Informationssicherheitspolitik

Inhalt

Datum	Version	Anmerkung
16.05.2022	1.0	Verabschiedung des Dokuments durch die Direktion

1. Hintergrund / Wort der Direktion

Die HES-SO Valais-Wallis ist eine tertiäre Bildungs- und Forschungseinrichtung. Um ihre Aufträge zu erfüllen, sammelt oder erzeugt, speichert, verarbeitet, verbreitet, archiviert oder entsorgt die HES-SO Valais-Wallis im Rahmen ihrer verschiedenen Tätigkeiten Informationen. Diese Informationen sind für unsere Institution ein wertvolles Gut, das es mit grösster Sorgfalt zu schützen gilt, da diese Informationen zur Aufwertung unserer Innovationen, Forschung und Lehre beitragen.

Vor diesem Hintergrund ist die Direktion davon überzeugt, dass die Sicherung unseres Informationsvermögens für die Tätigkeiten der HES-SO Valais-Wallis von entscheidender Bedeutung ist. Im Rahmen ihres Entwicklungsplans verpflichtet sich die HES-SO Valais-Wallis, eine Strategie umzusetzen, die die Sicherheit des Informationssystems gewährleistet.

Das Ziel der Informationssicherheitspolitik besteht darin, die Sicherheitsstrategie der Direktion der HES-SO Valais-Wallis allen Personen und Partnern, die mit der HES-SO Valais-Wallis in Verbindung stehen, aufzuzeigen.

Die Politik richtet sich insbesondere an die Personen, die im Rahmen der Aufträge der HES-SO Valais-Wallis Informationen verwenden, erwerben, erstellen oder verändern.

Die Direktion verpflichtet sich, die notwendigen Mittel für den Aufbau und den Betrieb der Organisation für Informationssicherheit bereitzustellen. Die Politik beschreibt die Leitlinien im Hinblick auf die Gewährleistung der Umsetzung der technischen und organisatorischen Massnahmen gemäss den bewährten Praktiken der Informationssicherheit.

2. Ziel der Informationssicherheitspolitik

Die von der Direktion verabschiedete Informationssicherheitspolitik legt die Strategie, den Rahmen und die Zuständigkeiten in Zusammenhang mit der Informationssicherheit an der HES-SO Valais-Wallis fest.

Die Politik soll vor allem Folgendes gewährleisten:

- Die Einhaltung von Gesetzen, Vorschriften und unseren vertraglichen Verpflichtungen.
- Die Sicherheit der Informationen gemäss den folgenden Kriterien:
    - Die **Vertraulichkeit** soll sicherstellen, dass Informationen nur denjenigen zugänglich sind, die dazu befugt sind.
    - Die **Integrität** soll sicherstellen, dass die Informationen und die Methoden, mit denen sie verarbeitet werden, korrekt und vollständig sind.
    - Die **Verfügbarkeit** soll sicherstellen, dass die Informationen oder das System, das sie verwendet, gemäss den festgelegten Kriterien zugänglich sind.
- Eine Ausrichtung der Sicherheitsmassnahmen an der Strategie und den geschäftlichen Anforderungen der Schule.
- Die Sensibilisierung aller Interessengruppen für die Informationssicherheit und die Risiken, die mit der Nutzung der Informationstechnologie einhergehen.

Diese Ziele sollen zur Erfüllung der Aufträge der HES-SO Valais-Wallis, zum Schutz ihres Rufs und zur Einhaltung der geltenden gesetzlichen Vorschriften beitragen.

3. Anwendungsbereich

Die Politik gilt für die nachstehend beschriebenen Informationsvermögenswerte, Interessengruppen und Tätigkeiten.

Informationsvermögen

Als Informationsvermögen gelten Informationen, die als wertvoll für die HES-SO Valais-Wallis betrachtet werden, unabhängig von ihrer physischen oder elektronischen Form und der Art und Weise, wie sie gespeichert werden.

