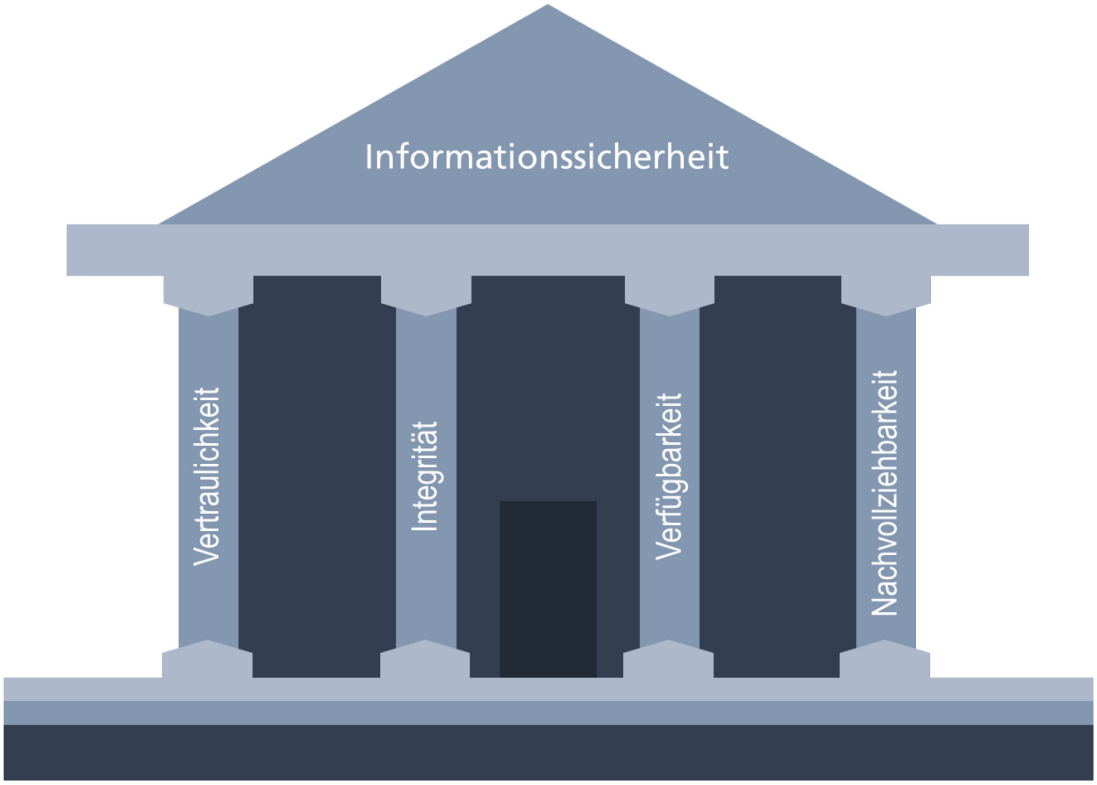
KANTON solothurn



Konzept Informationssicherheit der kantonalen Verwaltung

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

1.1 Zweck

Das Informationssicherheitskonzept soll:

- Aufzeigen, welche Aufgaben zur Sicherstellung der Informationssicherheit erfüllt werden müssen;
- Die Aufgaben, Kompetenzen und Verantwortlichkeiten für die auszuführenden Aufgaben definieren;
- Die Basis für den Aufbau und Betrieb eines Informationssicherheitsmanagementsystems bieten.

1.2 Geltungsbereich und Abgrenzung

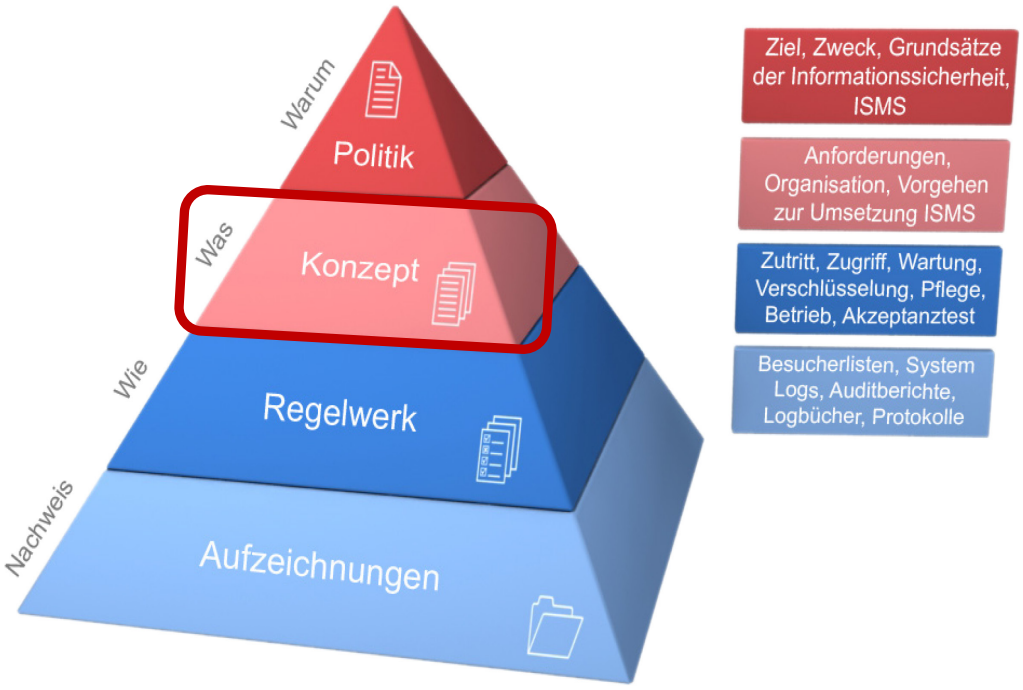
Der Geltungsbereich dieses Konzepts entspricht demjenigen der IKT-Strategie.

