

Vorbemerkung

Aus Gründen der besseren Lesbarkeit wird in der Informationssicherheitsleitlinie nur eine Geschlechterform gewählt. Sie gilt grundsätzlich in gleicher Weise auch für das jeweils andere Geschlecht.

Präambel

Der AZV Südholstein ist zur effizienten Erfüllung seiner Aufgaben darauf angewiesen, dass die Informationsverarbeitung, besonders in der Automatisierungs- und Informationstechnik sicher und zuverlässig funktioniert. Vor dem Hintergrund der Cyber-Bedrohungslage und der damit verbundenen Risiken sowie den gesetzlichen Anforderungen ist ein angemessenes Informationssicherheitsniveau nachhaltig zu gewährleisten.

Der AZV Südholstein versteht Informationssicherheit als gemeinsame Aufgabe aller Führungskräfte und Mitarbeiter. Die Verbandsvorsteherin bekennt sich mit der vorliegenden Informationssicherheitsleitlinie zu ihrer Gesamtverantwortung für die Informationssicherheit und den Datenschutz und steht in vollem Umfang hinter den daraus abgeleiteten Konzepten und Maßnahmen. Die erforderlichen Personal-, Zeit- und Finanzressourcen werden bereitgestellt.

Die Geschäftsleitung verpflichtet sich zur Umsetzung der zu ergreifenden Risikomanagementmaßnahmen (z.B. aus dem BSIG) und die Umsetzung zu überwachen. Sie nimmt regelmäßig an Schulungen teil, um die Fähigkeit zum Erkennen und Bewerten von Risiken im Bereich der Informationssicherheit zu erlangen und die Auswirkungen auf den AZV beurteilen zu können. Sie ist sich bewusst, dass §38 BSIG eine persönliche Haftung bei schuldhafter Pflichtverletzung vorsieht.

Die Regelungen dieser Informationssicherheitsleitlinie basieren auf der ISO-Norm 27001 sowie dem IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Geltungsbereich

Die Informationssicherheitsleitlinie gilt für den gesamten Tätigkeitsbereich des AZV Südholstein. Dazu gehören die Kern- Führungs- und unterstützenden Prozesse sowie alle Anlagen an allen vom AZV Südholstein betreuten Standorten (Hetlingen, Glückstadt, Helgoland, Lentförden, Langeln, Groß Offenseth-Aspern und Krempe sowie alle zugehörigen Kanalnetze und Außenstellen).

Aufgrund der Stellung des AZV Südholstein als Betreiber Kritischer Infrastrukturen (nach IT-Sicherheitsgesetz) gilt die Informationssicherheitsleitlinie neben dem Automatisierungsnetzwerk, also das PLS-, SPS- und FWT-Netzwerk, auch für das Verwaltungsnetzwerk.

Die Informationssicherheitsleitlinie ist für jeden, der bei oder für den AZV Südholstein arbeitet, bindend. Ihre Einhaltung wird überprüft.

Die Nutzung von Cloud-Diensten, KI-Systemen und mobilen Endgeräten wird durch spezifische Sicherheitsrichtlinien geregelt.

Ziele

Für die Automatisierungs- und Informationstechnik sind die Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität nach dem Stand der Technik zu erreichen. Die notwendigen Sicherheitsmaßnahmen sind auch dann anzuwenden, wenn sich daraus Beeinträchtigungen ergeben.

Sicherheitsstrategie

Die Informationssicherheitsleitlinie schafft die Grundlage für den Aufbau eines Informationssicherheitsmanagementsystems (ISMS), das die Herstellung und den Erhalt eines angemessenen Informationssicherheitsniveaus beim AZV Südholstein sicherstellt. Das ISMS wird in das vorhandene Integrierte Managementsystem eingebunden und beinhaltet Aufbauorganisation, Ablauforganisation (Prozesse) und Regelwerk, die geeignet sind, Planung, Umsetzung und regelmäßige Überprüfung sowie Weiterentwicklung der Informationssicherheitsmaßnahmen zu gewährleisten.