Man unterscheidet zwischen folgenden Informationsvermögenswerten:

- Sie gehören der HES-SO Valais-Wallis und werden von dieser genutzt;
- Sie gehören der HES-SO Valais-Wallis, sind jedoch im Besitz eines Partners, Lieferanten oder anderer Beteiligter;
- Sie gehören einem Partner, Lieferanten oder anderen Beteiligten und werden zugunsten der HES-SO Valais-Wallis genutzt.

Interessengruppen

Die Studierenden und Mitarbeitenden der HES-SO Valais-Wallis.

Alle externen Berater, Lieferanten, Partner, Institutionen oder Unternehmen, die auf das Informationsvermögen der HES-SO Valais-Wallis zugreifen oder dieses nutzen müssen.

Tätigkeiten

Das Sammeln oder die Produktion, der Erwerb, die Speicherung, die Verarbeitung, die Verbreitung, die Archivierung oder die Entsorgung von Informationsvermögen, das sich in den Räumlichkeiten der HES-SO Valais-Wallis oder an einem anderen Ort befindet.

4. Gesetzlicher Rahmen

Die HES-SO Valais-Wallis verpflichtet sich zur Einhaltung sämtlicher für sie geltenden Rechtstexte, insbesondere bei der Aktualisierung und Aufrechterhaltung der Informationssicherheit. Sie berücksichtigt insbesondere die folgenden Texte:

Art. 28 des Schweizerischen Zivilgesetzbuches (ZGB) über den Schutz der Persönlichkeit

Bundesgesetz über die Ergänzung des Schweizerischen Zivilgesetzbuches (OR)

Gesetz über die Information der Öffentlichkeit, den Datenschutz und die Archivierung (GIDA)

Bundesgesetz über den Datenschutz (DSG)

Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Datenschutz-Grundverordnung (DSGVO)

Interkantonale Vereinbarung der Fachhochschule Westschweiz (HES-SO)

Gesetz über die Fachhochschule Westschweiz Valais/Wallis, insbesondere Artikel 12

Verordnung über den Status des Personals der Fachhochschule Westschweiz Valais/Wallis, SR 414.701, insbesondere Artikel 4 und Artikel 71 über die Rechte des Arbeitnehmers

Bundesgesetz über die Forschung (FIFG), insbesondere Artikel 26

5. Umsetzung der Informationssicherheit

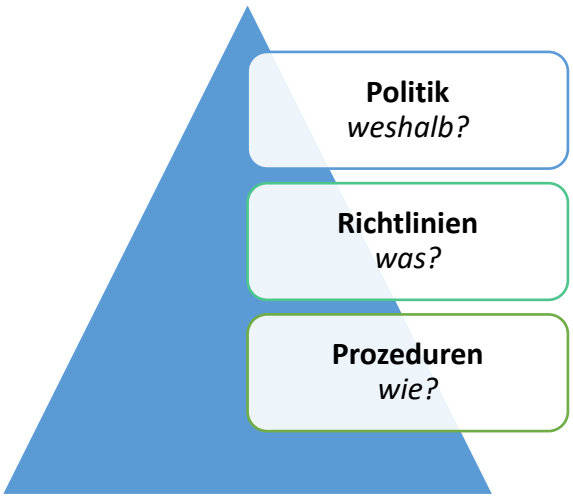
Die HES-SO Valais-Wallis anerkennt, dass diese für ihre Lehr- und Forschungstätigkeiten wesentlichen Informationen während des gesamten Lebenszyklus angemessen bewertet, genutzt und geschützt werden müssen. Es müssen kohärente technische und organisatorische Sicherheitsmassnahmen eingeführt werden, die auf einem Sicherheitsrisikomanagement-Ansatz beruhen.

Diese Sicherheitsmassnahmen finden sich in verschiedenen Dokumenten wieder, die sich mit der Informationssicherheit befassen. Diese muss auf allen hierarchischen Ebenen der Schule umgesetzt werden. Das Konzept der Informationssicherheit lässt sich in drei Dokumentenebenen unterteilen:

Informationssicherheitspolitik: Willensbekundung der Direktion; ausgehend von einer strategischen Analyse beschreibt diese Politik den Rahmen für das Management der Informationssicherheit.