Bei der Zusammenarbeit mit Dritten (Kunden, Partner, Dienstleistungsunternehmen, Lieferanten etc.) müssen die zur Informationssicherheit definierten Sicherheitsstandards so weit als möglich vertraglich eingebunden werden.

2 Ziele und Anforderungen Informationssicherheitskonzept

Das vorliegende Konzept dient als Grundlage für ein einheitliches Sicherheitsmanagement innerhalb der kantonalen Verwaltung. Ziel ist es, ein unternehmensweites Informationssicherheitsmanagementsystem, ein einheitliches Vorgehen und einen umfassenden Sicherheitsstandard im Bereich der Informationssicherheit etablieren und unterhalten zu können. Informationssicherheit soll die Sicherheit und den Schutz aller Daten, elektronischer Informationen und der zu ihrer Bearbeitung benötigten Systeme, Prozesse und Infrastruktur für den Geschäftsbetrieb der kantonalen Verwaltung gewährleisten.

Das Informationssicherheitskonzept beschreibt, welche Tätigkeiten durchgeführt werden müssen, um die Anforderungen an die Informationssicherheit gewährleisten zu können. Das Konzept zeigt, was zur Einhaltung dieser notwendig ist.



3 Gesetzliche, vertragliche und interne Anforderungen

Bei der Informationsverarbeitung, beim Einsatz von IT-Systemen sowie beim Anbieten von Dienstleistungen und Produkten, gewährleistet die kantonale Verwaltung die Einhaltung der gesetzlichen, vertraglichen und internen Bestimmungen und Vereinbarungen.

Bei der elektronischen Bearbeitung von Informationen und der Benutzung von IT-Systemen werden insbesondere folgende Gesetze und Vereinbarungen beachtet:

- Informations- und Datenschutzgesetz (InfoDG)
- Informations- und Datenschutzverordnung (InfoDV)

Weitere rechtliche Vorgaben haben ebenfalls Gültigkeit. In Bezug auf die Zusammenarbeit mit Dritten werden die geltenden IT-Sicherheitsbestimmungen der kantonalen Verwaltung entsprechend dem Vertragsverhältnis vertraglich eingebunden.