Als zentrale Sicherheitsinstanz ernennt die Verbandsvorsteherin einen Informationssicherheitsbeauftragten, der für alle Belange und Fragen der Informationssicherheit zuständig ist. Er ist der Verbandsvorsteherin in dieser Rolle direkt unterstellt und berichtet ihr unmittelbar. Ein Austausch mit der Leitung der Automatisierungs- und Informationstechnik findet regelmäßig statt.

Dem Informationssicherheitsbeauftragten werden erforderliche Ressourcen bereitgestellt. Ihm werden geeignete Qualifizierungsmaßnahmen ermöglicht, um seine Aufgaben zeitlich und fachlich zu erfüllen.

Der Informationssicherheitsbeauftragte ist bei allen organisatorisch-technischen Neuerungen oder Änderungen, die Auswirkungen auf die Informationssicherheit haben können, durch die Verfahrensverantwortlichen frühzeitig einzubinden.

Bei Gefahr im Verzug ist der Informationssicherheitsbeauftragte oder sein Stellvertreter berechtigt, erforderliche Sicherheitsmaßnahmen auch kurzfristig umzusetzen oder anzuordnen. Das kann bis zur vorübergehenden Sperrung von Anwendungen oder Netzübergängen führen.

Maßnahmen

Die Sicherheitsmaßnahmen orientieren sich am IT-Grundschutz-Kompendium des BSI und setzen den im IT-Sicherheitsgesetz geforderten Stand der Technik um.

Die Informationssicherheitsleitlinie wird jährlich überprüft und an neue Bedrohungen, gesetzliche Anforderungen und technologische Entwicklungen angepasst; dabei werden die ausgewählten Maßnahmen auf Wirksamkeit und Angemessenheit überprüft und kontinuierlich weiterentwickelt.

Der Zugriff auf IT-Systeme, -Verfahren und Daten ist auf den unbedingt erforderlichen Personenkreis zu beschränken (Least Privilege-Prinzip). Jeder Mitarbeiter erhält nur diejenigen Zugriffsberechtigungen, die zur Erfüllung der dienstlichen Aufgaben erforderlich sind (Need-To-Know-Prinzip).

Informationen, die nach den Vorschriften des Informationszugangsgesetzes (IZG-SH), den in § 3 IZG-SH genannten Personen zugänglich zu machen sind, können allen Beschäftigten des AZV Südholstein zugänglich gemacht werden.

Mitarbeiter werden regelmäßig und bedarfsgerecht für die Belange der Informationssicherheit sensibilisiert und geschult. Näheres regelt das zentrale Schulungskonzept des AZV Südholstein.

Allen Personen, die bei oder für den AZV Südholstein tätig sind, wird die Informationssicherheitsleitlinie bekannt gegeben. Sie sind verpflichtet, die Informationssicherheit durch verantwortliches Handeln sicherzustellen und dabei die relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Regelungen zu beachten.

Sicherheitsanforderungen an Lieferanten und Dienstleister werden vertraglich festgelegt und stichprobenartig überprüft.

Sicherheitsrelevante Ereignisse und Schwachstellen sind dem IT-Helpdesk bzw. der A&I-Bereitschaft umgehend zu melden.

Verstöße gegen die Informationssicherheitsleitlinie sowie gegen sonstige verbindliche Regelungen der Informationssicherheit und der IT/OT-Nutzung können, abhängig von Art und Schwere des Verstoßes sowie unter Beachtung der geltenden arbeitsrechtlichen Bestimmungen, arbeitsrechtliche Maßnahmen bis hin zu disziplinarischen Konsequenzen nach sich ziehen.

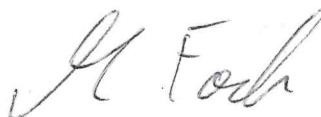
Inkraftsetzung

Die Verbandsvorsteherin setzt die Informationssicherheitsleitlinie zum 05.08.2026 in Kraft und ersetzt damit die am 01.03.2020 in Kraft gesetzte Informationssicherheitsleitlinie.

Hetlingen, den 05.08.2026



Christine Mesek
Verbandsvorsteherin



Malte Fock
Informationssicherheitsbeauftragter