Source SILGENEVE PUBLIC

Dernières modifications au 14 novembre 2023

Règlement sur l'organisation et la gouvernance des systèmes d'information et de communication (ROGSIC)

B 4 23.03

du 26 juin 2013

(Entrée en vigueur : 3 juillet 2013)

Le CONSEIL D'ÉTAT de la République et canton de Genève,
vu la loi sur l'exercice des compétences du Conseil d'Etat et l'organisation de l'administration, du 16 septembre 1993,
arrête :

Chapitre I Dispositions générales

Art. 1 But

Le présent règlement a pour but de définir l'organisation et la gouvernance des systèmes d'information et de communication de l'administration cantonale, notamment dans le domaine de la sécurité de l'information.

Art. 2 Champ d'application

[1] Le présent règlement s'applique à tous les offices, directions et services des départements et de la chancellerie d'Etat, tels que définis par le règlement sur l'organisation de l'administration cantonale, du 1er juin 2023[8], à l'exception des organismes placés sous la surveillance des départements.

[2] Le cas échéant, sont réglées par des conventions spéciales les relations entre l'office cantonal des systèmes d'information et du numérique[5] (ci-après : l'office cantonal[5]) et :

a) le pouvoir judiciaire;
b) le Grand Conseil.

[3] La relation entre l'office cantonal[5] et le département de l'instruction publique, de la formation et de la jeunesse[4], pour la part consacrée aux systèmes d'information et de communication pédagogiques, est également réglée par une convention spéciale.

[4] Toute personne s'intégrant dans un rapport de hiérarchie avec l'Etat et accédant aux systèmes d'information et de communication de l'administration cantonale doit se soumettre aux principes et dispositions du présent règlement, en particulier en matière de sécurité de l'information.

Art. 3 Définitions

[1] Au sens du présent règlement, on entend par système d'information et de communication un ensemble organisé d'éléments en interaction, dont chacun concourt à la collecte, au traitement, à la classification, à la communication et à la conservation de l'information dans un environnement donné.

[2] Les éléments en interaction sont :

a) des personnes;
b) des processus et des procédures;
c) des ressources matérielles et immatérielles appartenant au domaine des technologies de l'information et de la communication (ci-après : ressources matérielles et immatérielles).

[3] Les ressources matérielles et immatérielles sont précisées dans une directive par le collège des secrétaires généraux.[7]

[4] Au sens du présent règlement, on entend par :

a) gouvernance : les moyens par lesquels les parties prenantes peuvent s'assurer de la prise en compte de leurs intérêts dans le fonctionnement d'un système d'information et de communication;

b) conseiller d'Etat chargé des systèmes d'information et de communication : le conseiller d'Etat chargé du département auquel est rattaché l'office cantonal[5];
c) département : un département de l'administration cantonale ou la chancellerie d'Etat;
d) office : un office, une direction ou un service de l'administration cantonale, à l'exception de l'office cantonal[5];
e) service : un moyen de fournir de la valeur à des offices bénéficiaires en facilitant les résultats que les offices bénéficiaires veulent obtenir sans avoir la propriété des coûts ou des risques spécifiques;
f) socle des systèmes d'information et de communication : l'ensemble des ressources matérielles et immatérielles communes aux systèmes d'information et de communication de l'administration cantonale, à savoir notamment de l'ensemble :
   1° des infrastructures informatiques et de télécommunication,
   2° des plateformes logicielles communes,
   3° des référentiels et des données de base partagés,
   4° des normes et standards en matière de technologies de l'information et de la communication;[7]
g) sécurité de l'information : la protection de la confidentialité, de l'intégrité et de la disponibilité de l'information – en outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées;[7]
h) politique de sécurité de l'information : les intentions et dispositions générales relatives à la sécurité de l'information formellement exprimées par l'Etat de Genève;[7]
i) maître de fichiers : l'office qui décide du but et du contenu de fichiers;[7]
j) plan directeur d'un système d'information et de communication (ci-après : plan directeur) : document décrivant comment le système d'information et de communication devrait évoluer, dans un laps de temps défini, pour répondre aux objectifs et besoins de ses parties prenantes, et fournir les services attendus.[7]

Chapitre II Organisation

Section 1 Conseil d'Etat

Art. 4 Cadre politique et réglementaire

[1] Le Conseil d'Etat fixe le cadre politique et réglementaire dans lequel doivent évoluer les systèmes d'information et de communication de l'administration cantonale.

