

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

## 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 sowie alle zugehörigen Kanalnetze und Außenstellen).

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

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

## 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 ausgewählten Informationssicherheitsmaßnahmen werden regelmäßig auf Wirksamkeit und Angemessenheit überprüft und ständig 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.

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

## Inkraftsetzung

Die Verbandsvorsteherin setzt die Informationssicherheitsleitlinie zum 01.03.2020 in Kraft und ersetzt damit die am 01.04.2018 in Kraft gesetzte Informationssicherheitsleitlinie.

Hetlingen, den 28.02.2020



Christine Mesek  
Verbandsvorsteherin



Malte Fock  
Informationssicherheitsbeauftragter