Freie Hansestadt Bremen

Informationssicherheitsleitlinie der Freien Hansestadt Bremen (IS-LL)

Inkrafttreten: 16.05.2017

Inhalt

1. Regelungsgegenstand, Geltungsbereich und Inkrafttreten 3
2. Ziele der Informationssicherheit 3
3. Grundsätze der Informationssicherheit 3
   - 3.1 Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) 3
   - 3.2 Bereitstellung von Ressourcen 3
   - 3.3 Prinzip der informierten und sensibilisierten Nutzerinnen und Nutzer 4
   - 3.4 Sicherheit vor Verfügbarkeit 4
   - 3.5 Es gelten die Grundsätze der Schutzbedarfsfeststellung 4
   - 3.6 Minimalprinzip bei Zugriffs- und Nutzungsrechten 4
4. Verantwortlichkeiten und Rollen 4
   - 4.1 Verantwortung der Leitungsebene 4
   - 4.2 Verantwortung der Beschäftigten 5
   - 4.3. Fachverantwortliche 5
   - 4.4. Einsatz externer Leistungserbringer 5
5. Informationssicherheitsorganisation 5
   - 5.1 Informationssicherheitsbeauftragte der FHB 5
   - 5.2 Informationssicherheitsbeauftragte der Ressorts 6
   - 5.3 Arbeitsgruppe Informationssicherheitsmanagement 6
   - 5.4 Computer Emergency Response Team (CERT Nord) 7
6. Fortschreibung und Revision 7
7. Schlussbestimmungen 7

1. Regelungsgegenstand, Geltungsbereich und Inkrafttreten

Die Senatorin für Finanzen erlässt im Bekenntnis zum Stellenwert der Informationssicherheit für die FHB die vorliegende Informationssicherheitsleitlinie als die grundlegende Regelung zur Informationssicherheit.

Die Senatorin für Finanzen und jedes Ressort achten in ihrem jeweiligen Geschäftsbereich auf die Einhaltung dieser Leitlinie. Soweit diese für ihre Geschäftsbereiche Regelungen zur Informationssicherheit erarbeiten, geschieht dies stets auf Grundlage dieser Leitlinie.

2. Ziele der Informationssicherheit

Für den Schutz von Informationen sind zunächst Zielzustände zu definieren, welche mit geeigneten Sicherheitsmechanismen erreicht werden sollen. Je nach Aufgabenspektrum können unterschiedliche Schwerpunkte gesetzt bzw. Grundwerte formuliert werden.

Übergeordnete und unabdingbare Bedeutung für die Freie Hansestadt Bremen erlangen die drei Grundschutzziele:

- *Vertraulichkeit* - Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.
- *Integrität* – Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Informationen.
- *Verfügbarkeit* – Eigenschaft, dass Informationen einer berechtigten Einheit auf Verlangen zugänglich und nutzbar sind.

Die Betrachtung weiterer Sicherheitsziele bzw. Grundwerte kann je nach Einsatzfall zu einer differenzierteren und ausgewogeneren Bewertung des Schutzbedarfes der Informationen führen. Insofern besteht grundsätzlich die Möglichkeit, weitere Sicherheitskriterien – unbeschadet etwaiger Schnittmengen zwischen einzelnen Kriterien – heranzuziehen. Beispielhaft seien hier die Authentizität, die Revisionsfähigkeit, die Nichtverkettbarkeit sowie die Transparenz genannt.

3. Grundsätze der Informationssicherheit

3.1 Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Zur Erreichung und Aufrechterhaltung eines angemessenen und ausreichenden Informationssicherheitsniveaus sind für die Freie Hansestadt Bremen die Standards und Kataloge des BSI maßgeblich.

3.2 Bereitstellung von Ressourcen

Zur Erreichung der IT-Sicherheitsziele sind durch die Senatorin für Finanzen und die Ressorts ausreichende Ressourcen zur Verfügung zu stellen. Sollten einzelne IT-Sicherheitsprozesse nicht finanzierbar sein, sind die Geschäftsprozesse, die IT-Sicherheitsstrategie sowie die Art und Weise des IT-Betriebs zu überdenken und gegebenenfalls anzupassen.

