Politique de sécurité de l'information

Table des matières

Date	Version	Observation
16.05.2022	1.0	Validation du document par la Direction générale

1. Contexte / mots de la Direction

La HES-SO Valais-Wallis est une institution de formation et de recherche de niveau tertiaire. Afin de mener à bien ses missions, la HES-SO Valais-Wallis collecte ou produit, stocke, traite, diffuse, archive ou élimine de l'information lors de ses différentes activités. Ces informations ont de la valeur pour notre institution et constituent un atout précieux qu'il convient de protéger avec la plus grande rigueur car elles participent à valoriser l'innovation, la recherche et l'enseignement que nous proposons.

Dans ce contexte, la Direction générale est convaincue que la sécurisation de notre patrimoine informationnel est primordiale aux activités de la HES-SO Valais-Wallis. Dans le cadre de son plan de développement, la HES-SO Valais-Wallis s'engage à mettre en œuvre une stratégie afin garantir la sécurité du système d'information.

L'objectif de la politique de sécurité de l'information est d'exprimer la stratégie de sécurité de la direction de la HES-SO Valais-Wallis à l'ensemble des personnes et partenaires en relation avec la HES-SO Valais-Wallis.

La politique s'adresse en particulier à ceux et celles qui utilisent, acquièrent, créent ou modifient de l'information dans le cadre des missions de la HES-SO Valais-Wallis.

La Direction générale s'engage à mobiliser les moyens nécessaires à la mise en place et au fonctionnement de l'organisation de la sécurité de l'information. La politique décrit les lignes directrices pour garantir la mise en œuvre des mesures techniques et organisationnelles selon les bonnes pratiques de la sécurité de l'information.

2. But de la Politique de sécurité de l'information

La Politique de sécurité de l'information, validée par la Direction générale, fixe la stratégie, le cadre et les responsabilités en matière de sécurité de l'information au sein de la HES-SO Valais-Wallis.

Les principaux objectifs de la politique sont d'assurer :

- La conformité légale, règlementaire et nos engagements contractuels
- La sécurité de l'information selon les critères ci-dessous :
    - La **confidentialité** a pour objectif de s'assurer que l'information n'est accessible qu'à ceux et celles dont l'accès est autorisé.
    - L'**intégrité** a pour objectif de s'assurer de l'exactitude et de l'intégralité de l'information et des méthodes de traitement de celle-ci.
    - La **disponibilité** a pour objectif de s'assurer que l'information ou le système qui l'utilise soit accessible selon les critères définis.
- Un alignement des mesures de sécurité à la stratégie et aux exigences métier de l'institution
- La sensibilisation des parties prenantes à la sécurité de l'information et aux risques inhérents à l'utilisation des technologies de l'information.

Ces objectifs ont pour but de contribuer à la réalisation des missions de la HES-SO Valais-Wallis,à protéger sa réputation et à respecter les prescriptions légales en vigueur.

3. Champ d'application

La politique s'applique aux actifs informationnels, parties prenantes et activités décrites ci-dessous.

Actifs informationnels

Les actifs informationnels sont des informations reconnues comme ayant une valeur pour la HES-SO Valais-Wallis, quelle que soit leur forme physique ou électronique et la manière dont elles sont stockées.

On distingue les actifs informationnels :

- appartenant à la HES-SO Valais-Wallis et exploités par celle-ci ,
- appartenant à la HES-SO Valais-Wallis mais détenus par un partenaire, fournisseur ou autre intervenant·e.
- appartenant à un partenaire, fournisseur ou autre intervenant·e et exploités au profit de la HES-SO Valais-Wallis.

Parties prenantes

Les étudiant·e·s, les collaborateur·trice·s de la HES-SO Valais-Wallis.

Tout consultant, fournisseur, partenaire, institution ou entreprise externe appelés à accéder ou à utiliser les actifs informationnels de la HES-SO Valais-Wallis.

Activités

Les activités impliquant la collecte ou la production, l'acquisition, le stockage, le traitement, la diffusion, l'archivage ou l'élimination des actifs informationnels localisés dans les locaux de la HES-SO Valais-Wallis ou dans un autre lieu.