[2] A ce titre, le Conseil d'Etat :
a) définit, notamment au début de chaque législature, ses orientations politiques en matière d'évolution des systèmes d'information et de communication;
b) approuve :
   1° la stratégie des systèmes d'information et de communication de l'administration cantonale,
   2° les conventions spéciales découlant de l'article 2, alinéas 2 et 3,[7]
   3° les règlements en matière de systèmes d'information et de communication,[7]
   4° la politique de sécurité de l'information,[7]
   5° la méthode de priorisation des demandes en matière de systèmes d'information et de communication;[7]
c) détermine les moyens – financiers et en ressources humaines – qu'il entend consacrer aux investissements et au fonctionnement des systèmes d'information et de communication de l'administration cantonale.

Section 2 Office cantonal des systèmes d'information et du numérique[5]

Art. 5 Mission générale

L'office cantonal[5] a pour mission de développer, d'entretenir, d'exploiter et de faire évoluer – avec les départements et offices bénéficiaires – les systèmes d'information et de communication de l'administration cantonale, en adéquation avec les objectifs de politiques publiques du Conseil d'Etat et en conformité avec les dispositions légales.

Art. 6 Missions spécifiques

[1] L'office cantonal[5] est chargé, en collaboration avec les départements et offices ainsi que les organes désignés dans le présent règlement :
a) de l'élaboration, puis de la concrétisation :
   1° de la stratégie des systèmes d'information et de communication de l'administration cantonale,
   2° de la politique de sécurité de l'information;
b) du développement, de l'entretien, de l'exploitation et du retrait des systèmes d'information et de communication de l'administration cantonale;
c) d'élaborer et de gérer les budgets de fonctionnement et les crédits d'investissement relatifs aux systèmes d'information et de communication;
d) d'élaborer et de piloter le système de contrôle interne :

1° des systèmes d'information et de communication de l'administration cantonale, et en particulier,
2° de la sécurité de l'information, en identifiant et en évaluant les risques;

e) d'élaborer les règlements et directives en matière de systèmes d'information et de communication, en particulier dans le domaine de la sécurité de l'information;
f) de préaviser tout projet de loi ou de règlement ayant des conséquences sur les systèmes d'information et de communication;
g) de conduire les projets relatifs aux systèmes d'information et de communication, et d'en gérer le portefeuille;
h) de l'élaboration, puis du suivi des plans directeurs;(3)
i) d'assurer le bon fonctionnement, le cycle de vie technique, la cohérence, l'efficience, la compatibilité et l'interopérabilité des systèmes d'information et de communication;
j) d'inventorier les actifs de l'administration cantonale dans le domaine des systèmes d'information et de communication;
k) de formaliser le niveau de ses services, pour répondre aux besoins des offices, mais dans la limite des ressources à disposition, puis d'en suivre les modalités d'exécution;
l) de veiller à l'utilisation de normes et standards reconnus;
m) d'organiser le support et de participer à la formation des utilisatrices et des utilisateurs relativement au socle des systèmes d'information et de communication;
n) de développer des synergies avec des partenaires publics et privés dans le domaine des systèmes d'information et de communication.

2 Par une veille stratégique, sociétale et technologique continue, l'office cantonal(5) se donne les moyens d'anticiper les évolutions futures.

Art. 7 Personnel

1 L'office cantonal(5) regroupe l'ensemble des ressources humaines de l'administration cantonale dans les domaines :

a) des services en matière de systèmes d'information et de communication;
b) des technologies de l'information et de la communication.

2 Il s'agit des personnes dont tout ou partie des activités se rapportent notamment aux fonctions suivantes :

a) directeur / responsable de systèmes d'information et/ou de communication;
b) directeur / responsable informatique / télécommunication;
c) directeur / chef de projet en systèmes d'information et de communication;
d) architecte ou urbaniste en systèmes d'information et de communication;
e) développeur;
f) programmeur;
g) analyste-programmeur;
h) intégrateur d'application;
i) ingénieur en informatique / en télécommunication;
j) administrateur de base de données / systèmes / de réseaux;
k) technicien en informatique / en télécommunication; et
l) administrateur / concepteur / développeur de site web (à l'exclusion des activités directement liées à la communication ou d'utilisation des outils mis en place),

quelle que soit la nature de leur relation avec l'Etat (fonctionnaire, employé, agent spécialisé, auxiliaire, apprenti, stagiaire, sous contrat de location de services, sous mandat, etc.).

3 Les activités décentralisées doivent se résumer à du support de proximité.

4 Le cahier des charges du personnel décentralisé doit prévoir un lien fonctionnel avec l'office cantonal(5).

5 Ce lien doit être formalisé conjointement par le département ou l'office concerné et l'office cantonal(5), en particulier avant toute démarche de recrutement de personnel.

