POLITIQUE GÉNÉRALE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION (PGSSI)

Classification :	Public
Public cible :	Administration Cantonale Vaudoise
Propriétaire :	DGNSI
Identifiant :	DSI-05.1-SX0002
Statut :	Validé
Version & Date :	1.4 du 05.09.2022
Révision :	Annuelle
Emplacement :	Référentiel documentaire DGNSI
Fichier :	05.1 politique générale de sécurité des systèmes d'information (pgssi).docx

TABLE DES MATIÈRES

1 RESUME

UN BESOIN CROISSANT DE PROTECTION POUR UNE RESSOURCE ESSENTIELLE

Les systèmes d'information (SI) sont de plus en plus essentiels aux activités de l'Administration alors que l'interconnexion entre les systèmes ainsi que le déploiement de la cyberadministration exposent les SI à des risques nouveaux et croissants.

Un objectif principal

En conséquence, le Conseil d'Etat s'engage à soutenir les mesures visant à **assurer une protection appropriée des systèmes d'information de l'Administration Cantonale contre toutes les menaces, qu'elles soient d'origine interne ou externe, naturelle, accidentelle ou délibérée.**

Une politique générale de sécurité

Cette **politique générale de sécurité des systèmes d'information** (PGSSI) fixe le périmètre, les principes de mise en œuvre ainsi que les responsabilités nécessaires pour atteindre l'objectif général de protection.

13 principes de mise en œuvre selon 5 axes

Pour atteindre les objectifs généraux de protection, le Conseil d'Etat a défini 13 principes de mise en œuvre regroupés en 5 axes :

1. Un système de management de la sécurité conforme aux meilleures pratiques
2. Une gestion des risques régulière, efficace et proportionnée
3. Des mesures de sécurité conformes aux meilleures pratiques
4. Une exploitation et une évolution des SI conformes aux politiques de sécurité.
5. Une mise en œuvre progressive et pragmatique

Une implication nécessaire de toutes les parties prenantes

La mise en œuvre de la politique de sécurité nécessite l'implication de toutes les parties prenantes : usagers externes, départements et Services de l'Administration, personnel, Direction des systèmes d'information ainsi que fournisseurs.

2 INTRODUCTION

BUT DU DOCUMENT

Le Conseil d'Etat définit dans ce document la politique générale de sécurité des systèmes d'information (PGSSI) qu'il entend mettre en œuvre pour s'assurer que les systèmes d'information (SI) soient protégés contre les risques qui menacent leur disponibilité, leur intégrité et leur confidentialité.

Cette politique fixe le périmètre, l'objectif principal, les principes ainsi que les responsabilités nécessaires à sa mise en œuvre.

DOMAINE D'APPLICATION

La politique générale de sécurité (PGSSI) s'applique :

Périmètre

- Au périmètre tel que défini par le règlement informatique [1], soit à toutes les entités de l'Administration cantonale, à l'exception de l'informatique pédagogique, de l'informatique des hautes écoles et de l'informatique des Hospices/CHUV.
- A l'ordre judiciaire vaudois dans le respect des conventions spéciales réglant ses relations avec la DGNSI.
- Par convention, à toute autre entité partenaire.

Champ d'application

Pour ces entités, la politique s'étend à :

- tous les **fournisseurs de prestations dans le domaine des SI** : entités internes ou externes fournissant, directement ou indirectement, des biens et services dans le domaine des systèmes d'information,
- tous les **usagers** internes et externes des SI : entités, collaborateurs, personnel externe disposant d'un accès autorisé aux systèmes d'information,
- toutes les **données dématérialisées** nécessaires à l'exécution des missions de l'Etat,
- tous les **traitements** des informations : ensemble des opérations effectuées avec des données sources pour produire des résultats permettant la prise de décision et/ou l'accomplissement d'une action ; ceci concerne tout le cycle de vie des informations, depuis la saisie jusqu'à la destruction, en passant par le traitement, le transport, le stockage, l'exploitation et l'archivage,
- tous les **éléments techniques matériels ou logiciels** utilisés pour acquérir, produire, traiter, échanger, transporter, modifier ou stocker de l'information sous forme électronique,
- toutes les **infrastructures** : sites, bâtiments ou locaux contenant des biens matériels ou immatériels composant les systèmes d'information.