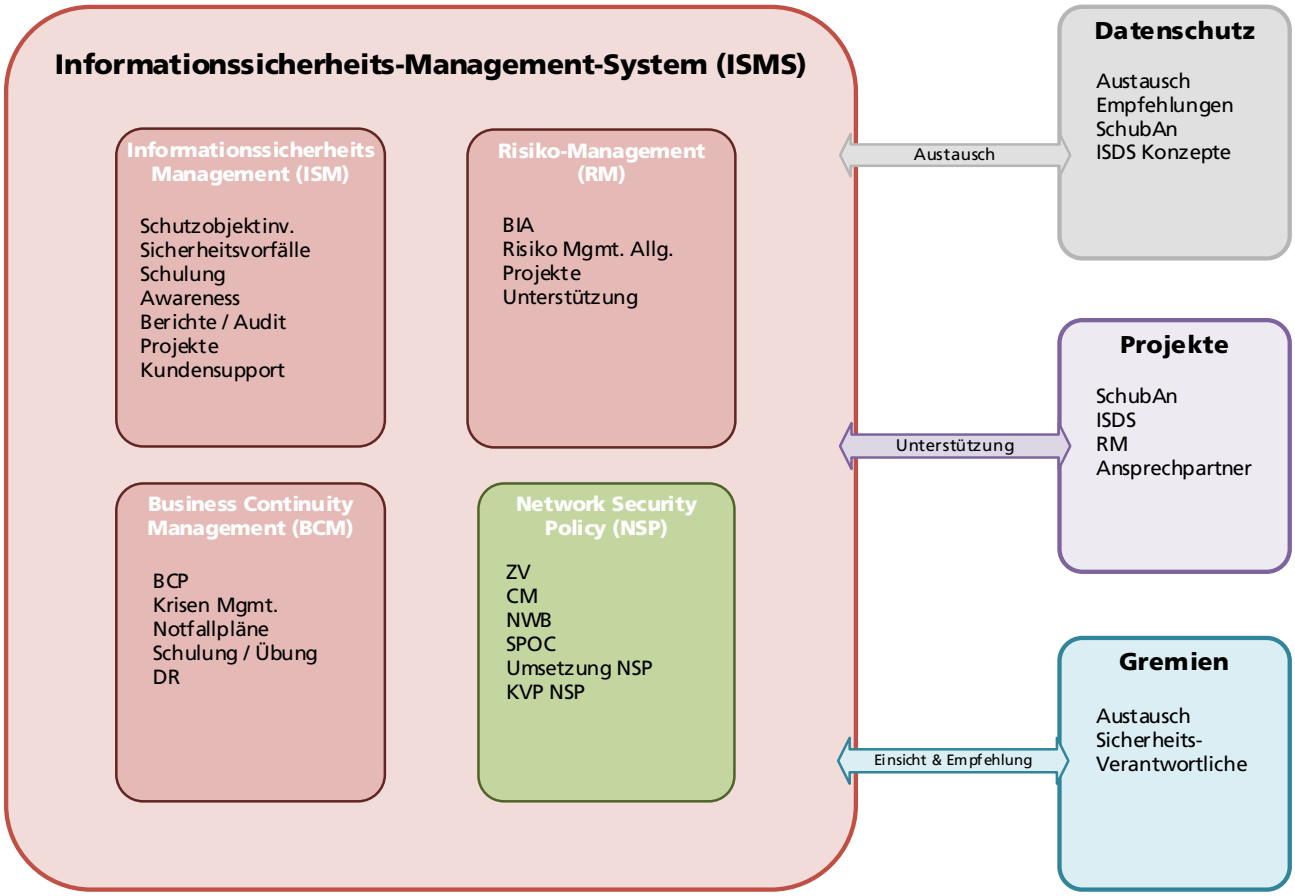
4 Organisation

4.1 Allgemein

Zum Aufbau und Betrieb eines Informationssicherheitsmanagementsystems (ISMS) muss die Organisation entsprechend den zugrundliegenden Normen angepasst werden. Alle Dienststellen sind verantwortlich für ihre Daten und Informationen und müssen bei der Erfüllung der Sicherheitsanforderungen mitarbeiten.

4.2 Bereiche und Verantwortlichkeiten

Die Sicherheit der Informationen wird mit den nachfolgenden Bereichen koordiniert, gesteuert und überwacht. Als integriertes Managementsystem werden die einzelnen Bereiche als einheitliches System betrachtet und sind nach Aufgabenbereich miteinander verbunden.



Information Security Management (ISM)

Der Bereich Information Security Management bearbeitet ein breites Gebiet von Aufgaben, welches Kontrollen, Bewusstsein, Audits etc. beinhaltet. In Kapitel 5 werden die einzelnen Aufgaben detailliert beschrieben.

Hauptverantwortlich für das ISM ist der Stabsbereich Informationssicherheit im AIO.

Risikomanagement (RM)

Risikomanagement ist ein zentraler Bestandteil, welcher übergeordnet in allen Bereichen (Betrieb, Projekte etc.) angewendet wird. Risiken und Massnahmen werden zentral verwaltet und kontinuierlich geprüft. Jede Dienststelle ist für das Risikomanagement in ihren Bereichen selber verantwortlich.

Business Continuity Management (BCM)

Business Continuity Management dient der Sicherstellung der Verfügbarkeit von geschäftskritischen Prozessen, den entsprechenden Rollen und Verantwortlichkeiten. Es beinhaltet Pläne zum Vorgehen nach Eintritt eines Vorfalles. Im Bereich der Informatik ist die Stabsstelle Informationssicherheit verantwortlich für BCM. Für das Continuity Management der Prozesse der jeweiligen Dienststellen sind die Informationssicherheitsverantwortlichen der Dienststellen verantwortlich. BCM ist in Kapitel 5.3 beschrieben und definiert.

Network Security Policy (NSP)

Der Network Security Officer des AIO hat die technische Sicherheitsverantwortung. Umsetzungen und Konzeptionen im technischen Netzwerkbereich sowie die Einhaltung der NSP sind die wichtigsten Aufgaben. Eine enge Zusammenarbeit mit den Bereichen ISM und RM ist dabei zwingend.

Datenschutz

Die Zusammenarbeit mit der kantonalen Information- und Datenschutzstelle ist sehr wichtig. Zur Überprüfung eines Schutzbedarfs ist die Vertraulichkeit in Bezug auf Personendaten mit den Datenschutzverantwortlichen abzugleichen. Ebenso werden ISDS Konzepte und Datensammlungen an die Information- und Datenschutzstelle weitergegeben, um Empfehlungen einzuholen.

