultierenden Sicherheitsmaßnahmen sind unter Abwägung von Kosten-Nutzen-Aspekten umzusetzen.

7. Berichtswesen

Zur Lage der Informationssicherheit sind Berichte regelmäßig vom InSiMa für die FHH insgesamt und von den beh. InSiBe für die jeweilige OE zu erstellen. Dabei ist eine Einheitlichkeit anzustreben. Eine Zusammenfassung über die Sicherheitslage in der FHH bzw. der jeweiligen OE sollte als Information für die entsprechende Leitungsebene und die mit den Prozessen befassten Beschäftigten aufbereitet werden. Darüber hinaus wird InSiMa eine Informationsplattform für Sicherheitshinweise und Warnmeldungen einrichten.

8. Restrisikodarstellung

Selbst wenn sämtliche sicherheitsrelevante Maßnahmen umgesetzt sind, verbleiben gegebenenfalls Restrisiken, die nicht mit vertretbarem Aufwand abgemildert werden können. Hierzu gehören unter anderem:

- Der zeitweise Totalausfall des Rechenzentrums bei gleichzeitigem Ausfall des Backup-Rechenzentrums.
- Der zeitweise Totalausfall des Verwaltungsnetzes (die Hauptknoten fallen komplett aus).
- Der zeitweise Totalausfall des Internets (z.B. Ausfall deutscher Internetknoten).

9. Salvatorische Klausel

Sollten in den Richtlinien der FHH oder aufgrund von später beschlossenen ITAB-Beschlüssen sich widersprechende Regelungen enthalten sein, so gilt die Regelung des jüngeren Datums. Im Zweifelsfall entscheidet die für die Informationstechnik zuständige Behörde.

10. Inkrafttreten

Dieses Sicherheitsrahmenkonzept tritt am 01.07.2015 in Kraft.

11. Änderungshistorie

Version	Änd.-Datum	Geänderte Stellen / Grund / Bemerkung	Autor

Version	Änd.-Datum	Geänderte Stellen / Grund / Bemerkung	Autor
0.40	17.09.2013	RaSiKo Entwurf	M. Taruttis
0.41	15.10.2013	RaSiKo-Fortschreibung innerhalb der AG InSiMa	AG InSiMa
0.95	30.06.2014	Redaktionelle und inhaltliche Überarbeitung	InSiBe in Zusammenarbeit mit der FB
0.96	01.08.2014	Kürzung Hauptteil und Verlagerung in Anhang	Jesch, Taruttis
0.97	22.08.2014	Überarbeitung	Schulz, Jesch, Taruttis
0.98	11.09.2014	Überarbeitung	Randl, Jesch, Taruttis
0.98	06.10.2014-17.03.2015	Überarbeitung der Rückmeldungen aus den Behörden	Jesch, Taruttis
0.98	17.03.2015	Änderungen angenommen zwecks 2. Abtimmung IT-Leitungen	Jesch, Taruttis
0.98a	23.04.2015	Weitere Ergänzungen durch die 2. Abstimmung erfasst	Jesch, Taruttis
1.00E	29.04.2015	Ändernugen angenommen, Kommentare entfernt	Jesch, Taruttis
1.00E	04.06.2015	Änderungen 113 und 173 erfasst	Jesch, Taruttis
1.00	23.06.2015	Änderungen 17 und 11 erfasst und redaktionelle Änderungen aus der 3. Abstimmung IT-Leitungen	Jesch, Taruttis
1.10	19.01.2016	Externe Links auf FHHPortal korrigiert.	Jesch, Taruttis

Anhang 1 Begriffsbestimmungen

Anwendungen und Fachverfahren

Gemäß Nr. 2 der Freigaberichtlinie der FHH (Freigabe-RL) umfasst eine Allgemeine Software (im folgenden „Anwendung“ genannt) Betriebssysteme, Systemprogramme, Dienstprogramme, Standardsoftware (z.B. Bürokommunikationssoftware), Herstellertools, Virenschutzprogramme und ähnliches und schafft die Grundlage für den Betrieb von Rechnern sowie für den Einsatz von Software zur Lösung einer konkreten Fachaufgabe. Sie ist nicht auf die Lösung einer speziellen Fachaufgabe zugeschnitten. Unter allgemeiner Software wird nicht die fachspezifische Nutzung von Bürokommunikationssoftware verstanden.
Demgegenüber sind Datenverarbeitungsverfahren (im folgenden „Fachverfahren“ genannt) automatisierte Arbeits- oder technische Prozesse zur Lösung einer fachlichen Aufgabe. Sie können aus einer Verknüpfung von verschiedener Software bestehen und organisatorische Zuständigkeiten sowie Abläufe festlegen. DV-Verfahren können sich auch der allgemeinen Software bedienen. Der Begriff DV-Verfahren wird synonym mit dem Begriff IT-Verfahren verwendet.

BASIS und Non-BASIS

BASIS (Büro Arbeitsplatz Standard Infrastruktur Services) bezeichnet den Standardarbeitsplatz und die dazugehörenden Services (ohne Fachverfahren) der FHH, die von Dataport zur Verfügung gestellt und betrieben werden. Arbeitsplätze und Services, die durch die Behörden selbst betrieben werden, werden als Non-BASIS bezeichnet.

Basis Sicherheitscheck (BSC)

Der Basis-Sicherheitscheck ist ein Organisationsinstrument nach BSI-Grundschutz, welches einen schnellen Überblick über das vorhandene IT-Sicherheitsniveau bietet. Er gibt Auskunft über die noch fehlenden Maßnahmen (Soll/Ist-Abgleich).

Basispolicy

Die Basispolicy konkretisiert die übergreifenden Aspekte der Netzöffnungspolicy des FHH-Netzes. Sie ist die grundsätzliche Netzöffnungspolicy des FHH-Netzes gemäß § 9 der Grundsatzvereinbarung über Kooperation, Auftragsdatenverarbeitung und Betrieb des Hamburgischen Telekommunikationsnetzes.

