Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Sport BASPO

Informationssicherheits-Politik

IS-Policy BASPO

Versionenkontrolle

Autor	Änderung	Version / Datum
fam	Erstellung	1.0 / 15.08.2023

Geht an:

Original
• Mitglieder der Geschäftsleitung BASPO • ISMS Betrieb (Informatik BASPO) • Mitarbeitende (Intranet)

Inhalt

1. Rahmenbedingungen

Die von der Geschäftsleitung festgelegte Informationssicherheitspolitik legt die Rahmenbedingungen für ein effizientes Informationssicherheits-Managementsystem (ISMS) im Bundesamt für Sport (BASPO) fest.

Als Vorgabe für die Informationssicherheitspolitik BASPO gelten die entsprechenden Bundesgesetze und Verordnungen, Weisungen des VBS und des BASPO sowie vertraglich eingegangene Verpflichtungen.

1.1. Ziel und Zweck

Das Bundesamt für Sport (BASPO) verwaltet zahleiche schützenswerte und besonders schützenswerte Daten. Daher gewichtet das BASPO die Informationssicherheit entsprechend hoch und erbringt seine Leistungen auf einem Sicherheitsniveau, das dem jeweiligen Schutzbedarf der Daten angemessen ist.

Als extern anerkanntes Qualitätsmerkmal implementierte das BASPO ein ISMS (Information Security Management System) gemäss ISO 27001 über sämtliche Bereiche und lässt dies jährlich durch eine unabhängige Stelle zertifizieren.

1.2. Geltungsbereich

Der Geltungsbereich erstreckt sich über sämtliche Geschäftstätigkeiten an allen Standorten des BASPO.

1.3. Grundsätze

Sicherheit wird durch das Zusammenwirken von Menschen, Prozessen und Technik erreicht. Dabei ist die Informationssicherheit für das BASPO, seine Kunden und seine Partner von zentraler Bedeutung.

Um die Daten vor Verlust der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit zu bewahren, werden die erforderlichen und wirtschaftlich vertretbaren Sicherheitsmassnahmen technisch und organisatorisch umgesetzt.

Das akzeptable Sicherheitsniveau wird im jeweiligen Fall durch den Schutzbedarf der Daten und die Gefährdungen, welchen diese Daten ausgesetzt sind, bestimmt.

Sicherheitsverfahren des NCSC

Jedem Schutzobjekt (siehe Definition in Kapitel 2.1) oder jeder Gruppe von Schutzobjekten ist eine verantwortliche Person zugeordnet. Diese verantwortet die Umsetzung und Aktualisierung der Sicherheitsmassnahmen. Der Schutzbedarf sämtlicher Schutzobjekte ist bekannt und alle Werte des BASPO, welche es zu schützen gilt, sind systematisch erhoben.

Werte des BASPO sind im Sinne des ISMS Informationen, welche in unterschiedlichen Formen und auf verschiedenen Medien gespeichert vorliegen. Informationen können hierbei auf Papiergeschrieben, digital oder in den Köpfen der Mitarbeitenden vorhanden sein. Gerade bei der Verarbeitung spielen heute die Informatik und die Informationssysteme eine zentrale Rolle.

2. Definition und Festlegung

2.1. Informationssicherheit am BASPO

Das ISMS BASPO hat zum Ziel, sämtliche Informationen, die durch die Unternehmenstätigkeit empfangen, erzeugt, verarbeitet, verbreitet, gespeichert und vernichtet werden angemessen zu schützen. Dies unter Einhaltung der gesetzlichen Grundlagen, der Vorgaben der Bundesverwaltung sowie der vertraglich eingegangenen Verpflichtungen. Nationale und internationale Normen und Standards werden als Guidelines im Sinne des Standes der Technik verwendet.

Die Informationssicherheit am BASPO ist risikobasiert. Basis für alle Massnahmen ist eine Risikobeurteilung. Können Risiken nicht vollständig überwälzt, vermieden oder vermindert werden, so muss die Geschäftsleitung des BASPO die verbleibenden Risiken akzeptieren oder auf die Tätigkeit verzichten.