Projekte

Die Einhaltung der Informationssicherheit in Projekten ist wichtig. Hilfe bei Schutzbedarfsanalysen, ISDS Konzepten und Risikoanalysen sind dabei die Hauptaufgaben innerhalb der Projekte. Die in Konzepten definierten ISDS Massnahmen müssen nach Abschluss des Projektes in den Betrieb überführt und kontinuierlich überprüft werden.

Gremien

Im neu zu schaffenden Gremium Informationssicherheit werden alle Informationssicherheitsverantwortliche teilnehmen können. Die Aufgabe des Gremiums besteht im Wesentlichen darin, aktuelle und zielführende Informationen an die entsprechenden Stellen weiterzuleiten und Optimierungen im Bereich Informationssicherheit zu definieren.

4.3 Organisation Dienststellen

Prozesse und Zuständigkeiten im Bereich der Informationssicherheit werden klar definiert und koordiniert, Handlungsanweisungen eindeutig formuliert. Die nachfolgend aufgeführten Funktionen geben einen Einblick in die Aufgaben rund um das ISMS.

Pflichten und Kompetenzen der einzelnen Funktionen und Gremien innerhalb der kantonalen Verwaltung werden voneinander abgegrenzt. Zwischen den verschiedenen Funktionsträgern wird eine enge Zusammenarbeit und ein intensiver Erfahrungs- und Gedankenaustausch angestrebt.

4.3.1 Leitung Dienststelle:

- trägt die oberste Verantwortung für die Informationssicherheit in ihrem Bereich;
- initialisiert und genehmigt die erforderlichen Richtlinien und Standards;
- bestimmt und stellt Ressourcen für die Informationssicherheit bereit;
- beurteilt die Sicherheits- und Bedrohungslage und initialisiert allfällige Reaktionen anhand von Risikomeldungen bzw. im Rahmen des Risikobehandlungsplans;
- beauftragt die interne oder externe Revision, um einzelne Sicherheitsbereiche auditieren zu lassen;
- entscheidet bezüglich Risikoübernahmen.

4.3.2 Informationssicherheitsverantwortliche der Dienststellen (ISV):

Die Informationssicherheitsverantwortlichen der Dienststellen erfüllen folgende Anforderungen:

Aufgaben	• Führt ein Register der Datensammlungen und der verantwortlichen Personen innerhalb seines Bereichs • Begleitet Projekte in seinem Bereich in der Rolle als Informationssicherheits- und Datenschutzverantwortlicher • Erstellt Schutzbedarfsanalysen, Risikoanalysen und ISDS-Konzepte • Instruiert und Berät die Mitarbeitenden im Bereich des Datenschutzes • Ist Ansprechperson für ISDS-Themen innerhalb seines Bereiches • Ist Ansprechpartner für die Abteilung ISM im AIO und für die kantonale Datenschutzstelle für ISDS-Themen des Amtes • Meldet Sicherheitsvorfälle / Datenschutzverletzungen innerhalb seines Bereiches an die Stelle Informationssicherheit im AIO
Kompetenzen	• Ist berechtigt, den Schutzbedarf von Schutzobjekten einzustufen • Ist berechtigt, Risiken einzuschätzen und zu bewerten • Ist berechtigt, Sicherheitsvorfälle zu beurteilen und zu melden • Ist berechtigt, Empfehlungen abzugeben • Ist berechtigt, Anträge zu stellen
Verantwortung	• Verantwortlich für die nachweisliche Einhaltung des Datenschutzes • Verantwortlich für die Führung des Registers der Datensammlungen in seinem Bereich • Verantwortlich für die Koordination von Informationssicherheit und Datenschutz • Verantwortlich für die Berichterstattung (Data Owner, ISB, Gremien)

4.4 Organisation AIO

Um die Anforderungen an die Informationssicherheit zu erfüllen, wurde im AIO der Bereich Informationssicherheit und QS als eine unabhängige Stelle (Stabsstelle) in der Organisation neu eingeführt.
Dieser Bereich der Informationssicherheit und QS ist verantwortlich für die Informationssicherheit mit allen Bereichen (ISM, RA, BCM), sowie hauptverantwortlich für die Umsetzung der Netzwerksicherheit (NSP).

