REPUBLIQUE ET CANTON DE GENEVE
Département de la sécurité et de l'économie
Direction générale des systèmes d'information (DGSI)

Niveau de protection :
Public

POLITIQUE DE SECURITE DE L'INFORMATION (PSI)

Date :	12 novembre 2014
Approbation par le Conseil d'Etat le :	17 décembre 2014
Version :	2
Auteur :	Comite de sécurité de l'information
Propriétaire :	Direction générale des systèmes d'information

L'ensemble des informations relatives aux personnes est valable aussi bien pour le personnel masculin que féminin. Néanmoins, pour des facilités de lecture, seule la forme masculine est utilisée.

SOMMAIRE DE LA POLITIQUE DE SECURITE DE L'INFORMATION

1 *But du document*

Une réponse à une exigence

Le règlement sur l'organisation et la gouvernance des systèmes d'information et de communication stipule à son article quatre que le Conseil d'Etat fixe le cadre politique et réglementaire dans lequel doivent évoluer les systèmes d'informations et de communication de l'administration cantonale.

Ce cadre est notamment fixé par la politique de sécurité de l'information (PSI).

La présente PSI fixe les objectifs, le périmètre, les règles ainsi que les responsabilités nécessaires à sa mise en œuvre.

Elle sera complétée par des directives et suivie de plans d'action spécifiques.

2 *Objectifs et engagements*

Un constat

L'Etat considère que la protection des informations et des ressources matérielles et immatérielles du domaine des technologies de l'information et de la communication placées sous sa responsabilité est devenue une nécessité prioritaire. La prépondérance des systèmes d'information et de communication, les évolutions technologiques marquées par l'interconnexion et la cyberadministration, et la multiplicité et la dangerosité croissantes des menaces et des risques, rendent indispensable la mise en place de mesures de sécurité cohérentes et efficaces, s'inscrivant dans une stratégie de sécurité de l'information.

Un engagement

Le Conseil d'Etat s'engage à soutenir toute mesure proportionnelle aux risques encourus, visant à protéger l'information, contre toutes menaces internes ou externes, accidentelles, naturelles ou délibérées.

Des objectifs principaux

Ces mesures doivent respecter et assurer les principes directeurs de la sécurité de l'information qui sont :

a) la préservation :
   1. du capital informationnel de l'Etat,
   2. de la continuité des activités de l'administration cantonale qui dépendent des systèmes d'information et de communication,
   3. des ressources matérielles et immatérielles;

b) la maîtrise des risques, conformément aux besoins de l'Etat;

c) l'application et le contrôle des dispositions légales et réglementaires, notamment en matière de protection des données personnelles.

Une sécurité répondant à 5 critères fondamentaux

Ces mesures visent à assurer la protection des informations relativement aux cinq critères de sécurité suivants :

- **Confidentialité** : *Propriété selon laquelle l'information est rendue accessible ou divulguée uniquement aux personnes, entités et processus autorisés*.
- **Intégrité** : *Propriété de protection de l'exactitude (non modification ou altération) et de l'intégralité (exhaustivité et cohérence) des ressources (actifs)[1] et des traitements.*

[1] Sans précision ou qualificatif, le terme ressource désigne en totalité ou partiellement les éléments listés au ch. 3 Domaines d'application – section "Des ressources spécifiques"

- **Disponibilité :** *Propriété pour une ressource d'être accessible et utilisable à la demande par une entité autorisée.*
- **Imputabilité** : *Propriété de pouvoir attribuer des actions et des décisions à une entité en assurant la traçabilité, la non-répudiation et la constitution de preuves.*
- **Conformité** : *Propriété de satisfaire à une exigence acceptée ou imposée à l'organisme (lois, obligations, politiques ou normes par exemple).*

Une politique transparente

Cette PSI est disponible et accessible à l'ensemble des parties prenantes[2] et en toute transparence. De ce fait, elle constitue un outil de sensibilisation et de prise de conscience pour l'ensemble des acteurs.