4. Cadre légal et règlementaire

La HES-SO Valais-Wallis s'engage au respect de l'ensemble des textes normatifs qui lui sont applicables, notamment dans la mise à jour et le maintien de la sécurité de l'information. Elle porte une attention particulière aux textes suivants :

L'art. 28 du Code Civil Suisse (CC) protégeant la personnalité

La Loi fédérale complétant le Code civil Suisse (CO)

La Loi sur l'information du public, la protection des données et l'archivage, LIPDA

La Loi fédérale sur la protection des données, LPD

L'Ordonnance relative à la loi fédérale sur la protection des données (OLPD)

Le Règlement général sur la protection des données, RGPD

La Convention intercantonale sur la Haute Ecole Spécialisée de Suisse occidentale (HES-SO)

La Loi sur la Haute Ecole spécialisée de Suisse occidentale Valais/Wallis, notamment son article 12.

L'Ordonnance concernant le statut du personnel de la Haute Ecole Spécialisée de Suisse occidentale Valais/Wallis, RS 414.701, notamment son article 4 et les articles 71 sur les droits de l'employé.

La Loi fédérale sur la recherche, LERI, notamment son article 26.

5. Démarche de la sécurité de l'information

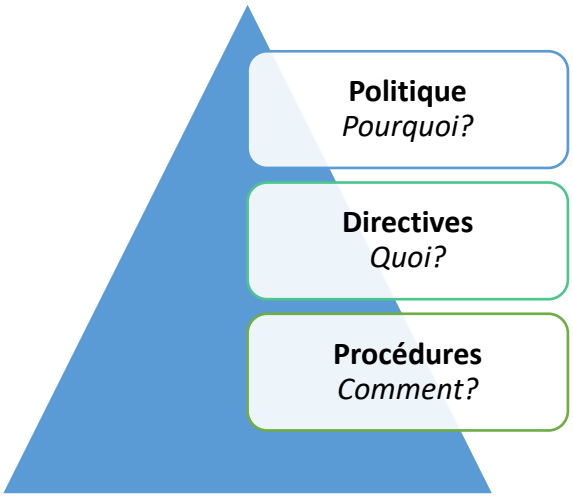
La HES-SO Valais-Wallis reconnait que ces informations, essentielles à ses activités d'enseignement et de recherche, doivent faire l'objet d'une évaluation, d'une utilisation et d'une protection adéquates, et ce, tout au long du cycle de vie. Il convient de mettre en œuvre un ensemble cohérent de mesures de sécurité techniques et organisationnelles définies par une approche de gestion des risques de sécurité.

Ces mesures de sécurité se retrouvent dans différents documents traitant de la sécurité de l'information. Celle-ci doit être présente à tous les niveaux hiérarchiques de l'institution. Le concept de sécurité de l'information se décompose en 3 niveaux de documents :

Politique de sécurité de l'information : Déclaration de la volonté de la Direction générale, basée sur une analyse stratégique, elle décrit le cadre de la gouvernance de la sécurité de l'information.

Directives de sécurité : ce sont les règles de conduite et des mesures appliquées dans des thématiques spécifiques.

Procédures et bonnes pratiques de sécurité : elles présentent les règles, les lignes de conduite, activités et bonnes pratiques pour la gestion de la sécurité.



6. Principes fondamentaux de la sécurité de l'information

Afin d'assurer ses objectifs de sécurité de l'information, la HES-SO Valais-Wallis se base sur des principes fondamentaux de la sécurité de l'information, notamment :

Référentiels de bonnes pratiques

S'appuyer sur les bonnes pratiques du domaine, en particulier les référentiels

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

Patrimoine informationnel

S'assurer de connaître ses actifs informationnels à protéger ainsi que leur degré de sensibilité et en identifier les responsables.

Défense en profondeur

Appliquer le principe de défense en profondeur pour protéger les actifs informationnels en mettant en œuvre des mesures cohérentes et complémentaires d'ordre humaines (comme la sensibilisation des utilisateurs), organisationnelles ou techniques.

Moindre privilège

Appliquer le principe du moindre privilège en limitant l'accès aux informations au strict nécessaire pour l'accomplissement de son activité en conformité avec les lois, règlements et directives.

Séparation / ségrégation des tâches

Appliquer le principe de séparation des tâches afin d'éviter et d'identifier les erreurs ou les irrégularités rapidement.

Renforcer la sécurité des technologies de l'information

Mettre en œuvre des mesures de sécurité techniques pour réduire les vulnérabilités et l'exposition aux menaces des différents systèmes hébergeant ou traitant de l'information comme par exemple les réseaux de communication, les serveurs, les logiciels et les postes de travail.