Folgendes Profil erfüllen die Mitarbeitenden:

4.4.1 Informationssicherheitsbeauftragte/r (ISB) / Information Security Officer (ISO):

Aufgaben	• Stimmt die Informationssicherheitsziele mit den Zielen der Organisation ab • Erstellt die Leitlinie zur Informationssicherheit und stimmt diese mit der Führungsebene ab • Erstellt das Informationssicherheitskonzept und passt dieses an neue Gegebenheiten an • Erstellt Richtlinien und Regelungen im Bereich Informationssicherheit • Plant und konzipiert die Notfallvorsorge (BCM) • Übernimmt die Leitung der Analyse und Nachbearbeitung von Informationssicherheitsvorfällen • Organisiert und plant Audits und Kontrollen im Informationssicherheitsbereich
Kompetenzen	• Ist berechtigt, Empfehlungen auf allen Ebenen im Bereich Informationssicherheit abzugeben • Ist berechtigt, Anträge an die IGV sowie an die Dienststellen der Verwaltung zu stellen • Ist berechtigt, Audits und Kontrollen in Dienststellen durchzuführen • Ist berechtigt, Aufgaben an die ISV zu delegieren und Aufträge an diese zu vergeben
Verantwortung	• Verantwortlich für den Aufbau, Betrieb und die Weiterentwicklung der Informationssicherheitsorganisation innerhalb der Organisation • Verantwortlich dafür, dass der notwendige Informationsfluss für das Informationssicherheitsmanagement sichergestellt ist • Verantwortlich für die Awareness und Schulungsmassnahmen für die Informationssicherheit • Verantwortlich für den Aufbau und Betrieb des ISMS der Organisation

4.4.2 Network Security Officer (NSO):

Aufgaben	• Beurteilt Change Requests im Bereich der Netzwerksicherheit und führt solche selbstständig durch • Anforderungs- und Risikoanalyse, Konzepterstellung und Systemarchitektur-Design im Netzwerksicherheitsbereich • Erarbeitet und plant Massnahmen zur Einhaltung der geforderten Netzwerksicherheit • Analysiert die Auswirkungen der umgesetzten Massnahmen und erarbeitet falls nötig Verbesserungen • Ist Mitglied in Gremien im Bereich der Informations- und Netzwerksicherheit • Hilft mit bei der Erstellung von Business Continuity Planungen und beim Erstellen von Richtlinien
Kompetenzen	• Ist berechtigt, Firewallpolicies und deren Änderungen zu genehmigen oder abzulehnen • Ist berechtigt, Sicherheitsstörungen und Notfälle an die Amtsleitung zu eskalieren • Ist berechtigt, nötige Sanktionen bei Zuwiderhandlungen gegenüber den gesetzten Vorgaben im Bereich Netzwerksicherheit zu ergreifen • Ist berechtigt, die im ISMS definierten Massnahmen im Bereich Netzwerk durchzusetzen
Verantwortung	• Definierung und Einhaltung von Netzwerksicherheitsvorgaben und Richtlinien • Schafft und fördert das Bewusstsein für die geforderte Netzwerksicherheit nach innen und aussen • Ist verantwortlich für die Einhaltung der geforderten Netzwerksicherheit aus den bestehenden Vorgaben und Richtlinien mit allen Teilaspekten • Verantwortlich für die Erstellung und Einhaltung von Vorgaben aus den Bereichen SIK und NSP

5 Aufbau und Betrieb des ISMS

5.1 Information Security Management

5.1.1 ISMS Anwendungsbereich

Der Anwendungsbereich des ISMS bestimmt und definiert die Informationen, welche geschützt werden müssen.
Es müssen interne und externe Themen, die interessierten Parteien und ihre Anforderungen, sowie Schnittstellen und Abhängigkeiten für Schutzobjekte berücksichtigt werden. Nicht kritische Informationen, welche keinen Schutzbedarf haben, werden nicht in den Anwendungsbereich aufgenommen. Der Anwendungsbereich der Informationssicherheit wird in Zusammenarbeit mit allen Informationssicherheitsverantwortlichen aller Dienststellen sowie mit den kantonalen Datenschutzbeauftragten koordiniert. Die Hauptverantwortung und somit der Lead zur Definierung des Anwendungsbereiches liegt beim Bereich Informationssicherheit des AIO.

5.1.2 Schutzobjektinventar

Damit definiert werden kann, in welchem Umfang und in welcher Tiefe die Massnahmen des ISMS durchgeführt werden, wird ein Schutzobjektinventar erstellt.
Darin ist aufgeführt, welche Schutzobjekte (Assets) bei welchen Dienststellen innerhalb des definierten Anwendungsbereiches vorhanden sind. Als Schutzobjekte gelten Informationen, Räume, Personen sowie Informatikmittel. Das Schutzobjektinventar kann sich aus anderen, bereits vorhandenen Inventaren zusammensetzen. Das AIO pflegt diese Inventare; die jeweiligen Dienststellen müssen jedoch eine Übersicht der vorhandenen Schutzobjekte haben und helfen, diese zu pflegen und aktuell zu halten.