Behördenübergreifende Infrastrukturen

Behördenübergreifende Infrastrukturen im Sinne des RaSiKo sind alle zentralen Systeme, die zum IT-Betrieb für Arbeitsplätze zur Verfügung gestellt werden. Diese werden durch die für die Informationstechnik zuständige Behörde verantwortet und durch Dataport bereitgestellt.

Behördliche Informationssicherheitsbeauftragte (beh. InSiBe)

Offiziell bestellte Person, die die Aufgabe der Koordinierung der Informationssicherheit für die jeweilige OE wahrnimmt. In diesem Dokument wird der Terminus beh. InSiBe verwendet, auch wenn dezentrale Strukturen innerhalb der Behörden Teile der Aufgaben Informationssicherheit wahrnehmen.

Cyber-Angriff

Gezieltes Hacking von Webservern und anderen IT-Systemen mit dem Ziel der Platzierung von Schadsoftware oder zur Vorbereitung der Spionage in angeschlossenen

Netzen oder Datenbanken (Definition in Anlehnung an BSI). Das gezielte Hacking kann auch zum Ausfall von IT-Systemen führen.
Demgegenüber kann auch ein Softwarefehler zum Ausfall von Systemen führen. Ein solcher Ausfall wird aber nicht als Sicherheitsvorfall klassifiziert.

FHH-Netz / FHHNET

Das Netz der FHH besteht aus zwei Ebenen. Grundlage sind die physikalischen Netze der Behörden, das Backbone der FHH einschließlich Übergaberouter (FHH-Backbone) sowie die Netze von Dataport und Dritten. Diese sind auf einer höheren Ebene zum FHHNET oder anderen Netzen (z.B. Polizei) zusammengeschaltet, die dem Nutzer die unterschiedlichen physikalischen Netze jeweils als ein logisches Netzwerk präsentiert.

Geschäftskritische Verfahren

Geschäftskritische Verfahren sind Verfahren, die von zentraler Bedeutung für die Verwaltung und deren Kundensind. Diese Verfahren haben meist hohe Anforderung an die Performance und die Verfügbarkeit oder beinhalten sehr vertrauliche Informationen.

Informationssicherheitsbeauftragter der FHH

Offiziell bestellte Person, die die Aufgabe der Koordinierung der Informationssicherheit für die FHH wahrnimmt.

Informationssicherheitsmanagement-System

Das Informationssicherheitsmanagement-System (ISMS) ist eine Aufstellung von Organisation, Verfahren und Regeln innerhalb eines Unternehmens oder einer öffentlichen Einrichtung, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Informationssicherheitsmanagement der FHH

Das 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) und ist in der für die Informationstechnik zuständigen Behörde eingerichtet.

IT-Notfall

Ein IT-Notfall ist ein Schadensereignis, bei dem wesentliche Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. IT-Notfälle zeichnen sich dadurch aus, dass die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen innerhalb einer geforderten Zeit nicht wieder hergestellt werden kann und der Geschäftsbetrieb stark beeinträchtigt ist.

Organisationseinheiten

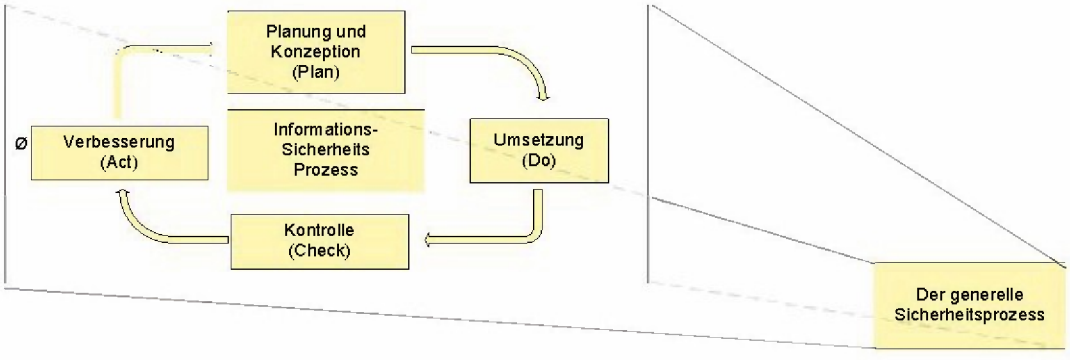
Organisationseinheiten (OE) sind alle Dienststellen der Freien und Hansestadt Hamburg (FHH), Organe der Rechtspflege sowie die sonstigen öffentlichen Stellen der FHH einschließlich der Landesbetriebe nach § 15 und § 26 LHO, soweit diese im staatlichen Auftrag tätig werden. Diese Stellen müssen zu diesem RaSiKo ergänzende Aussagen treffen, wie die Informationssicherheit in deren Verantwortungsbereichen für Fachverfahren oder behördeneigene Netze geregelt wird.

PDCA-Modell

PDCA-Modell umfasst die Schritte Planung (Plan), Durchführung (Do), Kontrolle (Check), Verbesserung (Act) des Sicherheitsprozesses. Dabei werden u. a. folgende Fragen herangezogen:

- Sind die Prozesse noch aktuell?
- Hat sich die Sicherheitslage geändert?
- Gibt es neue Technologien, die eine Anpassung notwendig machen?

Das folgende Schaubild zeigt den Ablauf.



Policymanagement der FHH

Das Policymanagement der FHH konkretisiert die in der „Grundsatzvereinbarung über Kooperation, Auftragsdatenverarbeitung und Betrieb des Hamburgischen Telekommunikationsnetzes“ (GüKAB) getroffenen Vereinbarungen. Der Zweck besteht darin, den Forderungen der GüKAB nach einer Sicherheitspolicy nachzukommen, um ausschließlich erwünschte Kommunikationsverbindungen zwischen dem FHH-Netz und anderen Netzen zu zulassen und zu dokumentieren.

Sicherheitsvorfälle

Sicherheitsvorfälle sind Ereignisse, die den Verlust der Verfügbarkeit, Integrität oder Vertraulichkeit bedeuten können sowie Ereignisse, durch die die Belange der Informationssicherheit berührt werden. Ein Sicherheitsvorfall ist ein Verstoß oder ein vermuteter Verstoß gegen die Sicherheitsziele bzw. gegen die im IT-Handbuch festgelegten Sicherheitsmaßnahmen oder Richtlinien.

