Freie Hansestadt Bremen

Rundschreiben des Senators für Finanzen Nr. 09/2026 – Compliance Informations- und Cybersicherheit

Inkrafttreten: 13.04.2026

Verteiler: Alle Dienststellen

Über Verteilerlisten:

organisation@dienststelle.bremen.de

personal@dienststelle.bremen.de

dienststellenleitung@dienststelle.bremen.de

it-stelle@dienststelle.bremen.de

haushalt@dienststelle.bremen.de

Adressatenkreis:

zuständige Fachstellen (ISB und Cyber Verantwortliche in den Dienststellen)

Bezug (Rechtsnorm):

EU:	NIS-2-Richtlinie, Cyber Resilience Act (CRA), Cybersecurity Act (CSA), Critical Entities Resilience (CER) Directive), etc.
D:	BSI-Gesetz (BSIG), IT-Sicherheitsgesetz, NIS2-Umsetzungsgesetz (NIS2UmsuCG), KRITIS-Dachgesetz, etc.
FHB:	Informationssicherheitsleitlinie der Freien Hansestadt Bremen (IS-LL), Verwaltungsvorschrift zur Umsetzung der EU-NIS-2-Richtlinie („VV NIS2Ums FHB“)

Die Anforderungen an Informations- und Cybersicherheit in der öffentlichen Verwaltung nehmen deutlich zu. Für die Dienststellen der Freien Hansestadt Bremen bedeutet dies

nicht nur, geeignete technische und organisatorische Maßnahmen umzusetzen, sondern diese auch nachvollziehbar, einheitlich und prüffähig zu dokumentieren. Hintergrund sind sowohl europäische und nationale Regelungen (insbesondere NIS-2-Richtlinie) als auch landesspezifische Vorgaben der Freien Hansestadt Bremen.

Die Gewährleistung eines angemessenen Niveaus an Informations- und Cybersicherheit in der öffentlichen Verwaltung der Freien Hansestadt Bremen ergibt sich verbindlich aus europäischen, nationalen sowie landesspezifischen Vorgaben. Neben der Umsetzung geeigneter technischer und organisatorischer Maßnahmen ist insbesondere die nachvollziehbare, revisionssichere Dokumentation der Compliance sicherzustellen.

Die Einführung des neuen dNetz Dataport, der vollständigen Integration von Sprach- und Datenkommunikation, sowie die fortschreitende Digitalisierung und Vernetzung von Fachverfahren erzeugen einen erheblich wachsenden Anspruch an Steuerung, Transparenz und Nachweisfähigkeit der Informationssicherheitsmaßnahmen.

Zur besseren Einordnung richtet sich dieses Rundschreiben sowohl an die Dienststellenleitungen als auch an die jeweils zuständigen Fachstellen (insbesondere IT, Organisation, Datenschutz/Informationssicherheit, Fachreferate mit Fachanwendungen).

Die Dienststellenleitung trägt die Gesamtverantwortung dafür, dass ein angemessenes Sicherheitsniveau hergestellt, aufrechterhalten und nachweisbar dokumentiert wird. Die Fachstellen unterstützen hierbei operativ durch Umsetzung, Fortschreibung und Dokumentation der erforderlichen Maßnahmen (z. B. Schutzbedarfsfeststellungen, Risikobewertungen, ISMS-Dokumentation und Nachweisführung).

Sofern Leistungen von Dataport genutzt werden, entbindet dies nicht von der Verantwortung der Dienststelle, insbesondere dort, wo organisatorische, fachliche oder bauliche Rahmenbedingungen (z. B. physischer Schutz, Eigenbetrieb von IT-Komponenten oder Sonderlösungen) außerhalb des Leistungsumfangs von Dataport liegen.

Folgende Aspekte sind verbindlich zu berücksichtigen:

1. Umsetzung der BSI-Grundschutzstandards
Die Anforderungen des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bilden den maßgeblichen Referenzrahmen für ein angemessenes Sicherheitsniveau (grundschutzkonformer Betrieb). Dies umfasst insbesondere:

- die Durchführung und Fortschreibung von Schutzbedarfsfeststellungen,
- die Modellierung nach IT-Grundschutz,

- die Umsetzung geeigneter Basis-, Standard- und ggf. erhöhter Sicherheitsmaßnahmen,
- sowie eine strukturierte Risikoanalyse bei erhöhtem Schutzbedarf.

Die Umsetzung ist prüffähig zu dokumentieren und regelmäßig zu evaluieren.

2. Konforme CISIS12- oder 27001-Zertifizierung
Dienststellen, die z. B. nach CISIS12 oder ISO 27001 zertifiziert sind oder eine Zertifizierung anstreben, haben sicherzustellen, dass Anforderungen des Standards vollständig umgesetzt, regelmäßig überprüft und dokumentiert werden. Die kontinuierliche Weiterentwicklung des Informationssicherheitsmanagementsystems (ISMS) ist verpflichtend. Abweichungen sind systematisch zu erfassen, zu bewerten und zu behandeln.

3. Grundschutzkonformer Betrieb der Clients im Full Management von Dataport
Für Clients, die im Full Management Service von Dataport (BASIS.bremen) betrieben werden, ist ein grundschutzkonformer Betrieb sichergestellt. Dies gilt hier auch für die zur Verfügung gestellten Netzwerkanbindungen. Dies beinhaltet insbesondere:

- die Einhaltung zentral vorgegebener Sicherheitskonfigurationen,
- ein geregeltes Patch- und Schwachstellenmanagement,
- die Absicherung von Authentifizierungs- und Berechtigungsstrukturen,
- sowie die Integration in zentrale Monitoring- und Incident-Management-Prozesse.

Fachliche oder organisatorische Abweichungen vom definierten Sicherheitsstandard sind zu begründen, zu dokumentieren und durch geeignete Kompensationsmaßnahmen abzusichern. Dies gilt insbesondere für den physischen Perimeterschutz oder auch selbstbetriebene IT-Infrastrukturen, für die Dataport grundsätzlich nicht zuständig ist und die insoweit ohne Begründung nicht grundschutzkonform betrieben werden.

4. Systematische Compliance-Kontrolle
Alle Organisationseinheiten sind verpflichtet, Verfahren zur kontinuierlichen Überwachung und Dokumentation der Einhaltung europäischer Vorgaben (z. B. NIS-2-Richtlinie, sofern betroffen), bundesrechtlicher Anforderungen sowie bremischer Regelungen zu etablieren oder fortzuschreiben. Die Dokumentation muss geeignet sein, internen wie externen Prüfungen standzuhalten.

Die Einhaltung der genannten Anforderungen ist durch die Dienststellen fortlaufend sicherzustellen und prüffähig zu dokumentieren. Ziel ist ein einheitliches, angemessenes und revisionssicher nachweisbares Sicherheitsniveau innerhalb der gesamten bremischen Verwaltung, insbesondere im Kontext zentraler Infrastrukturen und gemeinsamer IT-Dienstleistungen.

Kontakt

Der Senator für Finanzen

Rudolf-Hilferding-Platz 1

28195 Bremen

E-Mail: Informationssicherheit-FHB@finanzen.bremen.de