5.1.3 Festlegung des Schutzbedarfs

Für alle Schutzobjekte wird der jeweilige Schutzbedarf mittels Schutzbedarfsanalyse bestimmt (Bedarf an Verfügbarkeit, Vertraulichkeit sowie Integrität).
Verantwortlich für die Erstellung der Schutzbedarfsanalysen sind die Informationssicherheitsverantwortlichen der Dienststellen mit (falls nötig) Unterstützung des Bereichs Informationssicherheit im AIO.
Die bereits vorhandenen Schutzbedarfsanalysen müssen überprüft und wenn nötig aktualisiert werden. Die Schutzbedarfsanalysen werden nach deren Erstellung zur weiteren Prüfung an die kantonale Datenschutzstelle eingereicht. Die Datenschutzverantwortlichen können Empfehlungen zur Einstufung, vor allem im Bereich Vertraulichkeit, abgeben.
Die Schutzbedarfsanalysen werden im AIO durch den Bereich Informationssicherheit verwaltet und aufbewahrt.

5.1.4 Reglemente und Richtlinien

Gesetzliche Vorgaben

Gesetze und Verordnungen gelten als übergeordnete Vorgaben für die Erstellung von Reglementen, Richtlinien und Weisungen. Verantwortlich für die Einhaltung der gesetzlichen Vorgaben ist jede Dienstelle in ihren Bereichen.

Organisatorischer Schutz

Organisatorische Reglemente und Richtlinien müssen geprüft und wo nötig erstellt werden. Als Grundlage dazu dient der IKT-Grundschutz. Verantwortlich für Reglemente und Richtlinien im Umgang mit Informatikmitteln mit Bezug auf den Informationssicherheitsbereich ist die Stelle Informationssicherheit des AIO.

Technischer Schutz

Vorgaben und Konzepte werden erstellt, damit für den IKT-Grundschutz sowie bei Audits und Sicherheitsvorfällen klar ist, wann was zu tun ist und wo was zu finden ist. Die Verantwortung des technischen Schutzes innerhalb von Anwendungen liegt bei den jeweiligen Dienststellen, welche Anwendungsverantwortliche sind.
Infrastruktur-Systeme der Informatik sind für die Informationssicherheitsthemen des AIO verantwortlich.

Physischer Schutz

Um den physischen Schutz der Schutzobjekte zu gewährleisten und zu dokumentieren, müssen entsprechende Konzepte und Reglemente vorhanden sein. Das Hochbauamt des Kantons Solothurn hat die Hauptverantwortung für gebäudetechnische Themen. Die nötige Sicherheit der Gebäude und Räume wird durch die jeweiligen Informationssicherheitsverantwortlichen der Dienststellen, welche eine Räumlichkeit verwenden, definiert.

5.1.5 Audits und Prüfungen

Interne Audits

Interne Audits werden für alle Bereiche periodisch durchgeführt. Diese können interne Abläufe, technische Überprüfungen wie Backups, Firewall Logs etc. mit Bezug auf die Informationssicherheit betreffen. Die Audits werden von der Stelle Informationssicherheit geplant und durchgeführt. Dazu wird ein Auditplan erstellt. Die Informationssicherheitsverantwortlichen der Dienststellen gelten als Ansprechpartner für die Audits und können interne Überprüfungen für ihre Bereiche selbstständig ausführen.

Ebenfalls führt die kantonale Finanzkontrolle periodisch Audits durch, welche durch die Finanzkontrolle selber geplant werden.

Externe Audits

Externe Audits können nach Bedarf definiert und durchgeführt werden. Diese können durch berechtigte kantonale Stellen, mit den entsprechenden Kompetenzen (Regierungsrat, Gerichtsverwaltungskommission, Kantonale Finanzkontrolle, Informationssicherheit AIO) veranlasst werden.

Prüfungen

Massnahmen aus Risikoanalysen und ISDS-Konzepten, Pendenzen aus Security Boards oder die Einführung kritischer Security Patches müssen periodisch auf ihre Erfüllung geprüft werden. Verantwortlich dafür ist die Stelle Informationssicherheit des AIO sowie die Informationssicherheitsverantwortlichen der Dienststellen für ihre jeweiligen Bereiche.

5.1.6 Bewusstsein und Schulung (Awareness)

Awareness Kampagnen

Zur Förderung des Bewusstseins aller Mitarbeiter der kantonalen Verwaltung werden laufend Awareness Kampagnen und Sensibilisierungsmassnahmen durchgeführt. Diese können verschiedene Art, wie Mailings, Infoblätter, Newsletter, Intranet Meldungen, Schulungen etc., sein.

Die Verantwortung der Awareness liegt bei der Informationssicherheitsstelle des AIO. Die Förderung der Awareness wird in Zusammenarbeit mit der kantonalen Datenschutzstelle behandelt, welche im Bereich Datenschutz selber auch Massnahmen durchführt.

Informationen

Informationen betreffend Informationssicherheit für die Mitarbeitenden werden nach Bedarf über verschiedene Wege verteilt. Wichtig dabei sind auch die Informationssicherheitsverantwortlichen der Dienststellen, welche als Ansprechpartner der Informationssicherheitsstelle des AIO, Informationen erhalten und weitergeben müssen.