Sicherheitsrichtlinien: Verhaltensregeln und Massnahmen, die für bestimmte Themenbereiche gelten.

Sicherheitsprozeduren und bewährte Praktiken: Regeln, Verhaltensregeln, Tätigkeiten und bewährte Praktiken für das Sicherheitsmanagement.



6. Grundprinzipien der Informationssicherheit

Um ihre Zielsetzungen im Bereich der Informationssicherheit zu erreichen, stützt sich die HES-SO Valais-Wallis auf die Grundprinzipien der Informationssicherheit, insbesondere:

Bewährte Praktiken

Sich auf bewährte Praktiken in diesem Bereich stützen, insbesondere

- ISO/IEC 27000,
- NIST Cybersecurity Framework,
- COBIT (Control Objectives for Information and related Technology).

Informationsvermögen

Die zu schützenden Informationswerte und deren Sensibilitätsgrad sowie die Verantwortlichen kennen.

Defense in Depth (DID)

Das Defense in Depth Prinzip anwenden, um das Informationsvermögen mittels kohärenter und komplementärer Massnahmen (auf menschlicher, organisatorischer oder technischer Ebene) zu schützen.

Least Privilege-Prinzip

Das Least Privilege-Prinzip anwenden, indem der Zugang zu Informationen darauf beschränkt wird, was für die Erfüllung der Tätigkeiten in Übereinstimmung mit Gesetzen, Verordnungen und Richtlinien unbedingt erforderlich ist.

Aufgabentrennung

Das Prinzip der Aufgabentrennung anwenden, um Fehler oder Unregelmässigkeiten zu vermeiden oder rasch zu erkennen.

Stärkung der Sicherheit der Informationstechnologien

Technische Sicherheitsmassnahmen umsetzen, um die Schwachstellen und die Gefährdung der verschiedenen Systeme, die Informationen beherbergen oder verarbeiten, z. B. Kommunikationsnetzwerke, Server, Software und PCs, zu verringern.

Schutz personenbezogener und vertraulicher Daten

Sichere Verarbeitung von personenbezogenen Daten und sensiblen personenbezogenen Daten zum Schutz der betroffenen Personen unter Einhaltung der geltenden Gesetze, insbesondere des GIDA, des DSG und der DSGVO. Auch alle anderen vertraulichen Informationen der HES-SO Valais-Wallis schützen.