REFERENCES LEGALES ET NORMATIVES

La politique générale de sécurité s'appuie et tient compte des bases légales et normatives suivantes :

[1] Règlement relatif à l'informatique cantonale (172.62.1), ainsi que les directives d'application associées

[2] Règlement relatif à l'organe d'audit des systèmes d'information et de télécommunication

[3] Normes ISO de la série 27000

[4] Loi sur le personnel, ainsi que les directives d'application associées

[5] Loi sur la protection des données

ENTREE EN VIGUEUR

La PGSSI entre en vigueur dès son adoption par le Conseil d'Etat.

Elle annule et remplace tous les autres documents publiés antérieurement sur le thème de la sécurité des systèmes d'information. Ceci concerne en particulier les documents de base suivants ainsi que leurs diverses versions qui avaient été validés et publiés par le CE en 2004 :

- Ligne directrice SSI-VD
- SSI-VD

DEFINITIONS

Sécurité des systèmes d'information (SSI)
Protection des systèmes d'information contre les accidents (pannes, pertes, événements naturels ou physiques, etc.), les erreurs (d'utilisation, de conception ou de fuite d'information) et les actes malveillants (piratage, falsification, fraude, vol, écoute, sabotage, ingénierie sociale, etc.) au moyen de mesures préventives et correctives, ainsi que de procédures de contrôle organisationnelles ou techniques appropriées.

Système d'information
Ensemble des moyens (organisation, acteurs, processus, procédures, données, systèmes informatiques) nécessaires à l'acquisition, au traitement, à la transmission et à la conservation des informations pour assurer les missions et les prestations de l'Administration.

Système informatique
Ensemble des moyens (matériels, logiciels, réseaux, téléphonie, applications) au sein desquels le traitement, la transmission et la conservation des informations se fait de manière électronique.

Système de management de la sécurité de ld'information (SMSI)
Partie du système de management global, basée sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité des systèmes d'information.

3 OBJECTIF GENERAL

UN BESOIN CROISSANT DE PROTECTION

Le Conseil d'Etat considère que :

- les systèmes d'information (SI) sont de plus en plus essentiels aux activités de l'Administration,
- l'interconnexion entre les systèmes ainsi que le déploiement de l'administration en ligne, exposent les SI à des risques nouveaux et croissants,
- le déploiement de la cyberadministration nécessite un niveau adéquat de protection des données pour gagner la confiance nécessaire des usagers.

Un objectif principal

En conséquence, le Conseil d'Etat s'engage à mettre en œuvre **une protection appropriée des systèmes d'information de l'Administration Cantonale, contre toutes les menaces, qu'elles soient d'origine interne ou externe, naturelle, accidentelle ou délibérée.**

Des niveaux de sécurité évalués selon 4 critères fondamentaux

Cet objectif de protection sera atteint par la mise en œuvre de mesures proportionnées visant à assurer le niveau de sécurité requis en termes de :

- **Confidentialité** : capacité du système à protéger les informations de toute divulgation non autorisée.
- **Intégrité** : capacité du système à préserver les informations de toute altération, destruction ou modification non autorisée.
- **Disponibilité** : capacité du système à maintenir l'accessibilité aux informations en toute circonstance ainsi que le fonctionnement continu et fiable des applications.
- **Traçabilité :** capacité du système à relever et enregistrer les opérations qui sont effectuées dans un but de restitution ultérieure du déroulement des évènements lorsque cela est nécessaire.