Schulungen

Schulungen werden nach Bedarf durchgeführt. Wo und wie muss spezifisch je nach Fall definiert werden.

Diese können je nach Anforderungen von den Informationssicherheitsverantwortlichen oder von Externen durchgeführt werden.

5.1.7 IKT-Grundschutz und Umgang mit Ausnahmen

Der IKT Grundschutz beinhaltet den Standardschutz mit Massnahmen, welche zur Einhaltung der Anforderungen an die Informationssicherheit dienen. Sind keine erhöhten Anforderungen an den Schutzbedarf von Schutzobjekten vorhanden, reicht der Grundschutz aus und es müssen keine zusätzlichen Massnahmen definiert werden. Der Grundschutz wird periodisch überprüft und wenn nötig aktualisiert.
Es können Ausnahmen definiert werden, bei welchen die Grundschutzmassnahmen nicht durchgeführt werden. Diese sind zu begründen, schriftlich festzuhalten und periodisch zu überprüfen. Die Verantwortung für den Grundschutz liegt bei der Stelle Informationssicherheit des AIO, welche diesen definiert und verwaltet.

5.1.8 Informationssicherheit in Projekten

Der Prozess, wie die Informationssicherheit in Projekten gewährleistet wird, ist bereits im Leitfaden „Projektmanagement des AIO“ beschrieben.

Innerhalb der Projekte gibt es immer die Rolle des Informationssicherheits- und Datenschutzverantwortlichen (ISDSV) für das Projekt. Dieser ist zuständig für die Erstellung der Schutzbedarfsanalysen und der ISDS-Konzepte. Die Rolle des ISDSV übernimmt der Informationssicherheitsverantwortliche der jeweiligen Dienststelle. Wird Unterstützung benötigt, kann beim Informationssicherheitsbereich des AIO angefragt werden.

Wie bereits erwähnt, werden die Schutzbedarfsanalysen durch die Datenschutzverantwortlichen sowie durch den Bereich Informationssicherheit des AIO geprüft. Gleiches gilt auch für die ISDS-Konzepte.

Die Massnahmen aus den ISDS-Konzepten müssen auf deren Erfüllung überprüft werden, was im Verantwortungsbereich der Informationssicherheitsstelle des AIO liegt. Diese können dazu die Informationssicherheitsverantwortlichen der Departemente beiziehen.

Auch werden ISDS-Konzepte sowie auch Schutzbedarfsanalysen bei Änderungen von Schutzobjekten überprüft und wenn nötig angepasst. Auch dies ist im Verantwortungsbereich der Informationssicherheitsstelle des AIO.

5.1.9 Datensammlungen

Jede Dienststelle ist für ihre Daten selber verantwortlich. Es ist wichtig, Datensammlungen zu erkennen und ein Inventar über diese zu führen. Jeder Informationssicherheitsverantwortliche ist verantwortlich dafür, die Datensammlungen in seinem Bereich zu führen und bei der kantonalen Datenschutzstelle zu melden.

5.1.10 Behandlung von Sicherheitsvorfällen

Definition und Identifikation eines Sicherheitsvorfalles

Sicherheitsvorfälle grenzen sich vom normalen Tagesgeschäft ab. Allen Mitarbeitern muss dabei klar sein, was die Definition eines Sicherheitsvorfalles ist.

Als Sicherheitsvorfall wird ein Ereignis bezeichnet, das die Vertraulichkeit, Verfügbarkeit und Integrität der definierten Schutzobjekte mit hohem oder sehr hohem Schutzbedarf derart beeinträchtigt, dass ein grosser Schaden für uns oder unsere Kunden und Geschäftspartner entstehen kann.

Nachfolgend einige Beispiele zum besseren Verständnis:

- Fehlkonfigurationen, die zur Offenlegung vertraulicher Daten, zum Verlust der Integrität schutzbedürftiger Daten oder zu Datenverlusten führen;
- Auftreten von Sicherheitslücken in Hard- oder Softwarekomponenten;
- (massenhaftes) Auftreten von Computer-Viren;
- kriminelle Handlungen (etwa Hacking von Internet-Servern, Einbruch, Diebstahl oder Erpressung mit IT-Bezug).

Meldung von Sicherheitsvorfällen

Sämtliche Mitarbeitenden der im Geltungsbereich definierten Dienststellen müssen wissen, wie und wo ein Sicherheitsvorfall gemeldet werden muss. Dies wird über Schulungen und Informationen sichergestellt.

Die Mitarbeiter sollen Sicherheitsvorfälle aller Art den Informationssicherheitsverantwortlichen der Dienststellen melden, welche diese als erstes beurteilen und an die Stelle Informationssicherheit des AIO weiterleiten.

Die Stelle Informationssicherheit des AIO verwaltet die Sicherheitsvorfälle und bearbeitet diese. Es wird über Sofortmassnahmen und die weitere Bearbeitung der Vorfälle entschieden und diese werden bis zu deren Abschluss weiterverfolgt.