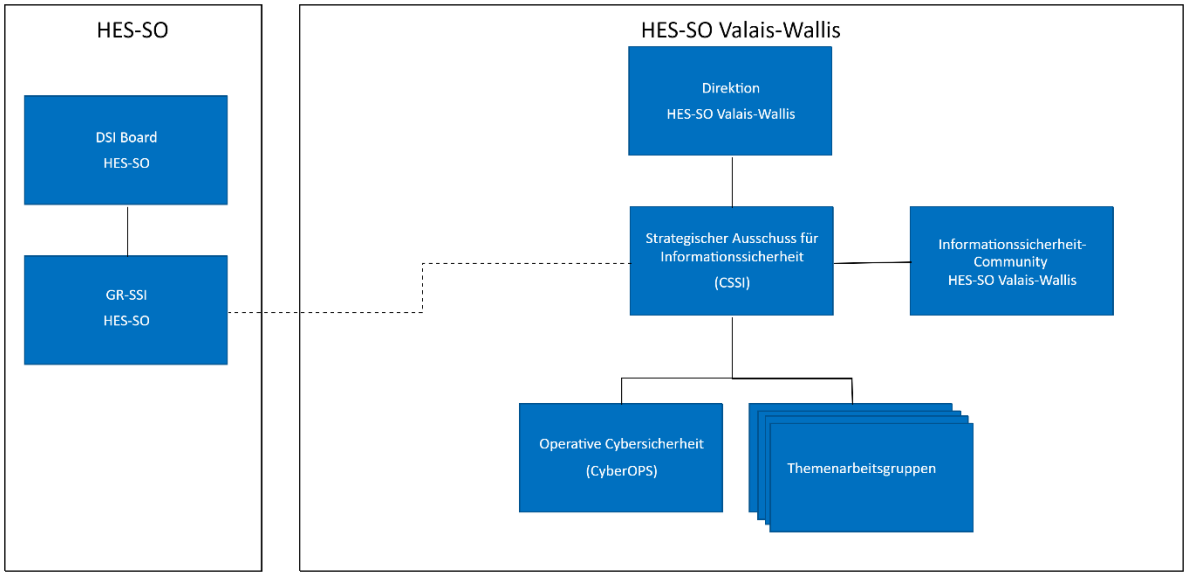
7. Prinzipien und Umsetzung

Im Hinblick auf die Informationssicherheit werden die folgenden Prinzipien umgesetzt:

- Managementsystem für Informationssicherheit (ISMS), das auf den bewährten Praktiken in diesem Bereich beruht.
- Regelmässige Bewertung der Informationssicherheitsrisiken im Einklang mit den institutionellen Risiken, die jährlich von der Direktion überprüft wird.
- Durchführung von Audits und Dokumentenprüfungen alle zwei Jahre
- Eine Folgenabschätzung bei jeder Änderung und jedem Projekt an der Schule, die das Informationsvermögen betreffen.
- Eine progressive und pragmatische Umsetzung der Informationssicherheit.

8. Organisation und Zuständigkeiten

Um die Erreichung der Zielsetzungen der Informationssicherheitspolitik zu gewährleisten, wird die folgende Organisation aufgebaut:



Direktion

Die Direktion unterstützt und bestätigt die vom Strategischen Ausschuss für Informationssicherheit vorgeschlagene Informationssicherheitspolitik.

Sie stellt insbesondere sicher, dass:

- die Informationssicherheitspolitik und ihre Ziele mit der strategischen Ausrichtung der Schule vereinbar sind,
- die Anforderungen an die Informationssicherheit in die Geschäftsprozesse der Schule integriert sind,
- die zur Gewährleistung der Informationssicherheit erforderlichen Ressourcen verfügbar sind,
- die Management- und Governance-Grundsätze für die Informationssicherheit zu den gewünschten Ergebnissen führen.

Strategischer Ausschuss für Informationssicherheit (CSSI)

Unter der Verantwortung der Direktion übernimmt der Strategische Ausschuss für Informationssicherheit (CSSI) die Führungsrolle beim Schutz des Informationsvermögens der HES-SO Valais-Wallis.

Der CSSI hat folgende Aufgaben:

- die Informationssicherheitspolitik ausarbeiten und der Direktion unterbreiten,
- die Richtlinien zur Informationssicherheit erarbeiten und pflegen,
- alle Massnahmen in Zusammenhang mit der Informationssicherheit koordinieren und priorisieren,

- die Umsetzung und Einhaltung der Politik und der Richtlinien überwachen,
- die für die HES-SO Valais-Wallis geltenden bewährten Praktiken für die Informationssicherheit definieren,
- die Umsetzung der Massnahmen an die betroffenen operativen Verantwortlichen oder an speziell gebildete Themenarbeitsgruppen delegieren,
- den Krisenmanagementprozess in Zusammenhang mit der Informationssicherheit implementieren und koordinieren,
- eine auf die strategischen Risiken abgestimmte Risikoanalyse der Informationssicherheit durchführen und aufrechterhalten,
- die umzusetzenden Schutzmassnahmen unter Berücksichtigung der Entwicklung der strategischen Risiken der HES-SO Valais-Wallis regelmässig aktualisieren,
- an der HES-SO Valais-Wallis eine Kultur der Informationssicherheit fördern.
- Jedes Ausschussmitglied ist dafür verantwortlich,
    - die für seinen Bereich spezifischen Bedürfnisse in Bezug auf die Informationssicherheit zu definieren,
    - sein Team über die vom CSSI getroffenen Massnahmen zu informieren.