4 PRINCIPES DE MISE EN OEUVRE

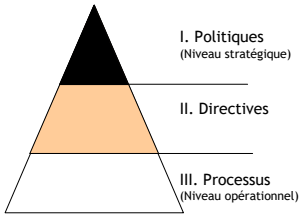
13 PRINCIPES DIRECTEURS POUR METTRE EN ŒUVRE LA POLITIQUE

Pour atteindre les objectifs généraux de protection, le Conseil d'Etat a défini 5 axes regroupant les 13 principes de mise en œuvre :

Axe 1. Un système de management de la sécurité conforme aux meilleures pratiques

1. Un **système de management de la sécurité de l''information (SMSI)** est établi, mis en œuvre, exploité, surveillé, audité, mis à jour et amélioré en continu conformément aux meilleures pratiques et aux principes exposés dans les normes telles que celles de la série ISO27000.

2. La **documentation du système de management de la sécurité** se fonde sur une architecture à 3 niveaux :



   I. Les **politiques** sont des documents de niveau stratégique qui fixent les objectifs, les principes et l'organisation. On distingue deux politiques :

      - La politique générale de sécurité des SI (PGSSI), le présent document, définit les objectifs principaux, principes de mise en œuvre et responsabilités. La PGSSI est adoptée par le Conseil d'Etat.
      - La politique de sécurité des SI (PSSI) est élaborée par la DGNSI, elle définit l'organisation et les processus DGNSI mis en place pour répondre aux exigences de la PGSSI.

   II. Les **directives de sécurité** sont des documents qui déclinent les politiques pour un domaine spécifique, afin de définir les exigences organisationnelles ou techniques de sécurité correspondantes. On distingue trois types de directives :

      - Les directives de sécurité générales sont élaborées par la DGNSI, constituent le socle sécuritaire et s'appliquent à tout le périmètre de la PGSSI.
      - Les directives de sécurité métiers à caractère technique peuvent compléter les directives générales de sécurité émises par la DGNSI. Ces directives peuvent être élaborée par les Services bénéficiaires pour répondre à des besoins spécifiques. Elles sont soumises à l'approbation de la DGNSI, qui en évaluera l'impact et assurera la cohérence globale.
      - Les directives de sécurité métiers à caractère non technique peuvent compléter les directives générales de sécurité émises par la DGNSI. Elles sont élaborées par les Services bénéficiaires en fonction de leurs besoins spécifiques.

   III. Les **processus, procédures et modes opératoires** sont des documents de niveau opérationnel qui décrivent les activités à réaliser (par qui, comment et avec quoi). Les processus des Services bénéficiaires et de la DGNSI intègrent les exigences de sécurité exprimées par les directives tant générales que spécifiques aux métiers.

Axe 2. Une gestion des risques régulière, efficace et proportionnée

3. **Tout système d'information fait l'objet d'une gestion des risques liés à la sécurité**. Cette gestion assure que les exigences en matière de sécurité des systèmes sont identifiées et que l'identification, l'appréciation et le traitement des risques sur les systèmes d'information sont régulièrement effectués. Elle permet de définir et de mettre en œuvre des mesures de sécurité adaptées en s'assurant que les actions prévues et les coûts engendrés sont proportionnés à la réduction de risque qui sera obtenue.