Anhang 2 Aufgaben und organisatorische Beziehungen

Aufgaben des InSiMa

Die Informationssicherheitsleitlinie der FHH (IS-LL) legt allgemeinverbindliche Grundsätze für die Informationssicherheit in der Hamburgischen Verwaltung fest, die in diesem Konzept weitere Konkretisierung erfahren. Zu den Aufgaben des InSiMa gehören:

- Beschreibung sämtlicher zentraler und behördenübergreifender Informationssicherheits-Prozesse,
- Abgrenzung, was zentral durch InSiMa und was dezentral durch die beh. InSiBe zu dokumentieren und zu überprüfen ist,
- Prioritätensetzung beim Basis-Sicherheitscheck nach IT-Grundschutz für BASIS und Non-BASIS im Sinne des Standards 100-2,
- Beschreibung der Zusammenarbeit / organisatorischen Beziehungen des InSiMa mit den beh. InSiBe sowie mit der Sicherheitsorganisation bei Dataport und dem HmbBfDI,
- Bestimmung der zentralen Informationssicherheitsziele auf Grundlage der Vorgaben des Senates und Fortschreibung der IS-LL und des RaSiKo,
- Prüfung, ob die IS-LL bzw. das RaSiKo und die darin vorgegebenen Maßnahmen umgesetzt werden und wirksam sind,
- Organisation und Durchführung von Schulungen zur Informationssicherheit für beh. InSiBe,
- Untersuchung von Vorfällen, die die behördenübergreifende 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 zentralen Informationssicherheitsmanagement,
- Vertretung der FHH in zentralen Informationssicherheitsthemen gegenüber anderen Ländern und dem Bund,
- Vorsitz der Arbeitsgruppe Informationssicherheit der FHH (InSiMa AG), in der die beh. InSiBe sich regelmäßig austauschen,
- Regelmäßiger Austausch mit dem IT-Dienstleister Dataport, wobei das InSiMa generelle Sicherheitsvorgaben festlegt und diese mit entsprechenden Controlling-Maßnahmen versieht,
- Planung und Durchführung von Infrastrukturmaßnahmen und Sicherheitsprojekten im Rahmen der Vorhabenplanung,
- Regelmäßige Aufbereitung und Zusammenfassung der Sicherheitslage in Berichten.

Kompetenzen des InSiMa

- Einsichtnahme in Dokumente aller Organisationseinheiten der FHH und bei Dataport, die die Informationssicherheit betreffen unter Berücksichtigung etwaiger einschlägiger Rechtsvorschriften,
- Vortragsrecht des InSiMa beim Amtsleiter/Staatsrat der für die Informationstechnik zuständigen Behörde,
- Ständiges, nicht stimmberechtigtes Mitglied im ITAB ,
- Teilnehmer in Besprechungen auf IT-Leiter-Ebene/IT-Beauftragten-Ebene,
- Anordnung und Durchsetzung von Maßnahmen, um bei Gefahr im Verzug Risiken für die FHH abzuwehren. Die Durchsetzung erfolgt nach vorheriger Information der betroffenen Behörden. Dabei ist sicherzustellen, dass einschränkende Maßnahmen des InSiMa im Bereich der Gefahrenabwehr, der Strafverfolgung, des Verfassungsschutzes und der Strafvollstreckung grundsätzlich nach Rücksprache mit der fachlich zuständigen Behörde erfolgen. Der Umgang mit abgestimmten geschäftskritischen Prozessen der FHH bleibt hiervon unberührt.

Aufgaben, Befugnisse und Besonderheiten der/des beh. InSiBe

- Beratung der mit Informationsprozessen befassten Stellen in Fragen der Informationssicherheit,
- Erstellung und Fortschreibung eines Sicherheitskonzepts für die Organisationseinheit. Das Sicherheitskonzept erfüllt die Rahmenvorgaben des RaSiKo und beschreibt alle weiteren erforderlichen Maßnahmen zur Informationssicherheit in der jeweiligen Organisationseinheit,
- Planung und Erarbeitung von behördenspezifischen Vorgaben und Konzepten im Rahmen der Informationssicherheit in Zusammenarbeit mit der IT-Leitung. Dazu gehören insbesondere die Verantwortung für
  - die Dokumentation der örtlichen Infrastruktur (Aufnahme des IT-Verbundes),
  - die Aufnahme der IT-Verfahren/Anwendungen (Verfahrenskataster) der Organisationseinheit in Zusammenarbeit mit den Fachlichen Leitstellen,
  - die Erarbeitung zusätzlicher behördenspezifischer Vorlagen und Checklisten für die Erstellung der sicherheitsrelevanten Verfahrens-Dokumentation und
  - die Unterstützung der zuständigen Stellen (Auftraggeber, Fachlichen Leitstellen) und des/der behDSB in Fragen zu Verfahrensbeschreibungen und Risikoanalysen,
- Unterstützen bei der Durchführung von Basis-Sicherheitschecks durch die zuständigen Stellen (z.B. Fachliche Leitstelle),
- Teilnahme am regelmäßigen Informationsaustausch bzw. an der Arbeitsgruppe des InSiMa. Dazu gehören das Mitwirken bei der Erarbeitung von Handlungsempfehlungen, der Austausch von Informationen bei der Behandlung von Sicherheitsvorfällen und die Erarbeitung von zentralen Sicherheitsmaßnahmen,
- Unterrichtung der Beschäftigten in Fragen der Informationssicherheit; insbesondere Beratung der Beschäftigten, Durchführung von Sensibilisierungsmaßnahmen, Information über ggf. auftretende Sicherheitsprobleme und Hilfestellung bei Aus- und Fortbildungsmaßnahmen,
- Prüfung, ob in der Behörde alle vorgeschriebenen Maßnahmen zur Informationssicherheit umgesetzt werden. Dazu gehören die Überprüfung im Rahmen der übergeordneten und behördenspezifischen Vorgaben und damit verbunden auch eine Berichtspflicht an die Leitungsebene, wenn gegen Vorgaben verstoßen wurde und die Unterstützung bei der Erstellung von Verfahrensbeschreibungen, Risikoanalysen und Schutzbedarfsfeststellungen,
- Regelmäßige Aufbereitung und Zusammenfassung der Sicherheitslage in Berichten an die Leitungsebene.