Art. 8 Sécurité de l'information

1 L'office cantonal(5) :

a) prend, conjointement avec les maîtres de fichiers, toutes les mesures appropriées pour :
1° préserver la sécurité de l'information de l'administration cantonale, et
2° appliquer les dispositions de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (ci-après : la loi sur l'information);
b) sépare, au sein de son organisation, les tâches normatives et de contrôle de la sécurité de l'information, de celles liées à sa mise en œuvre opérationnelle.

2 Seuls la Cour des comptes, le service d'audit interne de l'Etat de Genève et l'office cantonal(5) disposent de l'autorité pour réaliser ou mandater des audits relativement à la sécurité de l'information.(1)

Art. 9 Mandats externes et sous-traitance

[1] L'office cantonal[5] peut fournir des services à des bénéficiaires extérieurs à l'administration cantonale, au travers de conventions prévoyant son indemnisation sous la forme financière ou sous la forme de subvention pour prestations en nature (subvention non monétaire), conformément à la loi sur les indemnités et les aides financières, du 15 décembre 2005.

[2] A l'inverse, l'office cantonal[5] peut sous-traiter tout ou partie de certains de ses services.

[3] Il en assume dans ce cas la responsabilité vis-à-vis des départements et offices bénéficiaires.

[4] Les offices et départements ne peuvent proposer à des tiers, notamment à l'extérieur de l'administration cantonale, des services fournis par l'office cantonal[5] ou ses sous-traitants sans l'accord préalable de celui-ci.

Section 3 Organisation départementale

Art. 10 Offices

[1] En matière de systèmes d'information et de communication, les offices sont chargés :

a) de l'utilisation efficiente des ressources et des services fournis par l'office cantonal[5], notamment en désignant un ou plusieurs répondants bureautiques au sein de leur organisation;
b) de la maîtrise des fonctionnalités des applications spécifiques à leur domaine, notamment en désignant un ou plusieurs répondants applicatifs au sein de leur organisation;
c) de l'application et du contrôle au sein de leur organisation :
   1° de la législation, en particulier en matière de droits d'auteur et de protection des données,
   2° de la réglementation et des directives cantonales, dont le présent règlement,
   3° de la politique de la sécurité de l'information et des directives y relatives,
   4° des conventions et des contrats;
d) de l'expression de leurs besoins, en évitant toute marque de produit ou considération technique, sauf lorsqu'aucun autre moyen de description suffisamment précis n'existe;
e) de la rédaction de l'exposé des motifs des projets de loi pour les crédits d'ouvrage, conjointement avec l'office cantonal[5] et la direction départementale chargée de l'organisation et de la sécurité de l'information;[3]
f) dans le cadre des projets :
   1° de la documentation de leurs objectifs, de leur organisation, de leurs processus, de leurs activités et des services attendus, ainsi que de tout autre élément de formalisation « métier » requis par l'office cantonal[5] pour mener à bien ses travaux,
   2° de l'anticipation et de la mise en œuvre des changements au sein de leur organisation,
   3° des « tests utilisateurs » ou d'acceptation des services;
g) lorsqu'un projet exécuté à leur demande induit des charges de fonctionnement supplémentaires à l'office cantonal[5], de la recherche de toute compensation possible liée aux gains métier obtenus par le service fourni par l'office cantonal[5].

[2] En tant que maîtres de fichiers, les départements et les offices :

a) sont responsables de la qualité de leurs données;
b) définissent :
   1° les besoins en matière de sécurité de l'information,
   2° les autorisations et les contrôles d'accès à leurs données;
c) veillent à l'application de la loi sur l'information;
d) peuvent édicter des règles et mesures de sécurité spécifiques, conformément à la politique de sécurité de l'information ainsi que des directives y relatives, et après validation par le responsable LIPAD du département et l'office cantonal[5].

[3] L'office cantonal[5] formalise, d'entente avec chaque office, une convention de niveau de service.[3]

Art. 11[3] Direction départementale chargée de l'organisation et de la sécurité de l'information

[1] Chaque département désigne une direction départementale chargée de l'organisation et de la sécurité de l'information (ci-après : la direction départementale).