Axe 3. Des mesures de sécurité conformes aux meilleures pratiques

4. Tous les **biens liés aux systèmes d'information sont identifiés, inventoriés et attribués à un propriétaire**. Ils sont classifiés selon leur niveau d'importance afin de mettre en place et de maintenir une protection appropriée.
5. La **sécurité relative aux ressources humaines** est prise en compte, afin de réduire le risque de vol, de fraude ou de mauvais usage des SI, ainsi que de s'assurer que les utilisateurs connaissent leurs responsabilités et qu'ils sont en adéquation avec les fonctions qui leur sont attribuées.
6. La **sécurité physique** est assurée afin d'empêcher tout accès non autorisé et de protéger les éléments des systèmes d'information contre les menaces extérieures et environnementales.
7. Seuls les personnes ou systèmes autorisés ont **accès aux systèmes d'information**. Tout départ ou changement de fonction d'un utilisateur doit s'accompagner des ajustements nécessaires de ses droits d'accès.
8. Tous les **événements et les failles de sécurité** sont signalés, traités et analysés par les responsables désignés, afin de limiter leur impact et de permettre la mise en œuvre d'actions correctives dans les meilleurs délais.
9. La **continuité des activités est assurée** par l'identification des sinistres envisageables et de leurs impacts ainsi que par la mise en œuvre des solutions de secours permettant, même en mode dégradé, la continuité des activités en fonction de la nécessité qu'il y a de les préserver.
10. La **conformité des SI aux exigences légales**, contractuelles et techniques est vérifiée à échéances régulières.

Axe 4. Une exploitation et une évolution des SI conforme aux politiques de sécurité

11. **L'acquisition, le développement et la maintenance des systèmes d'information** sont maîtrisés en veillant à ce que la sécurité fasse partie intégrante des systèmes d'information, afin de répondre aux besoins exprimés par les métiers concernés.
12. **L'exploitation des systèmes d'information** est maîtrisée à travers des responsabilités et des procédures clairement définies et documentées, afin de sécuriser et de surveiller les moyens de traitement de l'information conformément aux besoins. La sécurité des échanges d'information est également prise en compte.

Axe 5. Une mise en œuvre progressive et pragmatique

13. **La mise en œuvre de la gestion des risques et des mesures de sécurité qui en découlent est réalisée de manière pragmatique** en abordant les risques transversaux et les risques sectoriels les plus importants dans le cadre de l'élaboration des schémas directeurs ou de l'évolution des systèmes d'information jugés par les parties prenantes comme les plus critiques.

5 RESPONSABILITES

DES RESPONSABILITES REPARTIES EN 9 PARTIES PRENANTES

Pour assurer la mise en œuvre de la politique de sécurité, les responsabilités sont réparties entre les parties prenantes comme suit, conformément au dispositif réglementaire en vigueur [1, 2, 4, 5] :

Le Conseil d'Etat

Le Conseil d'Etat a la responsabilité :

- d'adopter la politique *générale* de sécurité des systèmes d'information (PGSSI) afin de définir les **objectifs généraux et les principes de mise en œuvre** de la protection des informations, en particulier des données personnelles, afin de garantir en tout temps leur disponibilité, leur intégrité et leur confidentialité. [1-art 4,15],
- d'adopter, via une directive spécifique, les principes de gestion des risques ainsi que les critères d'évaluation et d'acceptation des risques,
- d'accepter formellement les risques transversaux résiduels identifiés par la DGNSI et préavisés par le CSG élargi,
- de mandater régulièrement des audits de sécurité [1-art.11a][2],
- d'adopter les propositions DGNSI d'amélioration du système de management de la sécurité.

Les organes de contrôle de l'Etat

Les organes de contrôle ont la compétence :

- de réaliser ou mandater des audits de sécurité.

Le Chef du département

Le Chef du département en charge de la DGNSI, a la responsabilité :

- de veiller à la mise en œuvre d'un système de gestion de la sécurité conforme à la politique générale de sécurité des SI.

Le collège des secrétaires généraux (CSG) élargi

Le Collège des Secrétaires Généraux élargi a la responsabilité :

- de prendre connaissance des **risques transversaux** identifiés par la DGNSI afin de sélectionner les mesures de sécurité appropriées et **de proposer au CE d'accepter formellement les risques résiduels.**
- d'arbitrer, si nécessaire, le **plan général de traitement des risques** soumis par la DGNSI.