Mit folgenden Befugnissen ist die/der beh. InSiBe unter Berücksichtigung der entsprechenden Spezialregelungen (z.B. Geheimschutz, Steuerrecht, Personalrecht) ausgestattet:

- Vortragsrecht bei der Leitungsebene,
- Zutrittsrecht zu besonders gesicherten Bereichen, sofern die Informationssicherheit betroffen ist,
- Einsichtnahmerecht in Dokumente, die die Informationssicherheit betreffen und zur Gewährleistung des erforderlichen Sicherheitsniveaus beitragen,
- Auskunftsrecht bei Prüfungen und in besonderen Fällen (z.B. wenn die Informationssicherheit gefährdet ist).

Die/der beh. InSiBe ist zu bestellen. Die Bestellung ist in der OE bekannt zu machen und sie/er sollte im Organigramm der Behörde/Amt/Organisationseinheit aufgeführt werden.

Aufgaben des IT-Dienstleisters Dataport

Im Rahmen der Datenverarbeitung im Auftrag ist Dataport für einen sicheren IT-Betrieb in der FHH verantwortlich. Zentrale Infrastrukturen (z.B. FHH-Netz, Firewall, Exchange, zentraler Virenschutz) werden durch Dataport betrieben sowie durch Dataport und das InSiMa einer Sicherheitsbetrachtung unterzogen. Dies gilt auch für den Standardarbeitsplatz der FHH.

Dataport betreibt ein IT-grundschutzkonformes und BSI-zertifiziertes Rechenzentrum. Um den IT-grundschutzkonformen Betrieb zu gewährleisten, pflegt Dataport eine Sicherheitskonzeption und entsprechende Betriebshandbücher. Zusätzlich pflegt Dataport Notfallhandbüchern, die die Abwicklung von Sicherheitsvorfällen und IT-Notfällen beschreibt.

Eine von der FB genehmigte Basispolicy (Anhang 5, A1; Begriffsbestimmungen) und das Policymanagement (Anhang 5, A1; Begriffsbestimmungen) ermöglichen Dataport, eine Netzöffnung selbstständig nach den genannten Vorgaben durchzuführen. Netzöffnungen, die von der Policy nicht abgedeckt sind, müssen durch das InSiMa genehmigt werden (näheres siehe Grundsatzvereinbarung über Kooperation, Auftragsdatenvereinbarung und Betrieb des Hamburgischen Telekommunikationsnetzes) (Anhang 5, A1).

Dataport hat bei Datenverarbeitung im Auftrag die erforderlichen Dokumente zur Verfügung zu stellen.

Organisatorische Beziehungen im Informationssicherheitsverbund der FHH

Das Zusammenspiel der Sicherheitsorganisation mit den in der FHH etablierten Prozessen, Gremien und Organisationseinheiten für zentrale übergreifende Aufgaben in der FHH stellt sich in der nachfolgenden Abbildung wie folgt dar. Eine Beschreibung inkl. der Nummern an den Pfeilen (Pfeil-Nr.) wird in der nachfolgenden Beschreibung (unterhalb der Abbildung) aufgeführt:

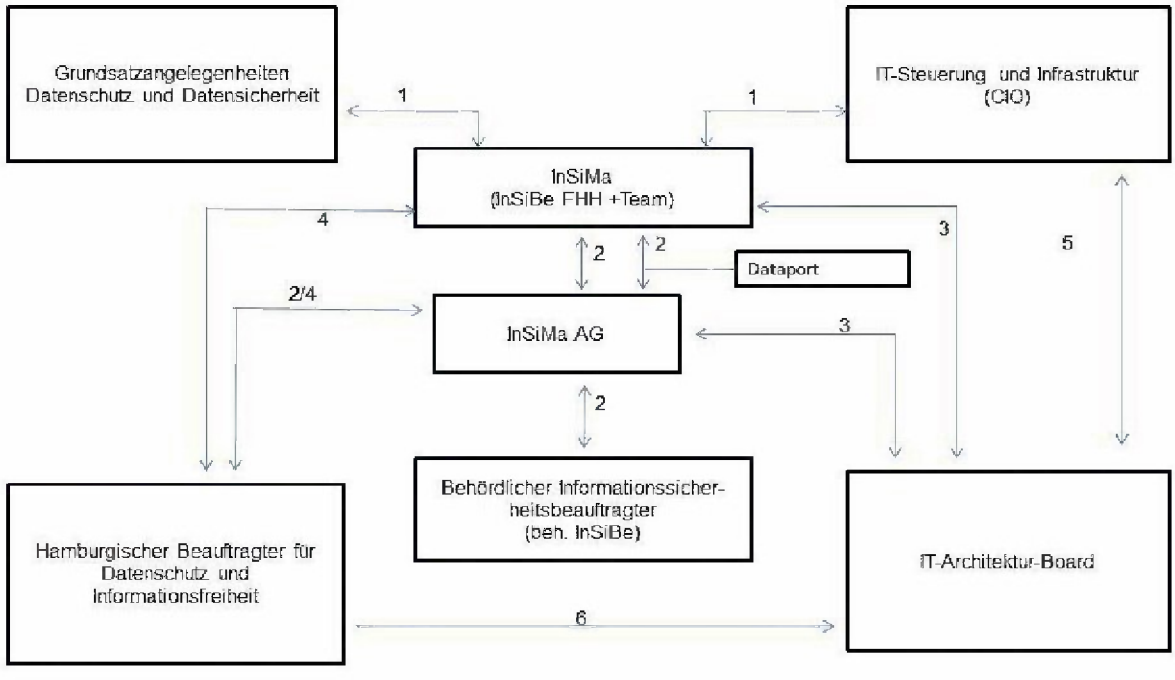


Abbildung: Einbindung Informationssicherheitsmanagement in der FHH

Das InSiMa besteht aus der/dem InSiBe der FHH (Informationssicherheitsbeauftragter der FHH) und dem InSiMa-Team (Beschäftigte aus den Bereichen IT-Technik, Datenschutz und Datensicherheit) und ist in der für die Informationstechnik zuständigen Behörde etabliert (Fachaufsicht IT, Pfeil-Nr. 1). Es wird in technischen Fragen vom zentralen IT-Dienstleister Dataport beraten und unterstützt. Es besteht eine enge Zusammenarbeit mit dem Chief Information Officer der FHH (CIO), der für Grundsatzangelegenheiten „Datenschutz und Datensicherheit" zuständigen OE in der Finanzbehörde und dem zentralen IT-Dienstleister auf dem Gebiet der Informationssicherheit. Das dort eingesetzte IT-Sicherheitsmanagement sorgt für die techni-