3 *Domaines d'application*

Un périmètre organisationnel

La PSI s'applique à toute personne, entité ou tout autre partenaire s'intégrant dans un rapport de hiérarchie avec l'Etat et accédant aux ressources matérielles et immatérielles de l'administration (ci-après utilisateur).

Elle s'applique également à toute autre personne physique ou morale ayant accepté par voie contractuelle ou conventionnelle la présente politique ainsi que les directives et procédures qui en découlent.

Des ressources spécifiques

Sont pris en compte dans cette PSI les ressources qui constituent les systèmes d'information et de communication (ci-après SIC) de l'Etat et assurent directement ou indirectement le processus global de traitement de l'information et la délivrance des prestations.
Ces ressources sont listées ci-dessous de manière non exhaustive :

- les données et informations qui constituent le patrimoine informationnel de l'Etat et qu'il convient de protéger de manière adaptée, quel que soit son support et sa forme (documents papier, fichiers électronique, processus, bases de données ou autres) et l'état de son traitement (saisie, échange, stockage, modification, exploitation, archivage et destruction),
- les ressources matérielles et immatérielles appartenant au domaine des technologies de l'information et de la communication,
- les entités physiques et morales qui développent, possèdent, fournissent, gèrent, maintiennent et utilisent les SIC de l'Etat,
- les entités et les ressources matérielles et immatérielles n'appartenant pas à l'Etat et se connectant de manière autorisée aux SIC de l'Etat,
- le cadre physique et environnemental en relation avec les systèmes d'information.

4 *Référentiels*

Un cadre légal et règlementaire

Le cadre légal et réglementaire comprend notamment les textes suivants:

[2] Les gouvernements, les entreprises et organisations et les utilisateurs individuels qui développent, possèdent, fournissent, gèrent, maintiennent et utilisent les systèmes et réseaux d'information (cf. document "Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information").

- Règlement sur l'organisation et la gouvernance des systèmes d'information et de communication (ROGSIC – B 4 23.03).
- Lois et règlements relatifs au personnel de l'Etat, en particulier la loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux (LPAC - B 5 05) et son règlement d'application (RPAC - B 5 05.01).
- Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD – A 2 08), ainsi que son règlement d'application (RIPAD – A 2 08.01).
- Loi sur les archives publiques (LArch – B 2 15) et son règlement d'application (RArch – B 2 15.01).
- Règlement sur le télétravail (RTt – B 5 05.13)
- Règlement sur la gestion des risques (RGR - D 1 05.10).
- Règlement sur la communication électronique (RCEL – E 5 10.05)

Un cadre normatif

Cette politique de sécurité prend en compte l'ensemble des normes internationales relatives à la sécurité de l'information (normes de la famille ISO 27000).

Elle s'intègre dans la gouvernance et la gestion des SIC (référentiel Cobit), et le système de contrôle interne (référentiel COSO), tels que mis en œuvre au sein de l'Etat.

En principe, la version la plus récente de ces normes et référentiels s'applique.

5 *Hiérarchie des textes*

Une défense en profondeur

Pour atteindre les objectifs principaux, la présente PSI établit les règles et mesures générales de sécurité.

Celles-ci sont à appliquer dans une démarche globale permettant d'assurer la cohérence de l'ensemble du dispositif de sécurité, couvrant à la fois les couches stratégique, tactique et opérationnelle et les dimensions relatives aux personnes et à l'organisation, aux processus et aux technologies.

L'application du concept de défense en profondeur permet de construire une défense globale, coordonnant plusieurs lignes de protection.

La sensibilisation, la formation et l'information du personnel de l'Etat sont essentielles à sa mise en œuvre.

Une documentation structurée

L'ensemble de la politique de sécurité de l'Etat est composé du présent document complété par des politiques spécifiques, des directives, des instructions et toute autre documentation validée ayant pour objectif la protection de l'information.