Les Services bénéficiaires

Les services ont la responsabilité :

- de définir les directives de sécurité métier à caractère non technique,
- de proposer à la DGNSI, si nécessaire, les directives de sécurité métier à caractère technique,
- d'assurer l'utilisation des SI conformément aux politiques et directives de sécurité,
- d'identifier les besoins de sécurité, les exigences légales, les menaces et vulnérabilités propres à leur métier,
- d'analyser et d'évaluer les risques, avec l'appui de la DGNSI, afin de déterminer les niveaux de sécurité requis, de sélectionner les mesures appropriées et d'accepter formellement les risques sectoriels résiduels,
- d'arbitrer, si nécessaire, le plan sectoriel de traitement des risques,
- d'assurer l'application de la politique générale et des directives associées dans le cadre de leur périmètre et, par extension, auprès de leurs usagers et fournisseurs internes ou externes,
- de demander à la DGNSI, si nécessaire, les contrôles découlant de l'application de la loi sur le personnel.

Le personnel de l'ACV

Les collaborateurs de l'Administration Cantonale sont responsables :

- d'utiliser et de traiter les informations qui leur sont confiées conformément aux politiques et directives de sécurité ou autres réglementations applicables.

Le non respect des exigences de sécurité entraînera l'application du dispositif prévu par la loi du 12 novembre 2001 sur le personnel de l'Etat, art. 59 et suivants (concernant l'avertissement, voire le licenciement).

La Direction générale du numérique et des systèmes d'information (DGNSI)

La DGNSI a la responsabilité de :

- proposer au Conseil d'Etat et mettre en œuvre une politique générale de sécurité des systèmes d'information (PGSSI). [1-art. 7]
- mettre en œuvre l'organisation et les processus nécessaires à la mise en œuvre, au contrôle interne et à l'amélioration continue d'un système de management de la sécurité (SMSI) conforme à la politique.
- définir, mettre en œuvre et faire évoluer la politique de sécurité des SI (PSSI) ainsi que les directives de sécurité générale et de les intégrer dans ses processus et procédures.
- proposer au CE, via une directive de sécurité spécifique, les principes de gestion des risques ainsi que les critères d'évaluation et d'acceptation des risques de sécurité.
- soutenir les services bénéficiaires dans toutes les activités de gestion des risques de sécurité liées à leur système d'information.
- dresser périodiquement un état des lieux des risques *de* sécurité encourus et proposer des mesures préventives et correctives adaptées aux moyens qui lui sont alloués. [1-art. 20]
- mettre en œuvre et d'opérer les mesures de sécurité adoptées.
- proposer au CSG élargi et au CE, si nécessaire, un arbitrage du plan général de traitement des risques.
- valider les directives métiers à caractère technique.
- assurer l'utilisation, l'exploitation et l'évolution des SI conformément aux politiques et directives de sécurité.
- coordonner les activités des parties prenantes en matière de sécurité des SI.
- sensibiliser le personnel et les tiers concernés aux risques encourus et aux mesures de sécurité correspondantes.
- communiquer les politiques et directives de sécurité, ainsi que de sensibiliser les utilisateurs à la sécurité des SI.

Le personnel de la DGNSI

Chaque collaborateur de la DGNSI ou intervenant externe pour le compte de la DGNSI est responsable :

- de réaliser ses activités, de faire usage de ses droits d'accès ainsi que d'utiliser et de traiter les informations qui lui sont confiées, conformément aux politiques, directives et procédures de sécurité.
- de signaler à l'instance compétente de la DGNSI tout fait ou comportement anormal qu'il pourrait observer dans le domaine de la sécurité des systèmes d'information.

Le non - respect des exigences de sécurité entraînera l'application du dispositif prévu par la loi du 12 novembre 2001 sur le personnel de l'Etat, art. 59 et suivants (concernant l'avertissement, voire le licenciement).

Les intervenants techniques externes à la DGNSI

Chaque intervenant externe à la DGNSI, mettant en œuvre directement ou indirectement des systèmes techniques permettant de traiter des données de l'administration, est responsable :

- des données produites et traitées ainsi que des traitements qu'il effectue, conformément à la présente politique. Le non - respect des exigences de sécurité entraînera des poursuites conformément aux bases légales en vigueur.