sche Umsetzung der generellen Sicherheitsvorgaben und Richtlinien und gibt zu Sicherheitsrisiken Einschätzungen und Handlungsempfehlungen ab. Die/der beh. InSiBe koordiniert im Auftrag der Leitungsebene die Aufgabe Informationssicherheit für die Behörde, wobei die konkrete Aufgabenabgrenzung (originäre Aufgaben der IT-Stelle und Aufgaben im Zusammenhang mit der Informationssicherheit) der Leitungsebene vorbehalten bleibt.
Das InSiMa lädt regelmäßig die beh. InSiBe und Vertreter des IT-Dienstleisters Dataport zur Arbeitsgruppe InSiMa (InSiMa AG) ein. Näheres ist in der Geschäftsordnung zur InSiMa AG (Anhang 5, A5) geregelt (Beteiligung, Pfeil-Nr. 2).
Sicherheitsthemen werden u.a. in der InSiMa AG diskutiert und für das ITAB zur Beschlussfassung vorbereitet. Das InSiMa kann auch direkt Themen über das ITAB beschließen lassen (Entscheidungsvorbereitung, Pfeil-Nr. 3).

Es findet ein regelmäßiger Informationsaustausch zwischen dem InSiMa und dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) statt. Der HmbBfDI ist in der InSiMa AG mit zwei Rollen vertreten: Als beh. InSiBe und beratend als hamburgischer Beauftragter für Datenschutz und Informationsfreiheit (Beratung, Pfeil-Nr. 4).
Das ITAB (bestehend aus dem CIO und ausgewählten IT-Leitungen) fasst und veröffentlicht Beschlüsse für die Fortschreibung der IT-Infrastruktur in der FHH und zu infrastrukturellen Maßnahmen zur Verbesserung der IT-Sicherheit. (Entscheidung und Beschluss Pfeil-Nr. 3 und 5).
Der HmbBfDI nimmt an den Sitzungen des ITAB als Gast teil. (Pfeil-Nr. 6).

Ferner hat Dataport als zentraler IT-Dienstleister die Aufgabe, die organisatorischen Vorgaben technisch umzusetzen. Dataport unterliegt dabei einer ständigen Kontrolle durch die FHH. Darüber hinaus hat Dataport die Aufgabe, eine frühzeitige Erkennung einer Bedrohung der Informationssicherheit der FHH zu erkennen und abzuwehren. Dafür ist ein Team für Sicherheitsvorfälle – CERT (Computer Emergency Response Team) – zuständig. Neben diesem LandesCERT verfügt Hamburg auch über ein CERT bei der Polizei Hamburg, zu dem ein ständiger Kontakt besteht. Ein weiterer ständiger Kontakt in Fragen zur Informationssicherheit besteht zum BSI.

Anhang 3 Das FHH-Netz

Über das FHH-Netz werden verschiedene Dienste (IP-Datennetz und IP-Telefonie) abgewickelt. Mittels Segmentierung kann das Netz in mehrere logische Abschnitte eingeteilt werden, um eine Mandantenfähigkeit zu realisieren (z.B. Polizei).
Das Backbone der FHH einschließlich der Übergaberouter verbindet die Behördenstandorte untereinander mit der Infrastruktur von Dataport. Es liegt in der Verantwortung der für die Informationstechnik zuständigen Behörde, die Dataport mit dem Betrieb beauftragt hat.
Dataport betreibt die internen Netze, Rechenzentren und den Übergang in das Internet (WAN) in eigener Verantwortung nach Maßgabe der für die Informationstechnik zuständigen Behörde.
Von VPN-Clients aus ist über das Internet der Zugriff auf das FHHNET möglich. Darüber hinaus gibt es standardisierte Zugriffsmöglichkeiten auf Anwendungen im FHHNetz (z. B. über Zuvex), die in der Verantwortung der für die Informationstechnik zuständigen Behörde liegen.

Die Verantwortlichkeiten für die Netze und die Clients sind in der nachfolgenden Abb. dargestellt.

