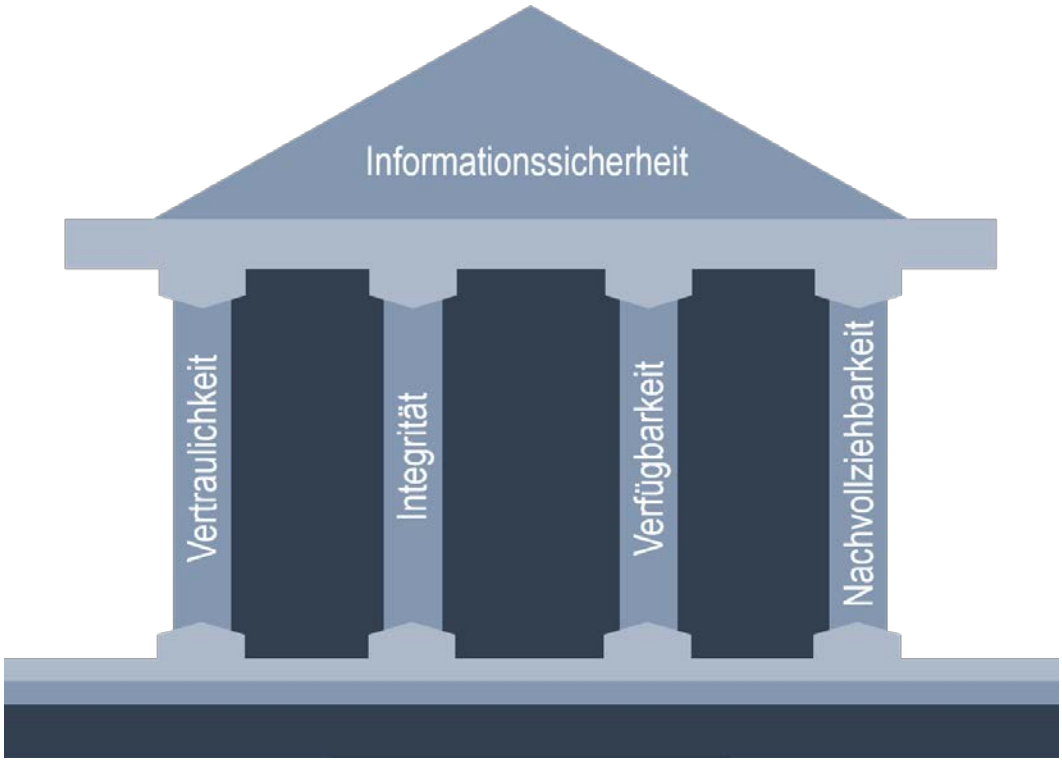

Leitlinie Informationssicherheit der kantonalen Verwaltung Solothurn V 1.0

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

1.1 Zweck

Die Leitlinie Informationssicherheit soll:

- der Informationssicherheit in der kantonalen Verwaltung Solothurn den entsprechenden Rahmen sowie die notwendigen Inhalte geben;
- die Datenbestände und (Fach-) Anwendungen der Leistungsbezüger sowie entsprechende Informatiksysteme des kantonalen Leistungserbringers AIO durch organisatorische und technische Massnahmen angemessen schützen.

1.2 Geltungsbereich

Der Geltungsbereich dieser Leitlinie ist in der kantonalen Informatikstrategie festgelegt.

2 Ziele der Informationssicherheit

2.1 Schutzziele

Die Einhaltung der Schutzziele (Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit) ist das zentrale Element der Informationssicherheit. Wichtig ist, dass die Informationen ihrem Schutzbedarf entsprechend:

- nur Berechtigten zugänglich sind (Vertraulichkeit);
- verfügbar sind, wenn sie benötigt werden (Verfügbarkeit);
- nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität);
- nachvollziehbar bearbeitet werden (Nachvollziehbarkeit).