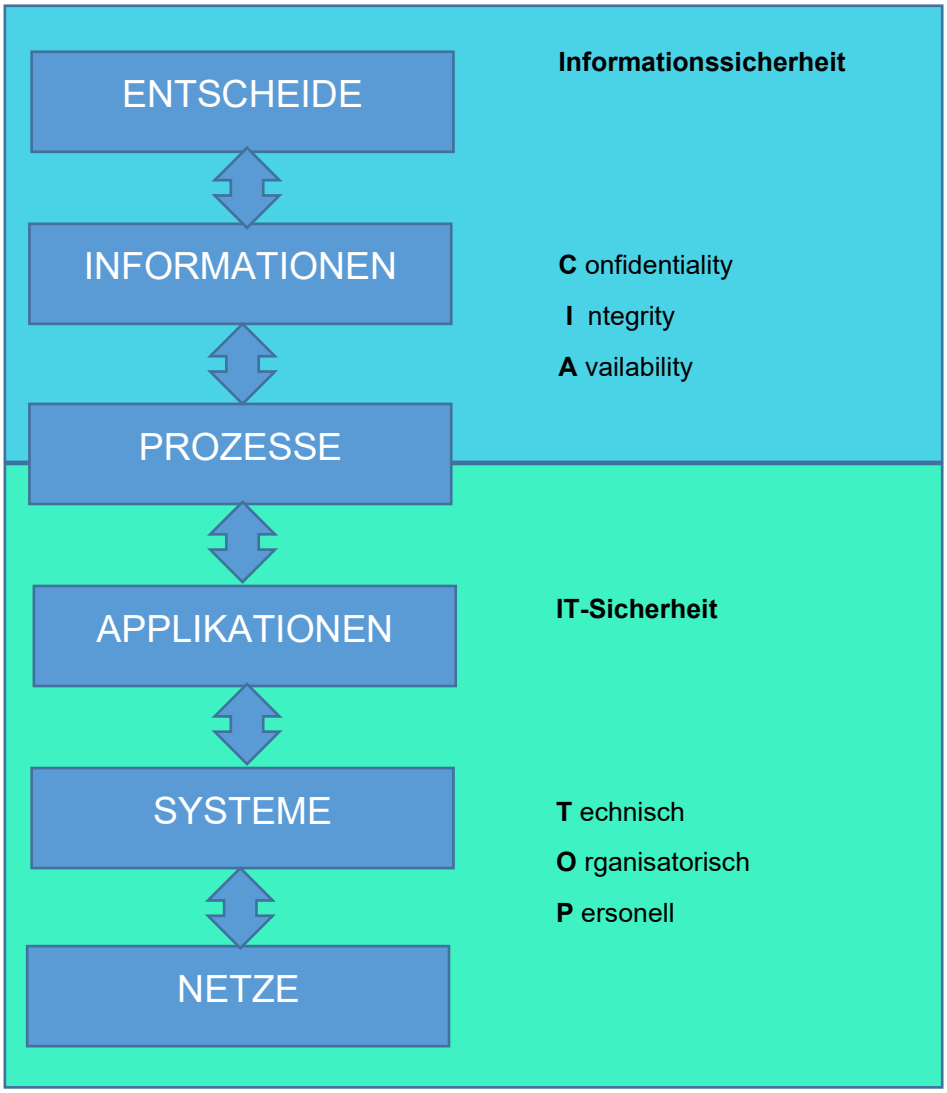
Informationen dienen als Grundlage für Entscheidungen, wobei folgende Fälle zu unterscheiden sind:

Die Information ist richtig und ich weiss, dass sie richtig ist.	Die Information ist falsch und ich weiss, dass sie falsch ist.
Die Information ist richtig und ich weiss nicht, dass sie richtig ist.	Die Information ist falsch und ich weiss nicht, das sie falsch ist.

Die Abgrenzung zwischen Informationen und Daten ist wie folgt definiert:

Informationen sind durch Menschen interpretierte Daten.

Maschinen können Daten verarbeiten, keine Informationen, deshalb wird in der folgenden Darstellung zwischen Informationssicherheit und IT-Sicherheit unterschieden.