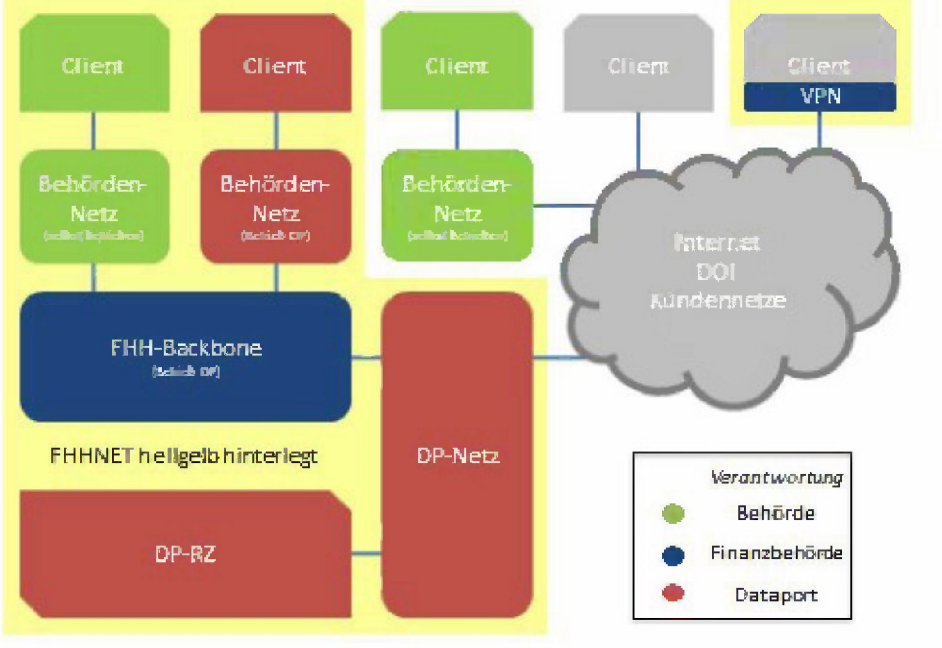


Abbildung: Verantwortlichkeiten im FHH-Netz

Anhang 4 Klassifizierung von Sicherheitsvorfällen

Die folgende Matrix stellt dar, wie Sicherheitsvorfälle zu klassifizieren sind. Dabei wird nach Dringlichkeit und Auswirkung die jeweilige Kritikalität festgelegt:

		Priorität / Kritikalität			
Dringlichkeit	Kritisch	Hoch	Hoch	Kritisch	Kritisch
	Hoch	Mittel	Hoch	Hoch	Kritisch
	Mittel	Niedrig	Mittel	Hoch	Hoch
	Niedrig	Niedrig	Niedrig	Mittel	Hoch
		Niedrig	Mittel	Hoch	Kritisch
		Auswirkung			

Die verschiedenen Stufen der Auswirkung und der Dringlichkeit sind dabei wie folgt zu verstehen, wobei jeweils alle der genannten Punkte erfüllt sein müssen:

Auswirkung

Niedrig

- Ereignis betrifft einzelne oder mehrere Anwender,
- die Geschäftstätigkeit der Organisation/der Anwender ist nicht eingeschränkt.

Mittel

- Ereignis betrifft einzelne Anwender,
- die Geschäftstätigkeit der Organisation/der Anwender kann mit leichten Einschränkungen aufrechterhalten werden.

Hoch

- Ereignis betrifft die Mehrzahl der Anwender oder mehrere Behörden, oder einzelne Anwender oder wenige Behörden, wenn der Ausfall erhebliche Folgen für die FHH hat,
- Kunden (z.B. Bürger, Firmen) sind teilweise betroffen oder Services eingeschränkt,
- geschäftskritische Systeme sind betroffen,
- die Geschäftstätigkeit der Organisation/der Anwender kann eingeschränkt aufrechterhalten werden.

Kritisch

- Ereignis betrifft alle Anwender oder mehrerer Behörden oder einzelne Anwender oder wenige Behörden, wenn der Ausfall gravierende Folgen für die FHH hat,

- Kunden (z.B. Bürger, Firmen) sind massiv betroffen oder Services stark eingeschränkt,
- geschäftskritische Systeme sind betroffen,
- die Geschäftstätigkeit der Organisation/der Anwender kann nicht aufrechterhalten werden.

Dringlichkeit

Niedrig

- Ersatzlösungen stehen zur Verfügung und können genutzt werden,
- die behinderten Tätigkeiten können später durchgeführt werden.

Mittel

- Ersatzlösungen stehen nicht für alle betroffenen Anwender zur Verfügung,
- die behinderten Tätigkeiten können später oder auf anderem Wege evtl. mit mehr Aufwand durchgeführt werden.

Hoch

- Ersatzlösungen stehen kurzfristig nicht zur Verfügung,
- die behinderten Tätigkeiten müssen durchgeführt werden.

Kritisch

- Ersatzlösungen stehen nicht zur Verfügung,
- die behinderten Tätigkeiten müssen kurzfristig durchgeführt werden.

Prioritätsstufen / Kritikalität / Zuständigkeiten / Meldewege

Priorität Niedrig

- Bearbeitung durch das InSiMa oder die zuständige dezentrale Organisationseinheit (in der Regel beh. InSiBe),
- Überwachung des Lösungsfortschritts,
- Information der Leitungsebene im periodischen Berichtswesen,
- ggf. Behörden-/Anwenderinformation im periodischen Berichtswesen.

Priorität Mittel

- Bearbeitung durch das InSiMa oder die zuständige dezentrale Organisationseinheit (in der Regel beh. InSiBe),
- Überwachung des Lösungsfortschritts,
- Information der Leitungsebene im periodischen Berichtswesen,
- ggf. Behörden-/Anwenderinformation im periodischen Berichtswesen.

Priorität Hoch

- bevorzugte Bearbeitung durch das InSiMa oder ggf. die zuständige dezentrale Organisationseinheit (in der Regel beh. InSiBe),

- besondere Überwachung des Lösungsfortschritts,
- Information der Leitungsebene und InSiMa innerhalb 12 Stunden,
- ggf. Behörden-/Anwenderinformation innerhalb von 12 Stunden (Absprache OE, InSiMa, Dataport).

Priorität Kritisch

- umgehende Bearbeitung durch den InSiMa oder ggf. die zuständige dezentrale Organisationseinheit (in der Regel beh. InSiBe),
- intensive Überwachung des Lösungsfortschritts,
- Information der Leitungsebene und InSiMa unverzüglich,
- Behörden bzw. Anwenderinformation erfolgt unverzüglich (Absprache OE, InSiMa, Dataport).

Anhang 5 Verbindliche und empfohlene Vorgaben

Die Verweise auf Richtlinien und Konzepte unterscheiden sich grundsätzlich in verbindliche und empfehlende Vorgaben.