Protection des données personnelles et confidentielles

Sécuriser les traitements de données personnelles et de données personnelles sensibles afin de protéger les personnes concernées, dans le respect des lois applicables, notamment la LIPDA, la LPD et le RGPD. Protéger également toute autre information confidentielle de la HES-SO Valais-Wallis.

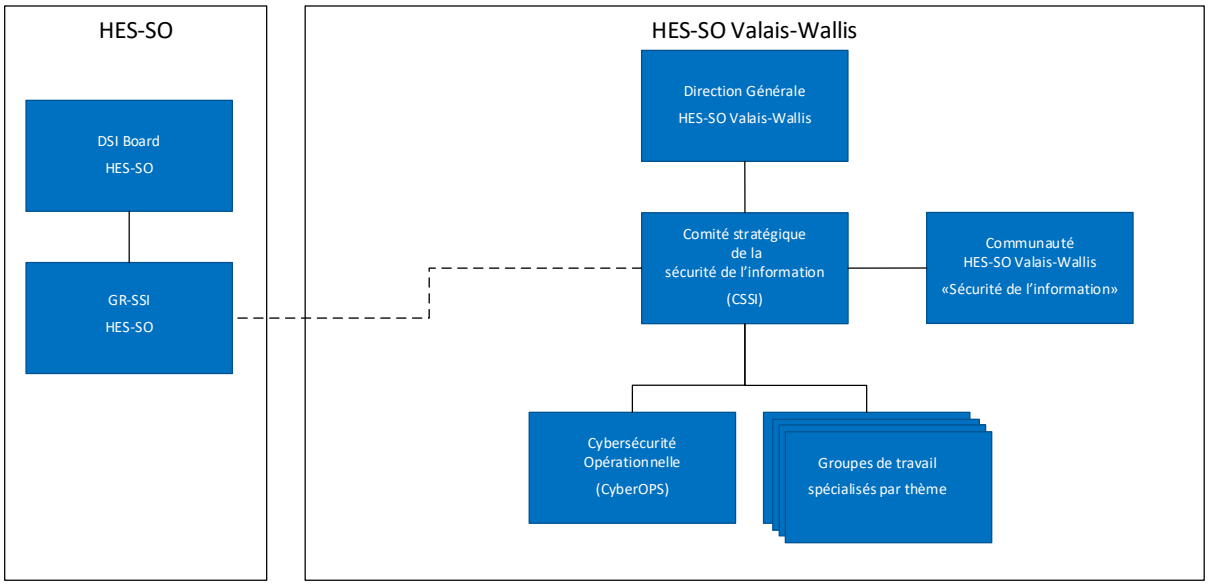
7. Principes et mise en œuvre

Pour assurer la sécurité de l'information, les principes suivants sont mis en œuvre :

- Un système de management de la sécurité de l'information (SMSI) respectant les meilleures pratiques du domaine
- Une évaluation régulière des risques de sécurité de l'information en cohérence avec les risques institutionnels revue annuellement par la Direction générale
- La mise en place d'audits et de revue de documents tous les 2 ans
- Une analyse d'impact à chaque changement et chaque projet dans l'institution qui concerne un actif informationnel
- Une mise en œuvre de la sécurité de l'information progressive et pragmatique

8. Organisation et responsabilités

Afin de garantir l'atteinte des objectifs de la politique de sécurité de l'information, l'organisation suivante est mise en place :



La Direction générale

La Direction générale soutient et valide la politique de sécurité de l'information proposée par le comité stratégique de la sécurité de l'information.

Elle s'assure notamment que :

- La politique de sécurité de l'information et ses objectifs sont compatibles avec l'orientation stratégique de l'organisation.
- Les exigences de sécurité de l'information sont intégrées aux processus métier de l'organisation.
- Les ressources nécessaires pour assurer la sécurité de l'information sont disponibles.
- Les principes de management et de gouvernance de la sécurité de l'information produisent les résultats escomptés.

Le comité stratégique de la sécurité de l'information (CSSI)

Sous la responsabilité de la Direction générale, le comité stratégique de la sécurité de l'information (CSSI) assure le leadership dans la protection des actifs informationnels de la HES-SO Valais-Wallis.