Cette documentation est structurée en trois niveaux, selon la Figure 1:

- Le premier niveau est composé des documents à caractère stratégique qui fixent les objectifs, les principes et l'organisation. Actuellement s'y trouvent le règlement sur l'organisation et la gouvernance des systèmes d'information et de communication qui établit les principes stratégiques, ainsi que la présente PSI qui décline ces principes en règles et mesures générales de sécurité.

- Le deuxième niveau comprend des directives qui définissent les exigences organisationnelles ou techniques de sécurité correspondantes, ainsi que les modalités d'application.
  Ces directives sont alignées au cadre normatif, en traitant des aspects de la sécurité de l'information dans les domaines tel que par exemple l'organisation, la gestion des ressources, notamment humaines, le contrôle d'accès, la cryptographie, l'exploitation, les communications, l'acquisition, le développement et la maintenance des systèmes, les relations avec les fournisseurs, la gestion des incidents, la continuité d'activité et la conformité, ainsi que la sécurité physique et environnementale.
- Enfin, le troisième niveau est composé de procédures de mise en œuvre et autres documents qui décrivent de façon opérationnelle les activités à réaliser (par qui, quand, comment et avec quoi).

Pour chaque document de portée transversale, il peut être créé un document spécifique correspondant, répondant à des problématiques ou à des exigences propres à un département, un système d'information, un métier ou autre (voir schéma ci-dessous). Ce document spécifique ne doit pas déroger aux contraintes des documents transversaux.

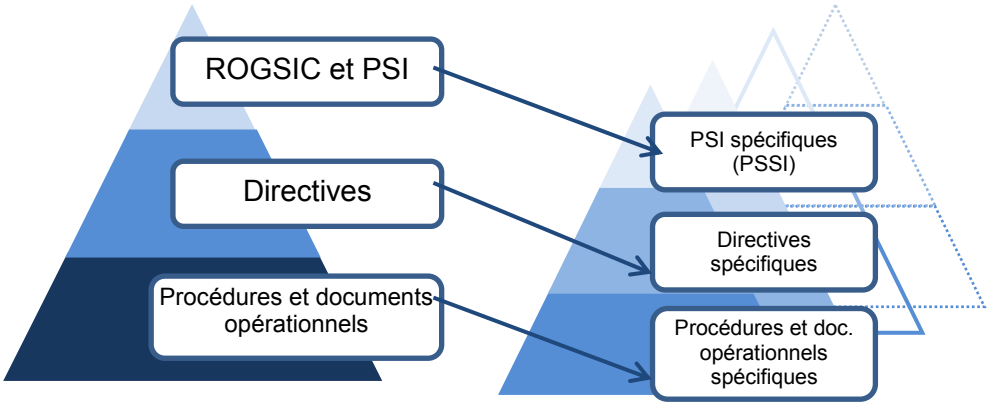

Figure 1

6 *Règles et mesures générales de sécurité*

Une gestion des risques au service de l'amélioration continue de la sécurité

Les exigences en matière de sécurité sont identifiées par une évaluation méthodique des risques.

Les résultats de l'appréciation du risque permettent de définir les actions de gestion appropriées et les priorités en matière de gestion du risque, et d'identifier les mesures adaptées destinées à protéger les ressources contre ces risques. Ces mesures sont cohérentes avec les exigences de sécurité exprimées par les autorités compétentes.

L'appréciation du risque doit être réalisée régulièrement afin de prendre en compte les modifications du contexte, de l'environnement, de l'exposition aux risques et des technologies.

Elle s'inscrit dans un système de gestion de la sécurité de l'information visant à son amélioration continue et s'intégrant dans le système de contrôle interne et de gestion des risques de l'Etat.

Une maîtrise des ressources

Les ressources sont identifiées, inventoriées, classifiées et attribuées à un responsable. Celui-ci s'assure que la protection adéquate est définie et mise en œuvre, en tenant compte des interactions entre les ressources.