2.2 Anforderungen

Zur Erfüllung der Anforderungen müssen folgende Punkte eingehalten werden:

- Die gesetzlichen Grundlagen und vertraglichen Anforderungen werden eingehalten.
- Die strategischen Zielsetzungen im Bereich der Informationssicherheit sind definiert, entsprechende Massnahmen umgesetzt und deren Wirksamkeit überprüft.
- Die Mitarbeitenden der kantonalen Verwaltung sind im erforderlichen Umfang sensibilisiert und sich ihrer Verantwortung im Umgang mit Informationen und in der Anwendung von IKT-Mitteln bewusst.
- Der Zugang zu Informationen erfolgt nur auf Basis definierter Aufgaben und entsprechender Funktionen und Rollen von Mitarbeitenden.
- Informationen werden bezüglich des notwendigen Schutzbedarfs periodisch durch die Verantwortungsträger beurteilt.
- Alle Daten und Informationen haben einen verantwortlichen Inhaber sowie einen definierten und dokumentierten Schutzbedarf.
- Technische und organisatorische Sicherheitsmassnahmen werden so gestaltet, dass diese ein integraler Bestandteil der Verwaltungsprozesse sind.

3 Steuerung der Informationssicherheit

3.1 Verantwortung

Verantwortlich für die Informationssicherheit und für die sichere Datenbearbeitung sind diejenigen Dienststellen, die Daten zur Erfüllung ihrer gesetzlichen Aufgaben bearbeiten oder durch Dritte bearbeiten lassen.

Verantwortlich für die Einhaltung und Umsetzung der Sicherheitsvorgaben und -ziele in ihrem Verantwortungsbereich sind alle Mitarbeitenden der Dienststellen. Sie sorgen für den Schutz der Informationen und stellen sicher, dass:

- die definierten Ziele erreicht werden;
- die definierten Sicherheitsmassnahmen im erforderlichen Umfang umgesetzt werden;
- die Informationssicherheit und der Datenschutz kontinuierlich verbessert wird;
- die Ziele regelmässig überprüft werden.

3.2 Organisation

Die Organisation (Rollen und Prozesse) ist definiert, dokumentiert sowie kommuniziert und wird periodisch überprüft. Die Verantwortlichkeiten der Leistungsbezüger und der Leistungserbringer sind definiert.

Für die Informationssicherheit betreibt das AIO ein Information Security Management System (ISMS), welches Standards, notwendige Verfahren, definierte Verantwortlichkeiten sowie ein stufengerechtes Reporting zur Unterstützung der Sicherheitsziele beinhaltet.

Eine übergreifende Zusammenarbeit mit Leistungspartnern, Kunden und Lieferanten im Bereich der Sicherheitsmassnahmen ist so zu positionieren, dass die Einhaltung der Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Daten und Services gewährleistet wird.

3.3 Bewusstsein und Schulung

Die kantonale Verwaltung fördert eine Kultur des sicheren Umgangs mit Informationen. Prävention und Eigenverantwortung bilden die zentralen Stützen der Sicherheitskultur. Die Mitarbeitenden werden regelmässig und rollengerecht bezüglich der für sie relevanten Sicherheitsmassnahmen informiert und geschult. Die fortwährende Sensibilisierung der Mitarbeitenden in sicherheitsrelevanten Themen muss gewährleistet sein.

3.4 Festlegung des Schutzbedarfs

Die Festlegung des Schutzbedarfs von Datenbeständen wie auch von (Fach-)Applikationen erfolgt mit Hilfe der Schutzbedarfsanalyse (SchubAn).
In dieser werden die betroffenen Daten und Systeme auf die Schutzziele geprüft.

3.5 Risikomanagement

Das Risikomanagement wird übergeordnet in allen Dienststellen durchgeführt.
Das Management der IKT- und Informationsrisiken identifiziert die Gefahren, welche die Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit von Informationen, IKT-Infrastrukturen und -Anwendungen bedrohen. Die damit verbundenen Risiken werden systematisch gemäss einer einheitlichen Methodik und einem einheitlichen Prozess bewertet.