Le CSSI a pour mission :

- D'élaborer et de proposer la politique de sécurité de l'information à la Direction générale
- D'élaborer, de maintenir et de réviser les directives de sécurité de l'information
- De coordonner et prioriser l'ensemble des actions liées à la sécurité de l'information
- De contrôler que la politique et ses directives soient appliquées et respectées

- De définir les bonnes pratiques de la sécurité de l'information applicables à la HES-SO Valais-Wallis
- De déléguer la mise en œuvre des actions aux responsables opérationnel·le·s concerné·e·s ou à des groupes de travail spécialisés constitués pour des thèmes spécifiques.
- D'implémenter et coordonner le processus de gestion de crise lié à la sécurité de l'information
- De réaliser et maintenir une analyse de risques de la sécurité de l'information alignée aux risques stratégiques
- D'actualiser régulièrement les mesures de protection à mettre en œuvre au regard de l'évolution des risques stratégiques de la HES-SO Valais-Wallis.
- De promouvoir une culture de la sécurité de l'information au sein de la HES-SO Valais-Wallis
- Chaque membre du comité a la responsabilité
    - d'identifier les besoins spécifiques métier à leur domaine en matière de sécurité de l'information,
    - d'informer leurs équipes des mesures prises par le CSSI.

Le CSSI est nommé par la Direction générale et est composé :

De membres permanents

- Responsable de la sécurité informatique
- Responsable du service informatique
- Représentant de la Direction générale
- Délégué à la protection des données
- Responsable du système de management intégré

Des membres non permanents

- Responsable du service infrastructure et sécurité
- Responsable du service des ressources humaines
- Responsable du service communication et marketing
- Juriste du service juridique
- Responsable du service éthique appliquée
- Un responsable de filière
- Un responsable d'institut

Le responsable de la sécurité informatique organise et anime les séances du CSSI.

Quatre séances par année sont organisées avec membres permanents et non permanents.

Le CSSI rapporte annuellement à la Direction générale.

Groupes de travail spécialisé

Sur mandat du CSSI, un groupe de travail spécialisé peut être créé autour d'un thème spécifique pour analyser ou mettre en œuvre un projet lié à la sécurité de l'information.

Cybersécurite opérationnelle (CyberOPS)

Au sein du service informatique, sous la supervision du responsable d'équipe architecture et sécurité, l'équipe CyberOPS a pour mission de :

- Mettre en œuvre les mesures techniques pour répondre aux exigences de la sécurité de l'information
- Identifier les vulnérabilités sécuritaires lors des missions quotidiennes du service informatique et appliquer les mesures correctives
- Garantir l'application des bonnes pratiques en matière de sécurité de l'information au sein du service informatique
- Traiter les incidents de sécurité informatique et en informer le CSSI
- Identifier les besoins de sécurité exprimés par les utilisateurs et les remonter au CSSI si nécessaire

L'équipe de cybersécurité opérationnelle est composée de ressources représentant les différentes équipes IT.

Communauté « Sécurité de l'information »

La communauté de la sécurité de l'information permet aux personnes de la HES-SO Valais-Wallis qui sont intéressées par la thématique de partager de manière informelle sur les sujets en lien avec la sécurité de l'information. Les demandes et propositions de la communauté seront transmises au CSSI.

La communauté est animée par le responsable de la sécurité informatique.

Groupe des répondants sécurité des systèmes d'information (GR-SSI)

Le GR-SSI est l'organe de pilotage des aspects communs de la sécurité au sein de la fédération des SI HES-SO.

DSI Board

Le DSI Board, direction de la fédération des Systèmes d'information de la HES-SO, est responsable de contrôler l'application des décisions concernant la fédération des SI HES-SO. Il propose les principes aux instances de décision, propose les dispositifs d'application, contrôle le portefeuille des projets et des solutions communes.

9. Déclaration d’applicabilité

Les domaines ci-dessous sont pris en compte dans cette politique de sécurité de l’information selon le référentiel ISO 27002 et seront détaillés dans les directives et procédures :

- Politique de sécurité de l'information
- Organisation de la sécurité de l’information
- Sécurité des ressources humaines
- Gestion des actifs
- Contrôle d’accès
- Cryptographie
- Sécurité physique et environnementale
- Sécurité liée à l’exploitation
- Sécurité des communications
- Acquisition, développement et maintenance des systèmes d’information
- Relations avec les fournisseurs
- Gestion des incidents liés à la sécurité de l’information
- Aspects de la sécurité de l'information dans la gestion de la continuité de l’activité
- Conformité