Les entités concernées mettent en œuvre les mesures de sécurité appropriées.

Une prise en compte du facteur humain

La sécurité relative aux ressources humaines est prise en compte dès le processus d'engagement afin de réduire le risque de fuite d'information, d'altération des données, de malveillance, notamment de vol et de fraude, ou de mauvais usage des SIC.

Les collaborateurs et les personnes en relation contractuelle avec l'Etat sont informés des lois, règlements, directives et règles de sécurité applicables et des conséquences résultant d'une violation de la sécurité de l'information.

Ils sont sensibilisés ou formés à la sécurité et aux risques pesant sur les SIC en adéquation avec les fonctions qui leur sont attribuées.

Au terme du contrat ou du mandat, la hiérarchie contrôle le retrait des droits d'accès et des ressources attribuées à l'utilisateur.

En cas de transfert organisationnel, la hiérarchie contrôle la mise à jour des droits d'accès.

Une protection physique et environnementale

La sécurité physique est assurée afin d'empêcher tout accès non autorisé et de protéger les ressources des systèmes d'information contre les menaces extérieures et environnementales.

Chaque hiérarchie organisationnelle définit, à son niveau de compétence, des zones de sécurité afin d'apporter un niveau de sécurité physique et environnementale adapté à ses ressources.

Une exploitation sécurisée des ressources

L'exploitation des systèmes d'information et de communication 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.

La sécurité liée à l'exploitation des informations et des ressources a pour objectif de limiter les risques d'accidents, d'erreurs et de malveillance.

Elle est mise en œuvre en appliquant les bonnes pratiques issues des normes, notamment en matière d'architecture technique, de surveillance, de renforcement de la sécurité des systèmes, de sauvegarde et de restauration, de protection contre les codes malveillants, de ségrégation[3] des ressources et de contrôle régulier des vulnérabilités et des mises à jour.

Les prestations en ligne font l'objet de mesures de sécurité spécifiques et de tests systématiques.

Une imputabilité des événements

Des mesures adaptées de surveillance et d'alarmes, ainsi que l'enregistrement sécurisé des événements (activités et accès notamment), sont mis en œuvre, permettant l'imputabilité des actions et la détection d'incidents de sécurité.

[3] Le principe de ségrégation vise à isoler les utilisateurs, les ressources matérielles et immatérielles et les environnements (développement, test et production par exemple) les uns des autres.

Une maîtrise des droits d'accès

Seuls les personnes ou systèmes autorisés ont accès aux ressources. Les autorisations d'accès sont délivrées selon les principes du moindre privilège[4] et de la séparation des rôles et responsabilités, afin d'éviter notamment les conflits d'intérêts et les fraudes. Un processus centralisé coordonne le cycle de vie des autorisations.

La sécurité dans le cycle de vie des ressources

L'acquisition, le développement et la maintenance des ressources sont maîtrisés en veillant à ce que la sécurité fasse partie intégrante du cycle de vie de ces ressources, dès l'origine du projet, afin de répondre aux besoins exprimés par les métiers concernés.

Finalement, les aspects d'archivage et de destruction des informations doivent être pris en compte, afin d'assurer la conformité au cadre légal.

Une gestion maîtrisée des incidents et des failles

Les incidents et les failles de sécurité sont signalés, traités et analysés par les responsables désignés, sur la base de procédures formelles, afin de limiter leur impact et de permettre la mise en œuvre d'actions correctives appropriées dans les meilleurs délais.

Une assurance de la continuité de l'activité

Par la gestion de la continuité de l'activité, l'organisation prend les mesures nécessaires afin de garantir la continuité des prestations et processus métier les plus critiques quelles que soient les circonstances.

Ces mesures prennent en considération les sinistres envisageables et leurs impacts, afin d'assurer le fonctionnement en mode dégradé des offices et le retour à la normale.