Bearbeitung von Sicherheitsvorfällen

Je nach Schwere eines Vorfalls werden verschiedene Massnahmen getroffen. Diese werden von Fall zu Fall entschieden. Wichtig ist dabei, dass auch, nachdem ein Vorfall behoben wurde, rückwirkend geprüft wird, wie es dazu kommen konnte und mögliche Risiken und Schwachstellen erkannt und beurteilt werden. Ein Vorfall durchläuft immer die nachfolgenden Phasen:

- Eindämmung
- Beseitigung
- Wiederherstellung
- Erkenntnisse

Verantwortlichkeiten

Jeder Mitarbeiter ist verantwortlich, bei der Behebung von Vorfällen mitzuarbeiten, diese zu erkennen und den verantwortlichen Stellen zu melden.

Kommunikation

Sobald ein Vorfall eingetreten ist und gemeldet wurde, ist die Stelle Informationssicherheit des AIO hauptverantwortlich, diesen bis zur Behebung zu verfolgen und somit auch die entsprechenden Stellen zu informieren.

Prozess und Rollen

Ein Prozessablauf sowie die nötigen Rollen und Aufgaben werden in einer separaten Prozessbeschreibung detaillierter behandelt.

5.2 Risikomanagement

Mittels Risikoanalyse werden Risiken identifiziert, welche die Informationssicherheit der definierten Schutzobjekte gefährden.
Nachdem die Risiken identifiziert und bewertet wurden, wird der Umgang mit diesen bestimmt (Akzeptieren, Reduzieren, Vermeiden oder Teilen).
Die Risiken sowie die Umsetzung deren Massnahmen im Bereich Informationssicherheit müssen laufend geprüft und wenn nötig aktualisiert werden. Dazu muss ein Inventar der Risiken und deren Massnahmen mit Verantwortlichkeiten und Terminen geführt werden.

Jeder Bereich ist verantwortlich, ein Risikomanagement für sich selber zu pflegen und zu definieren.

5.3 Business Continuity Management (BCM)

5.3.1 Business Continuity Management Konzept

Business Continuity Management regelt den Umgang mit Ereignissen, die dazu führten, dass geschäftskritische Prozesse nicht mehr verfügbar sind. Es wird ein Konzept erstellt, welches beschreibt, wie der Aufbau und die Aufrechterhaltung des BCM sichergestellt werden.
Jede Dienststelle ist für ihren Teil des Business Continuity Management verantwortlich.
Die Stelle Informationssicherheit des AIO ist verantwortlich für das Verwalten des BCM hinsichtlich Informatik und Infrastruktur. Die Dienststellen sind verantwortlich für die BCM-Aufgaben bezüglich ihren Prozessen, Räumlichkeiten und Ressourcen.

5.3.2 Aufbau BCM

Der Aufbau eines BCM wird in 4 Bereiche gegliedert, welche den BCM-Kreislauf darstellen:

- Unternehmenssituation verstehen:
  - Business Impact Analyse (BIA)
  - Geschäftsziele und Verpflichtungen
  - Schutzobjektinventar

- BCM Strategie:
  - Beschreibt zu schützende Betriebsaktivitäten (Prozesse, Schutzobjekte etc.)
  - Beschreibt, wie die Verminderung von Auswirkungen gemacht wird
  - Reaktionen auf Auswirkungen

- BC-Pläne entwickeln und umsetzen:
  - Pläne, welche zeigen, wie in welchem Fall zu reagieren ist
  - Rollen
  - Ressourcen
  - Informations- und Dokumentationsfluss

- BCM testen und überprüfen:
  - Testen der Pläne
  - Erkenntnisse
  - Optimierung

Der detaillierte Aufbau und Betrieb des BCM wird in einem separaten Konzept detailliert beschrieben.

Definitionen, Akronyme und Abkürzungen

Begriff	Bedeutung
AIO	Amt für Informatik und Organisation
BC	Business Continuity
BCM	Business Continuity Management
BIA	Business Impact Analyse
DR	Desaster Recovery
DSV	Datenschutzverantwortliche
GVK	Gerichtsverwaltungskommission
IGV	Informatikgruppe Verwaltung
IKT	Informations- und Kommunikations-Technologie
ISDS	Informationssicherheit und Datenschutz
ISM	Information Security Management
ISMS	Information Security Management System
KFK	Kantonale Finanzkontrolle
NSP	Network Security Policy
SchubAn	Schutzbedarfsanalyse

Referenzen

Titel, Quelle
Informations- und Datenschutzgesetz (InfoDG)
Informations- und Datenschutzverordnung (InfoDV)
AIO IKT-Grundschutz Basisdokument
AGB ISDS (Allgemeine Geschäftsbedingungen ISDS Kanton Solothurn)
Informatikstrategie des Kantons Solothurn
Leitfaden Projektmanagement AIO
BSI 200-x Standard