3.3 Prinzip der informierten und sensibilisierten Nutzerinnen und Nutzer

Gezielte Sensibilisierung sowie Qualifizierung der Beschäftigten sind die Grundvoraussetzung für die Informationssicherheit. Die Beschäftigten der FHB gewährleisten die notwendige und angemessene IT-Sicherheit durch ihr verantwortungsvolles Handeln.

3.4 Sicherheit vor Verfügbarkeit

Wird die IT-Infrastruktur angegriffen oder bedroht, können entsprechend der Schutzbedarfe vorübergehende Verfügbarkeitsbeschränkungen der betroffenen IT-Systeme vorgenommen werden. Dabei sind Einschränkungen beim Betrieb sowie im Komfort der Bedienung, insbesondere bei Netzübergängen in das Internet, vertretbar.

Bei Gefahr im Verzug insbesondere bei ressortübergreifenden Sicherheitsvorfällen kann der Informationssicherheitsbeauftragte der FHB die erforderlichen Sicherheitsmaßnahmen kurzfristig anordnen. Dies kann bis zur vorübergehenden Sperrung von Anwendungen oder Netzzugängen führen. Die betroffene Dienststellenleitung sowie das zuständige Informationssicherheitsmanagement sind hiervon unverzüglich zu unterrichten.

3.5 Es gelten die Grundsätze der Schutzbedarfsfeststellung

Alle Informationen, die in Prozessen der FHB verarbeitet werden, sind hinsichtlich ihres jeweiligen Schutzbedarfs nach den BSI-Standards zu klassifizieren.

3.6 Minimalprinzip bei Zugriffs- und Nutzungsrechten

Der Zugriff auf IT-Systeme ist auf den erforderlichen Personenkreis einzuschränken. Die Zugriffsrechte werden auf das erforderliche Maß zur Aufgabenerfüllung beschränkt.

4. Verantwortlichkeiten und Rollen

4.1 Verantwortung der Leitungsebene

Die Verantwortung für die ordnungsgemäße und sichere Aufgabenerledigung und damit für die Informationssicherheit hat die Leitung der Behörde oder Einrichtung (Dienststellenleitung). Sie oder die vorgesetzte Dienstbehörde erlässt die erforderlichen Regelungen zur Informationssicherheit für den Bereich der Dienststelle oder Einrichtung. Die aktuellen Regelungen sind den Beschäftigten bekannt zu geben. Die Dienststellenleitung trägt die Verantwortung für die Umsetzung der vereinbarten Sicherheitsmaßnahmen und eine geeignete Dokumentation. Die Leitungen können die Verantwortung an die für die einzelnen Fachverfahren jeweils zuständigen Fachverantwortlichen delegieren. Hierzu gehört die Nutzungsverwaltung einschließlich der Zugriffsrechte auf der Ebene der Fachverfahren. Sie stellt die Mittel für die Beschaffung und den Betrieb der vereinbarten Sicherheitsmaßnahmen zur Verfügung und veranlasst erforderliche Schulungsmaßnahmen. Die Dienststellen und Einrichtungen sind für eine dem jeweiligen Aufgabengebiet angemessene Informationssicherheit verantwortlich.

4.2 Verantwortung der Beschäftigten

Alle Beschäftigten gewährleisten die Informationssicherheit durch ihr verantwortungsvolles Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein.

4.3. Fachverantwortliche

Fachverantwortliche für einen Geschäftsprozess oder ein IT-Fachverfahren sind zuständig für:

- die Festlegung der geschäftlichen Relevanz seiner Informationen und deren Schutzbedarf und
- die Sicherstellung, dass Verantwortlichkeiten explizit definiert und Sicherheits- und Kontrollmaßnahmen zur Verwaltung und zum Schutz seiner Informationen umgesetzt werden.