Un engagement de conformité

La conformité des ressources et de leur traitement aux exigences légales, réglementaires, contractuelles, conventionnelles, statutaires et techniques est vérifiée à échéances régulières tout au long de leur cycle de vie.

Cette conformité inclut notamment la prise en compte des droits de propriété intellectuelle, de l'application de mesures cryptographiques et de la protection des données.

Un usage maîtrisé des appareils mobiles et du télétravail

L'utilisation de ressources matérielles mobiles (smartphone, par ex.), des services en ligne et des réseaux de transmission publics et privés nécessite la prise en compte d'un environnement de travail qui n'est pas protégé, et donc la mise en place de mesures de défense appropriées.

Des mesures de sécurité complémentaires, incluant des dispositions techniques, des procédures formelles et des actions de sensibilisation spécifiques, protègent des risques supplémentaires liés à ces modes de fonctionnement.

Les dispositions nécessaires doivent être prises pour assurer une séparation entre l'utilisation privée et professionnelle de ces outils, surtout en ce qui concerne les échanges et le stockage de données.

Le télétravail est autorisé dans la limite de la règlementation existante. Sa mise en place doit respecter des mesures spécifiques de sécurité.

Une relation formalisée avec les fournisseurs

Les exigences de sécurité de l'information sont documentées pour limiter les risques résultant de l'accès, du traitement, du stockage et de la communication de l'information, ainsi que de la fourniture de services et de ressources.

[4] Le principe de moindre privilège dicte que chaque fonctionnalité ou chaque acteur ne doit posséder que les privilèges et ressources matérielles et immatérielles nécessaires à l'exécution de son travail, et rien de plus.

Ces exigences imposent des mesures de sécurité spécifiques aux accès des fournisseurs incluant une traçabilité de leurs interventions. Elles sont établies et convenues avec chaque fournisseur en conformité avec les aspects légaux et contractuels, ainsi qu'avec la présente PSI et les directives applicables.

Une révision régulière des autorisations

Les accès physiques et logiques octroyés doivent être revus de manière périodique. Les droits, leurs modifications et les violations doivent être enregistrés.

7 *Organisation, rôles et responsabilités*

Des responsabilités partagées

La sécurité est l'affaire de tous, en agissant avec précaution et prévoyance.

Tout collaborateur et toute entité doit ainsi être conscient de sa responsabilité lors de l'utilisation ou de la gestion des SIC en conformité avec les conditions d'usage.

Tout collaborateur et toute entité assurent que le traitement des données personnelles soit licite, effectué de manière conforme aux principes de la bonne foi et de la proportionnalité, réalisé uniquement dans le but indiqué et dont les finalités du traitement doivent être reconnaissables pour la personne concernée[5].

La sécurité des systèmes d'information et de communication de l'Etat s'appuie sur les responsabilités et l'organisation définies ci-dessous.

Des parties prenantes reconnues

Les rôles et responsabilités des autorités et parties prenantes sont définis principalement dans le règlement sur l'organisation et la gouvernance des systèmes d'information et de communication.

- Le Conseil d'Etat démontre sa volonté et son engagement dans la sécurité en approuvant la présente PSI.
- La direction générale des systèmes d'information (DGSI) élabore et concrétise, en collaboration avec les départements et offices, la présente PSI, les règlements et directives et le pilotage du système de contrôle interne de la sécurité de l'information, sur la base de l'évaluation des risques. De plus elle met en œuvre la présente politique et prend les mesures appropriées pour préserver la sécurité de l'information conjointement avec les maîtres de fichiers.
- La commission de gouvernance des systèmes d'information et de communication priorise les demandes de création et d'évolution substantielle des services fournis par la DGSI. Elle préavise la PSI et approuve les directives.
- Le comité de sécurité de l'information est la plate-forme d'échange et de concertation entre la DGSI et les départements. Il soutient toute action d'amélioration et d'anticipation dans son domaine de compétence.