3.6 IKT-Grundschutz und Umgang mit Ausnahmen

Der IKT-Grundschutz beschreibt die technischen und organisatorischen Massnahmen zur Gewährleistung einer angemessenen Informationssicherheit.

Der IKT-Grundschutz der kantonalen Verwaltung wird periodisch geprüft und wenn nötig aktualisiert. Er gilt als Basis für den Schutz der Informationen und (Fach-)Applikationen und darf nicht unterschritten werden.

Die oder der Vorgesetzte einer Dienststelle können in ihrem Verantwortungsbereich zusätzliche, über den Grundschutz hinausgehende Bestimmungen erlassen.

Muss im Einzelfall aus organisatorischen, technischen oder wirtschaftlichen Gründen der Grundschutz unterschritten werden, liegt eine bewilligungspflichtige Ausnahme vor.

Bei einer Unterschreitung des Grundschutzes müssen die dadurch entstehenden Risiken identifiziert, quantifiziert und in einem Antrag der verantwortlichen Stelle zur Beurteilung und Stellungnahme unterbreitet werden. Eskalationsinstanz ist die IGV.

Ausnahmen sollen zeitlich befristet sein.

3.7 Kontinuierliche Verbesserung der Sicherheit

Das Managementsystem zur Informationssicherheit wird regelmässig auf seine Aktualität und Wirksamkeit geprüft, um die Informationssicherheit aufrechtzuerhalten und zu verbessern. Daneben werden auch die definierten Massnahmen regelmässig daraufhin untersucht, ob sie angemessen sind, ob sie den betroffenen Mitarbeitenden bekannt sind, ob sie umgesetzt werden und ob sie in die Betriebsabläufe integriert sind.

Die Verantwortlichen unterstützen die kontinuierliche Verbesserung der Informationssicherheit. Mitarbeitende der Leistungsbezüger, des Leistungserbringers sowie der Lieferanten geben mögliche Verbesserungen und Schwachstellen an die zuständigen Stellen weiter.

Durch eine kontinuierliche Überprüfung der Regelungen (intern wie extern) sowie deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IKT-Sicherheitstechnik zu halten.

3.8 Behandlung von IKT-Sicherheitsvorfällen

IKT-Sicherheitsvorfälle werden nach definierten Prozessen bearbeitet und dokumentiert. Damit werden die Vorfälle nachvollziehbar abgehandelt. Die Erkenntnisse aus den Vorfällen fliessen in das IKT-Risikomanagement ein und werden zur kontinuierlichen Verbesserung der Informationssicherheit genutzt.

Bei der Behandlung von Sicherheitsvorfällen können das AIO und bei Bedarf externe Experten hinzugezogen werden.

3.9 IKT-Kontinuitätsmanagement

Das IKT-Kontinuitätsmanagement sorgt für die systematische Vorbereitung zur Bewältigung von Störungen und Schadensereignissen. Damit soll erreicht werden, dass wichtige IKT-Grundleistungen in ausserordentlichen Situationen verfügbar bleiben oder dass wichtige Dienste nach einem Ausfall so rasch wie möglich wiederhergestellt sind.

Verschiedene Szenarien von Störungen des ordentlichen IKT-Betriebes und davon abhängigen Geschäftsprozessen werden mit entsprechenden IKT-Notfallvorsorgeplänen abgestimmt. Die durch die Durchführung von Notfallübungen gewonnenen Erkenntnisse dienen der Stabilität und der Widerstandsfähigkeit der IKT-Leistungen gegenüber Störungen und ebenso der Verbesserung der Notfallpläne.

Definitionen, Akronyme und Abkürzungen

Begriff / Abkürzung	Bedeutung
AIO	Amt für Informatik und Organisation
IGV	Informatik Gruppe Verwaltung
IKT	Informations- und Kommunikations-Technologie
ISDS	Informationssicherheit und Datenschutz
ISMS	Information Security Management System

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