4.4. Einsatz externer Leistungserbringer

Personen, Dienststellen und Unternehmen, die nicht zur FHB gehören, für diese aber Leistungen erbringen, haben die Vorgaben des Auftraggebers zur Einhaltung der Informationssicherheitsziele gemäß dieser Leitlinie einzuhalten. Der Auftraggeber verpflichtet ihn in geeigneter Weise zur Einhaltung. Dazu gehört, dass der Auftragnehmer bei erkennbaren Mängeln und Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber zu informieren hat.

5. Informationssicherheitsorganisation

5.1 Informationssicherheitsbeauftragte der FHB

Für die FHB ist für die ressortübergreifende IT die Stelle des Informationssicherheitsbeauftragten des Landes (IT-SiBe Land) einzurichten. Die Aufgaben dieser Stelle umfassen:

- Planung, Koordination, Steuerung und Dokumentation des landesweiten Informationssicherheitsprozesses;
- Leitung der AG Informationssicherheitsmanagement (ISM);
- Erstellung von Berichten an die Landesregierung und an die AG ISM über den Status der Informationssicherheit (IT-Lageberichte);
- Untersuchung sicherheitsrelevanter Vorfälle von erheblicher Bedeutung und Initiierung und Steuerung von Angeboten für Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit.

5.2 Informationssicherheitsbeauftragte der Ressorts

Die Ressorts haben Informationssicherheitsbeauftragte für den jeweiligen Geschäftsbereich (IT-SiBe Ressort) zu benennen.

Die Aufgaben eines IT-SiBe Ressort umfassen:

- Planung, Koordination, Steuerung sowie Dokumentation des ressortspezifischen Informationssicherheitsprozesses;
- Mitwirkung an der IT-Strategie und IT-Architektur des Ressorts;
- Mitwirkung an strategischen Projekten mit IT-Bezug im Ressort;
- Unterstützung des Datenschutzbeauftragten bei der Freigabe automatisierter Verfahren zur Verarbeitung personenbezogener Daten;
- Mitarbeit in der AG ISM der FHB;

Die Zusammenarbeit der IT-SiBe und der behördlichen Datenschutzbeauftragten in Bezug auf den Umgang mit personenbezogenen Daten ist dabei unerlässlich.

Die entsprechenden Dienstvereinbarungen der FHB sind hierbei zu beachten.

Den IT-SiBe des Ressort bzw. der Dienststellen sowie deren Stellvertretungen sind dabei ausreichende Möglichkeiten einer qualifizierten Aus- und Fortbildung in Themen der Informationssicherheit zu gewähren.

5.3 Arbeitsgruppe Informationssicherheitsmanagement

Zur Umsetzung der Informationssicherheitsorganisation und Unterstützung der Informationssicherheitsbeauftragten wird eine Arbeitsgruppe Informationssicherheitsmanagement (AG ISM) gebildet. Um die verschiedenen Aspekte der Informationssicherheit in der FHB berücksichtigen zu können, arbeiten in der AG ISM ständige, nichtständige sowie sonstige Mitglieder zusammen. Die AG ISM gibt sich in Abstimmung mit den Ressorts eine Geschäftsordnung.

5.4 Computer Emergency Response Team (CERT Nord)

Für die FHB ist beim zentralen IT-Dienstleister ein CERT als zentrale Anlaufstelle für präventive sowie reaktive Maßnahmen in Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle aufzubauen. Relevante Sicherheitsvorfälle müssen dem CERT gemeldet werden.

6. Fortschreibung und Revision

Die vorliegende Informationssicherheitsleitlinie wird entweder anlassbezogen oder regelmäßig alle 2 Jahre einer überprüfenden Revision unterzogen. Die Informationssicherheitsleitlinie wird dabei durch Mitglieder der AG ISM inhaltlich überprüft und im Bedarfsfall aktualisiert und danach zur Abstimmung gebracht.

7. Schlussbestimmungen

Die Zuweisungen der Rollen sowie die Einrichtung der AG ISM gemäß der Inhaltsangabe sind mit einer Frist von 12 Monaten nach Inkrafttreten dieser Informationssicherheitsleitlinie umzusetzen.

Die Verwaltungsvorschrift tritt am Tage ihrer Veröffentlichung in Kraft.