[5] Cf. Loi fédérale sur la protection des données (LPD 235.1)

- Les départements et offices, en tant que maîtres de fichiers[6], sont responsables de la qualité de leurs informations et des besoins en matière de sécurité. Ils veillent à l'application et au contrôle du cadre légal applicable, de la présente politique et des directives y relatives. Ils peuvent édicter des règles et mesures de sécurité spécifiques dans la mesure où elles s'inscrivent dans le cadre légal et réglementaire en vigueur et sont conformes à la présente PSI.
- Les offices départementaux responsables de l'organisation de l'information conseillent et aident les offices dans l'application et le contrôle de la présente politique. Ils s'assurent de l'intégration de cette PSI dans l'élaboration de leur stratégie. Ils soutiennent le RSI de leur département dans ses activités.
- Les responsables départementaux de la sécurité de l'information (RSI) conduisent, avec la DGSI, la mise en œuvre de la PSI et des directives, et soutiennent la mission des départements, offices, et plus globalement des maîtres des fichiers, en matière de sécurité.

  Ils veillent et contrôlent l'application des lois et des normes en matière de sécurité de l'information.

  Ils communiquent, sur la base d'analyse de risque, les besoins des départements et les faiblesses constatées aux instances concernées.

  Ils collaborent avec les parties prenantes pour la réalisation des audits en matière de sécurité et la mise en place des mesures correctrices.
- Les responsables concernés du contrôle interne accompagnent la mise en œuvre de cette politique, en coordination avec les RSI et la DGSI.
- Seules la Cour des comptes, l'Inspection cantonale des finances et la DGSI disposent de l'autorité pour réaliser ou mandater des audits relativement à la sécurité de l'information.
- D'autres entités, tel que notamment le préposé cantonal à la protection des données et à la transparence et les responsables LIPAD des départements, les ressources humaines et les hiérarchies, accompagnent, appuient, coordonnent ou contrôlent les activités dans le domaine de la sécurité.

8 *Dispositions d'application de la PSI*

Des règles de mise en œuvre

La mise en œuvre de cette politique est réalisée de manière pragmatique et proportionnelle, dans l'intérêt global de l'Etat, en prenant toutefois en compte les besoins et le contexte métier, ainsi que les risques priorisés par les parties prenantes.

Un contrôle d'efficacité

L'efficacité des mesures de protection techniques, organisationnelles et légales est régulièrement contrôlée et mesurée, notamment par la DGSI, selon des indicateurs préalablement définis selon les domaines de la norme ISO 27002. Le niveau de sécurité atteint sera communiqué aux acteurs concernés.

[6] La personne privée ou l'organe fédéral ou cantonal qui décide du but et du contenu du fichier, et qui en est responsable.

Une gestion de la PSI	Pour garantir l'efficacité et l'adaptation de cette PSI aux besoins de l'Etat, le comité de sécurité de l'information est responsable du réexamen régulier de cette politique de sécurité, en cas de changement majeur ou de recommandations d'audits.
Une gestion des exceptions	Des procédures et un modèle d'arbitrage sont mis en œuvre pour traiter les demandes de dérogations à cette politique. Les demandes sont considérées de manière individuelle. Les exceptions validées sont documentées, revues régulièrement et ont une durée de validité limitée.
Des règles de traitement des urgences	En cas d'urgence ou de faille majeure, la DGSI prend toutes les mesures adéquates pour protéger l'intérêt de l'Etat. Elle en informe le magistrat chargé des SIC qui en avise immédiatement le ou les chefs des départements concernés. Ces mesures respectent, dans la mesure du possible, la sphère privée des collaborateurs.
Des mesures en cas de violation	En cas d'actes délictueux ou de non-respect des exigences l'application des mesures prévues dans le cadre légal ou réglementaire peut être réalisée notamment par des sanctions disciplinaires, civiles ou pénales.

9 *Entrée en vigueur*

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

Elle annule et remplace la directive "Politique de sécurité et d'usage des systèmes d'information" du 26.9.2002 (Aigle 02741-2004).