Der CSSI wird von der Direktion ernannt und setzt sich wie folgt zusammen:

Ständige Mitglieder

- Verantwortliche/r Informationssicherheit
- Leiter/in Informatikdienst
- Vertreter/in Direktion
- Datenschutzbeauftragte/r
- Verantwortliche/r Integriertes Managementsystem

Nicht-ständige Mitglieder

- Leiter/in Dienst für Infrastruktur und Sicherheit
- Leiter/in Human Resources
- Leiter/in Kommunikation und Marketing
- Jurist/in Rechtsdienste
- Leiter/in Dienst für angewandte Ethik
- 1 Studiengangsleiter/in
- 1 Institutsleiter/in

Der/die Verantwortliche der Informationssicherheit organisiert und leitet die Sitzungen des CSSI.

Pro Jahr finden vier Sitzungen mit den ständigen und nicht-ständigen Mitgliedern statt.

Der CSSI erstattet der Direktion jährlich Bericht.

Themenarbeitsgruppen

Im Auftrag des CSSI kann eine Arbeitsgruppe zu einem bestimmten Thema eingesetzt werden, um ein Projekt in Zusammenhang mit der Informationssicherheit zu analysieren oder durchzuführen.

Operative Cybersicherheit (CyberOPS)

Innerhalb des Informatikdienstes und unter der Aufsicht des Leiters des Teams Architektur und Sicherheit hat das CyberOPS-Team folgende Aufgaben:

- Technische Massnahmen umsetzen, um die Anforderungen der Informationssicherheit zu erfüllen.
- Sicherheitsschwachstellen bei den täglichen Aufgaben des Informatikdienstes identifizieren und Korrekturmassnahmen anwenden.
- Beim Informatikdienst die Anwendung bewährter Praktiken zur Informationssicherheit gewährleisten.
- IT-Sicherheitsvorfälle bearbeiten und den CSSI darüber informieren.
- Die von den Nutzern geäusserten Sicherheitsbedürfnisse ermitteln und ggf. den CSSI informieren.

Das Team für operative Cybersicherheit besteht aus Vertretern und Vertreterinnen der verschiedenen IT-Teams.

Informationssicherheit-Community

Die Informationssicherheit-Community ermöglicht es interessierten Personen der HES-SO Valais-Wallis, sich informell über Themen in Zusammenhang mit der Informationssicherheit auszutauschen. Die Anfragen und Vorschläge der Community werden an den CSSI weitergeleitet.

Die Community wird vom Verantwortlichen für die Informationssicherheit geleitet.

Gruppe der IT-Sicherheitsbeauftragten (GR-SSI)

Die GR-SSI ist das Steuerungsorgan für die gemeinsamen Sicherheitsaspekte der Informationssysteme der HES-SO.

DSI Board

Das DSI Board ist verantwortlich für die Informationssysteme der HES-SO und die Umsetzung der damit zusammenhängenden Entscheidungen. Es schlägt den Entscheidungsgremien die Grundsätze und Umsetzungsmassnahmen vor und kontrolliert das Portfolio der gemeinsamen Projekte und Lösungen.

9. Erklärung zur Anwendbarkeit

Die nachstehend aufgeführten Bereiche werden in dieser Informationssicherheitsrichtlinie nach ISO 27002 berücksichtigt und in den Richtlinien und Prozeduren näher erläutert:

- Informationssicherheitspolitik
- Organisation der Informationssicherheit
- Personalsicherheit
- Verwaltung der Werte
- Zugangssteuerung
- Kryptographie
- Physische und umgebungsbezogene Sicherheit
- Betriebssicherheit
- Kommunikationssicherheit
- Anschaffung, Entwicklung und Instandhaltung von Systemen
- Lieferantenbeziehungen
- Handhabung von Informationssicherheitsvorfällen
- Informationssicherheitsaspekte beim Business Continuity Management
- Compliance