[2] En matière de systèmes d'information et de communication, la direction départementale a pour missions :

a) de prendre en compte les objectifs de politique publique sur l'organisation, la circulation et le traitement de l'information au sein du département;
b) d'élaborer, puis de concrétiser des stratégies « métier » ou départementales :
   1° selon les règles et l'organisation de son département,
   2° en partenariat avec les offices et l'office cantonal[5],
   3° dans le cadre de la stratégie des systèmes d'information et de communication de l'administration cantonale;
c) de coordonner et de promouvoir au sein du département :
   1° le processus de gouvernance relatif à la priorisation des besoins, tel que spécifié à l'article 28,
   2° les projets conduits par l'office cantonal[5],
   3° les services fournis par l'office cantonal[5];
d) de tenir à jour ses plans directeurs, avec les différents offices de son département et l'office cantonal[5];

e) de communiquer à l'office cantonal[5]:
   1° de manière anticipée, l'évolution des besoins de son département et en particulier les modifications légales ainsi que les décisions des autorités politiques qui nécessiteront une intervention de l'office cantonal[5],
   2° les problèmes majeurs ou récurrents rencontrés par les différents offices de son département;
f) de conseiller et d'aider les différents offices de son département dans les activités décrites à l'article 10, en particulier, pour l'expression des besoins et l'accompagnement aux changements;
g) de porter les intérêts du département au collège spécialisé, en référence aux articles 20 et suivants;
h) de promouvoir et de mettre en application au sein de son département les recommandations du collège spécialisé.

Art. 12 Responsable départemental de la sécurité de l'information

1 Chaque département désigne, au sein de la direction départementale, une personne responsable de la sécurité de l'information au sein du département (ci-après : responsable départemental de la sécurité de l'information).[3]

2 Le responsable départemental de la sécurité de l'information a pour missions :[3]

a) au sein de son département :
   1° de conduire la mise en œuvre de la politique de sécurité de l'information et des directives y relatives,
   2° le cas échéant, d'édicter des directives en matière de sécurité de l'information propres aux activités du département, conformément à la politique de sécurité de l'information ainsi que des directives y relatives, et après validation par le responsable LIPAD du département et l'office cantonal[5],
   3° de veiller et de contrôler l'application des lois et des normes en matière de sécurité de l'information,
   4° de contribuer avec l'office cantonal[5] à la sensibilisation du personnel à la sécurité de l'information et à la protection des données,
   5° d'aider les maîtres de fichiers dans la définition de leurs besoins en matière de sécurité de l'information et des autorisations d'accès aux données ainsi que dans l'application de la loi sur l'information,
   6° d'identifier les risques et contrôles relatifs aux systèmes d'information et de communication avec l'office ou la personne chargée de la gestion des risques et de la qualité du département, en collaboration avec l'office cantonal;[6]
b) de communiquer à l'office cantonal[5] :
   1° la définition des besoins du département en matière de sécurité de l'information, sur la base d'une analyse des risques,
   2° les failles et faiblesses en matière de sécurité de l'information constatées dans son département, en particulier lors d'audits;[3]
c) de collaborer avec l'office cantonal[5] et l'ensemble des parties prenantes pour que les mesures correctrices soient apportées, en tenant compte des risques encourus;
d) de contribuer à l'organisation des audits en matière de sécurité de l'information menés par l'office cantonal[5].

Art. 13 Centres de compétence

1 Un centre de compétence a pour mission d'assurer – en collaboration avec l'office cantonal[5] – la constitution, la disponibilité et la valorisation des données et des savoirs relatifs à un système d'information spécifique, mais utilisé par plusieurs offices.

2 Son champ de compétence est défini par :

a) un domaine fonctionnel, correspondant par exemple à une politique publique ou à une catégorie de prestations;
b) un périmètre organisationnel, par exemple limité à un département ou au contraire interdépartemental.

3 Le centre de compétence valide les expressions des besoins dans son domaine fonctionnel des offices appartenant à son périmètre organisationnel.

4 Un centre de compétence est chargé, pour son système d'information spécifique :

a) du contrôle de la qualité des données;
b) d'organiser ou de pourvoir à l'information, la formation et l'assistance de l'ensemble des utilisateurs, sous l'angle « métier »;
c) d'élaborer les processus et les règles d'utilisation, puis de veiller à leur application;
d) de fournir aux maîtres de fichiers les moyens de contrôler régulièrement la validité des accès à leurs données;
e) de fixer les paramètres fonctionnels, dans la mesure où ils n'altèrent pas le bon fonctionnement ni la sécurité du système d'information et de communication;
f) d'élaborer les tableaux de bord et autres statistiques nécessaires au pilotage fonctionnel;
g) de qualifier les incidents, puis de les signaler à l'office cantonal[5] et de contribuer à leur résolution;
h) de recueillir, d'analyser et d'exprimer les besoins d'évolution, puis de participer aux projets résultants;
i) de conduire les « tests utilisateurs » ou d'acceptation;

j) de tenir à jour son plan directeur, avec les offices concernés et l'office cantonal(5).