	Verbindliche Vorgaben
A1	1. Sicherheitspyramide Informationssicherheitsmanagement 1.1 Informationssicherheitsleitlinie 1.2 IT-Richtlinien (IT-Handbuch im Rechtsportal) 1.3 ITAB-Beschlüsse 1.3.1 Konzept zur Bewertung und Verteilung von Sicherheits-Patches für Endgeräte in der FHH V1.1 vom 01.09.2014 1.4. Behördenübergreifende IT-Vorgaben, Konzepte 1.4.1 Grundsatzvereinbarung_DP_FHH 1.4.2 Basispolicy FHHNet v1.4 1.4.3 Policymanagement FHHNet v1.5
A2	Richtlinie zur Beteiligung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit Konzept behördliche Datenschutzbeauftragte
A3	Vereinbarungen nach § 94 HmbPersVG (alt), bzw. § 93 HmbPersVG (neu)
A4	Anlage 3, 5 und 10 zu den Verwaltungsvorschriften für Zahlungen, Buchführung und Rechnungslegung (VV-ZBR)
A5	Geschäftsordnung der InSiMa AG
	Empfehlende Vorgaben
A6	Konzept Einführung IT-Grundschutz in der FHH
A7	1. BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS) 2. BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise 3. BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz 4. BSI-Standard 100-4: Notfallmanagement 5. IT-Grundschutz-Katalog

Anlage 1 Schichtenmodell nach IT-Grundschutz

In den IT-Grundschutz-Katalogen wird beschrieben, wie auf der Basis von Standard-Sicherheitsmaßnahmen Sicherheitskonzepte erstellt und geprüft werden. Für typische Prozesse, Anwendungen und Komponenten in der Informationstechnik finden sich außerdem geeignete Bündel („Bausteine“) von Standard-Sicherheitsmaßnahmen. Das Schichtenmodell bildet die Grundlage für die Basis-Sicherheitschecks. Dabei sind im BASIS-Umfeld die Schicht 3 und 4 durch Dataport bereits abgebildet, die Schicht 1 durch das InSiMa. Diese Bausteine sind entsprechend ihrem jeweiligen Fokus in folgende fünf Schichten (Schichtenmodell) aufgeteilt:

- **Schicht 1**:
  Umfasst sämtliche übergreifenden Aspekte der Informationssicherheit. Beispiele sind die Bausteine Personal, Datensicherungskonzept und Outsourcing.
- **Schicht 2:**
  Befasst sich mit den baulich-technischen Gegebenheiten. Beispiele sind die Bausteine Gebäude, Serverraum und häuslicher Arbeitsplatz.
- **Schicht 3:**
  Befasst sich mit den einzelnen IT-Systeme. Beispiele sind die Bausteine Allgemeiner Client, Allgemeiner Server, TK-Anlage, Laptop und Mobiltelefon.
- **Schicht 4:**
  Betrachtet die Vernetzungsaspekte der IT-Systeme. Beispiele sind die Bausteine Heterogene Netze, WLAN, VoIP sowie Netz- und Systemmanagement.
- **Schicht 5:**
  Befasst sich mit den eigentlichen Anwendungen. Beispiele sind die Bausteine E-Mail, Webserver und Datenbanken.

Nachfolgend sind nach Ansicht des InSiMa wichtige Aspekte des Schichtenmodells in Kurzform wiedergegeben. Konkrete Maßnahmen hierzu können den Grundschutzkatalogen des BSI entnommen werden.

Um Doppelarbeit bei der Dokumentation zu vermeiden, wird sich in der InSiMa AG darüber verständigt, welche Teile zentral und welche Teile dezentral zu dokumentieren sind. Dabei gilt grundsätzlich, dass behördenübergreifende Infrastrukturen entweder durch Dataport oder durch zentrale fachliche Leitstellen beschrieben werden.

B1 Übergeordnete Aspekte (Schicht 1)

Sicherheitsmanagement

Das InSiMa hat die Sicherheitsziele und die Sicherheitsstrategie der FHH (Vorgaben zur Planung, Gewährleistung und ständiger Aufrechterhaltung der IT-Sicherheit) festzulegen und diese regelmäßig im Rahmen des generellen Sicherheitsprozesses auf ihre Wirksamkeit zu überprüfen.

Organisation

Verantwortlichkeiten im Aufgabenspektrum der Informationssicherheit sind zu bestimmen (siehe Anhang 2). Verantwortlich für die Informationssicherheit einer Behör-

de ist grundsätzlich die Behördenleitung als Teil der allgemeinen Leitungsverantwortung. Bei der Aufgabenverteilung ist soweit möglich eine Funktionstrennung zu berücksichtigen. Es ist zu bestimmen, welche Kommunikationsarten - abhängig von der Klassifizierung der Daten - intern und extern zulässig sind (z. B. E-Mail-Verschlüsselung, FAX, Datentransport). Insbesondere bei Auftragsdatenverarbeitung sind die Namen der Ansprechpartner schriftlich oder in Textform festzulegen und eine Änderung zeitnah den von den Verfahrensverantwortlichen bestimmten Kontaktpersonen mitzuteilen.

Personal:
Neue Beschäftigte für das Sicherheitsmanagement sind einzuweisen und einzuarbeiten. Im Falle des Ausscheidens von Beschäftigten ist ein strukturierter Prozess für die Änderung der Berechtigungen zu etablieren.

Notfallmanagement, Sicherheitsvorfälle und Datensicherung
Prozesse für die Bearbeitung von Sicherheitsvorfällen oder zur Notfallvorsorge sind zu etablieren. Diesbezüglich bestimmen die Organisationseinheiten, ob das übergeordnete Notfallkonzept (der FHH oder des IT-Dienstleisters) im jeweiligen Verantwortungsbereich zur Anwendung kommen kann oder ob darüber hinaus eigene Notfallkonzepte zu erstellen sind. Beim Vorgehen zur Behebung von IT-Notfällen sind außer dem Herstellersupport oder dem Support des IT-Dienstleisters Dataport auch andere Informationsquellen, wie BSI, Sicherheits-Newsletter und ähnliches einzubeziehen. Weitere Maßnahmen für den Betrieb sind im Einzelnen im Notfallkonzept darzustellen.
Die eingesetzten Datensicherungsverfahren, Datensicherungspläne, Art und Umfang der Datensicherungen sowie die Datenrekonstruktion sind in Service Level Agreements zu definieren. Die festgestellten Schutzbedarfe der Informationsverbünde sind regelmäßig zu überprüfen.