Informationen sind eine wertvolle Ressource im Unternehmen. Sie dienen dazu, Entscheide zu fällen. Um gute Entscheide fällen zu können, müssen die Informationen folgende Voraussetzungen erfüllen:

- Die Informationen sollen nur jene kennen, die dafür autorisiert sind (Confidentiality)
- Die Information muss richtig sein (Integrity)
- Die Information muss zeitgerecht zur Verfügung stehen (Availability)
- Die Nachvollziehbarkeit über den Lebenszyklus der Information muss gewährleistet sein.

Die Anforderungen an die Informationen vererben sich auf die dazugehörigen Prozesse, Applikationen, Systeme und Netze (siehe obige Abbildung). Die Applikationen, Systeme und Netze werden unter dem Oberbegriff IT-Objekte zusammengefasst und sind mit den Mitteln der IT-Sicherheit geschützt. IT-Objekte können durch technische, organisatorisch und personelle Massnahmen geschützt werden.

2.2. Funktion Informationssicherheit

Die Informationssicherheit stellt den risikobasierten Schutz von Informationen sicher. Dazu werden die Informationen klassifiziert. Entsprechend dieser Klassifizierung werden die Schutzmassnahmen für alle betroffenen Werte des BASPO, welche es zu schützen gilt, definiert.

Durch die regelmässige Überprüfung der Klassifizierung und der implementierten Sicherheitsmassnahmen wird der nachhaltige Schutz der Informationen sichergestellt.

2.3. ISMS am BASPO

Die Geschäftsleitung BASPO unterstützt und fördert die für das ISMS notwendigen Strukturen und Prozesse. Dazu benennt sie Verantwortliche, welche BASPO-interne Vorgaben zur Informationssicherheit machen, die Umsetzung der Vorgaben des Departements oder des Bundes koordinieren und die Einhaltung der Regelungen und Vorgaben in allen Bereichen einfordern und überwachen.

Die Informationssicherheit am BASPO wird durch ein definiertes Managementsystem (GRC Toolbox) sichergestellt. Dabei orientiert sich das BASPO an der Norm ISO 27001.

Die Verantwortung für die Einhaltung der ISMS Anforderungen bzw. für die Umsetzung der Konzepte liegt in der Linie.

Durch Schulungs- und Sensibilisierungsmassnahmen stellt das BASPO sicher, dass den Betroffenen die Anforderungen bekannt sind und das Bewusstsein der Informationssicherheit gefördert wird.

2.4. Organisation Informationssicherheit

Die Geschäftsleitung des BASPO bestimmt den Sicherheitsbeauftragten. Dieser führt das ISMS fachlich und stellt sicher, dass die Anforderungen in der Linie bekannt sind. In Absprache mit der Geschäftsleitung des BASPO ist er für die Weiterentwicklung des Managementsystems verantwortlich.

Der Sicherheitsbeauftragte schlägt der Geschäftsleitung BASPO jährlich die Sicherheitsziele vor; diese legt die definitiven Jahresziele fest.

2.5. Kontinuierliche Verbesserung

Der aktuelle Stand der Informationssicherheit wird regelmässig überprüft, notwendige Massnahmen werden identifiziert, bewertet und wo sinnvoll umgesetzt.

Jährlich findet ein Maturitätsmeeting mit der Geschäftsleitung statt. Daraus resultiert die Managementbewertung des ISMS.

Die Informationssicherheitspolitik wurde anlässlich der Geschäftsleitungssitzung am 13 September 2023 durch die gesamte Geschäftsleitung BASPO bewilligt.

Magglingen ……

Remund Matthias RNBIDT
Digital unterschrieben von Remund Matthias RNBIDT
Datum: 2023.09.18 16:48:23 +02'00'

……

Matthias Remund

Direktor BASPO

Waegli Hanspeter VXYTBZ
Digital unterschrieben von Waegli Hanspeter VXYTBZ
Datum: 2023.09.18 11:10:52 +02'00'

……

Hanspeter Wägli

Chef Ressourcen / SiVe BASPO

Amsler Fritz EZ00TV
18.09.2023

Info: admin.ch/esignature | validator.ch

……

Fritz Amsler

Sicherheitsbeauftragter BASPO