Ausgelagerte Datenverarbeitung "Outsourcing"
Große Teile der Datenverarbeitung der FHH werden beim IT-Dienstleister Dataport im Rechenzentrum durchgeführt. Die Gesamtverantwortung verbleibt dabei bei der Auftrag gebenden Stelle. Der Auftrag ist schriftlich zu erteilen. Dort sind insbesondere der Auftragsumfang, technische und organisatorische Maßnahmen und gegebenenfalls Unterauftragsverhältnisse festzulegen. Änderungen der benannten Ansprechpartner sind zeitnah und unaufgefordert mitzuteilen. Die Grundlage für das Outsourcing bilden die Staatsverträge der Länder.

Verschlüsselung
Nach Prüfung im Einzelfall und gegebener Notwendigkeit sind Daten innerhalb des FHH-Netzes zu verschlüsseln. Sofern sensible, personenbezogene Daten oder als schützenswert deklarierte Daten (insbesondere Daten von Liegenschaften der FHH) das FHH-Netz verlassen, müssen dem Schutzbedarf der Daten entsprechende Maßnahmen sichergestellt werden.

Hard- und Softwareverteilung
Informationssicherheit für Hard- und Softwareverteilung ist in Anlehnung an den IT-Grundschutz durch Dataport sicherzustellen. Dabei ist insbesondere die Konfiguration von IT-Systemen und Anwendungen über zentral gesteuerte Einstellungen (Group-Policies) vorzunehmen.

Sensibilisierung und Schulung zur Informationssicherheit

Alle Beschäftigten der FHH sind zur Informationssicherheit zu schulen und zu sensibilisieren (§ 94 HmbPersVG, Konzept behördliche Datenschutzbeauftragte, PC-Richtlinie, Eckpunktepapier behördliche Informationssicherheitsbeauftragte, Schulungskonzept). Grundsätzlich sind notwendige Schulungen und Sensibilisierungen zur Informationssicherheit von allen Beschäftigten wahrzunehmen. Darüber hinaus sind bei der Einführung neuer Verfahren darauf abgestimmte Schulungsangebote anzubieten.

Löschen und Vernichten von Daten
Es ist sicherzustellen, dass Datenträger für alle Datenbestände oder papiergebundene Daten datenschutzkonform entsorgt werden beziehungsweise elektronische Daten nach dem Stand der Technik endgültig gelöscht werden. Die Verwaltung und die IT-Administration, aber auch alle Beschäftigten haben dafür Sorge zu tragen, dass die gesetzlichen Vorgaben und internen Vorschriften Beachtung finden. Darüber hinaus können im Einzelfall gesonderte Regelungen erlassen werden.

B2 Infrastruktur (Schicht 2)

Die Gebäudeinfrastruktur der FHH und der weiteren Organisationseinheiten ist über das gesamte Stadtgebiet verteilt. Teilweise sind die Organisationseinheiten in eigenen Gebäuden untergebracht, teilweise werden angemietete Flächen genutzt. In jedem Fall trägt die nutzende Organisationseinheit die Verantwortung hinsichtlich der Gebäudesicherheit und der in den jeweiligen Gebäuden vorhanden IT-Technik. Sofern besondere Zutrittsregelungen zu beachten sind, sind angemessene organisatorische und technische Maßnahmen zu ergreifen.

Sofern in Schulungs- und Besprechungsräumen separate Netzzugänge eingerichtet sind, sind diese abzusichern und die Protokollierung datenschutzkonform zu gestalten. Die zentrale Installation und Re-Installation der IT-Systeme für den Schulungsbereich ist anzustreben. Für die Ausstattung mit WLAN sind gesonderte Konzepte zu beachten und in Anlehnung an BSI-Standards zu konfigurieren. Darüber hinaus gelten die Sicherheitsrichtlinien des LAN adäquat.
Grundlage für die Telearbeit ist das vorhandene Konzept zur Telearbeit.

B3 IT-Systeme (Schicht 3)

Informationssicherheit für IT-Systeme ist in Anlehnung an IT-Grundschutz durch Dataport sicherzustellen. Betriebs- und Supportleistungen für Endgeräte, lokale Netze und Clientkomponenten von Verfahren sind im Hinblick auf die Informationssicherheit und unter Beachtung des Service Level Agreements (SLA) zu regeln.

Sicherheitspatches sind unabhängig vom Release-Konzept der FHH je nach Kritikalität unter Beachtung der Freigaberichtlinie unverzüglich auszurollen. Das betrifft Patches für Microsoftprodukte sowie Adobe-Reader, Adobe-Flashplayer und Java. Die Non-BASIS-Bereiche sind verpflichtet, Sicherheitspatches analog den BASIS-Bereichen zu verteilen und sich am zentralen ePO-Dienst bei Dataport anzuschließen.

B4 **Netze (Schicht 4)**

Dataport betreibt das Hamburgische Telekommunikationsnetz (FHH-Netz) und stellt dieses der FHH und den weiteren Organisationseinheiten für Datenkommunikation als auch für sprachliche Kommunikation zur Verfügung (Grundsatzvereinbarung über

Kooperation, Auftragsdatenverarbeitung und Betrieb des Hamburgischen Telekommunikationsnetzes). Übergänge ins öffentliche Netz sind durch ein Sicherheitsgateway getrennt, das nach aktuellen Empfehlungen des BSI abgesichert ist (Basis-Policy-FHH-Netz, Policymanagement FHH-Netz).

Dataport ist von der für die Informationstechnik zuständigen Behörde als Netzbetreiber für die Planung, Errichtung, Instandhaltung, Optimierung und den Betrieb des Netzes, für die Unterstützung der Nutzer des FHH-Netzes sowie für die ordnungsgemäße und wirtschaftliche Nutzung des FHH-Netzes und seiner Einrichtungen beauftragt.

B5 Anwendungen und Fachverfahren (Schicht 5)

Die für die behördenübergreifenden Infrastrukturen fachlich zuständigen Stellen (z. B. FB17 für FHHPortal, ZPD für PAISY) müssen eine Sicherheitsbetrachtung nach diesem RaSiKo durchführen. Für behördliche Fachverfahren müssen Sicherheitsbetrachtungen nach diesem RaSiKo und ergänzenden Sicherheitskonzepten der jeweiligen Behörde durch die dezentralen Organisationseinheiten (in der Regel der Auftraggeber oder die Fachliche Leitstelle) angefertigt werden.