5 Les départements s'organisent pour désigner leurs propres centres de compétence.

6 En revanche, les demandes pour la création d'un centre de compétence interdépartemental sont adressées par le département au directeur général des systèmes d'information et du numérique, en vue d'une prise de décision par le collège des secrétaires généraux.(7)

Section 4(7) Organe de gouvernance des systèmes d'information et de communication

Art. 14(7) Mission générale

1 Le collège des secrétaires généraux est l'organe de gouvernance des systèmes d'information et de communication de l'administration cantonale.

2 Il priorise les demandes de création et d'évolution substantielle des services de l'administration cantonale dans le domaine des systèmes d'information et de communication.

Art. 15(7) Missions spécifiques

Le collège des secrétaires généraux :

a) convie le directeur général des systèmes d'information et du numérique lorsqu'il traite un sujet relatif aux systèmes d'information et au numérique;
b) sur proposition du directeur général des systèmes d'information et du numérique, préavise à l'intention du Conseil d'Etat;
c) sur proposition du directeur général des systèmes d'information et du numérique, approuve les directives en matière de systèmes d'information et de communication, y compris dans le domaine de la sécurité de l'information.

[Art. 16, 17, 18](7)

Art. 19(3)

Section 5 Collège spécialisé des systèmes d'information

Art. 20(3) Missions

Le collège spécialisé a pour missions :

a) d'être la principale plateforme d'échange de concertation, d'information et de collaboration entre l'office cantonal(5) et les départements, afin notamment de contribuer à :
   1° la cohérence des systèmes d'information et de communication de l'ensemble de l'administration cantonale,
   2° l'anticipation de l'évolution des besoins de l'administration cantonale,
   3° l'analyse des impacts des initiatives de changements transversaux concernant les systèmes d'information et de communication de l'administration cantonale;
b) d'être le garant de la cohérence et de l'harmonisation des processus des offices ainsi que de la promotion de l'information et de référentiels communs, en se basant sur les meilleures pratiques et sur une démarche d'innovation;
c) de contribuer avec l'office cantonal(5) à :
   1° la formalisation de la stratégie des systèmes d'information et de communication de l'administration cantonale, et à sa mise en œuvre, en particulier au sein des départements,
   2° l'expression de besoins généraux, puis à leur mise en place,
   3° l'élaboration des règlements et directives en matière de systèmes d'information et de communication,
   4° l'élaboration, puis au suivi des plans directeurs.

Art. 21 Composition

1 Le collège spécialisé est composé :

a) pour chaque département, du responsable de la direction départementale;(3)
b) d'un représentant pour chacun des pouvoirs spécifiés à l'article 2, alinéa 2, si la convention spéciale le prévoit;
c) d'un représentant de l'office cantonal(5), désigné par le directeur général des systèmes d'information et du numérique(4);
d) du directeur général adjoint de l'office cantonal(5);
e) du directeur général des systèmes d'information et du numérique(4).

2 Le collège spécialisé est présidé par le directeur général des systèmes d'information et du numérique(4); il est remplacé par le directeur général adjoint de l'office cantonal(5).

3 Un membre absent peut se faire remplacer par un autre représentant de son organisation.

4 Sont systématiquement invités aux séances du collège spécialisé, mais s'abstiennent lors des prises de décision :
a) les directeurs des Archives d'Etat de Genève et de l'office cantonal de la statistique;
b) les présidents des autres collèges spécialisés.

5 Le collège spécialisé invite toute autre personne utile à ses travaux, au gré des sujets à l'ordre du jour.

Art. 22 Groupe de travail

1 Le collège spécialisé peut mettre sur pied des groupes de travail pour étudier et ainsi anticiper l'évolution de la demande au sein de l'administration cantonale en matière de systèmes d'information et de communication, en évitant néanmoins toute considération technique, sauf lorsqu'aucun autre moyen de description suffisamment précis n'existe.

2 Le résultat de ces travaux fait l'objet d'expressions des besoins, transmises à l'office cantonal(5) dans le cadre du processus de gouvernance relatif à la priorisation des besoins, tel que spécifié à l'article 28.

Art. 23(3)

Section 6 Comité de sécurité de l'information

Art. 24 Mission

Le comité a pour mission :
a) d'être la principale plateforme d'échange de concertation, d'information et de collaboration entre l'office cantonal(5) et les départements dans le domaine de la sécurité de l'information, afin notamment de contribuer à :
   1° renforcer la sécurité de l'information au sein de l'administration cantonale, à un niveau conforme aux risques encourus,
   2° l'anticipation de l'évolution des besoins de l'administration cantonale;
b) de contribuer avec l'office cantonal(5) à :
   1° la formalisation de la politique de sécurité de l'information,
   2° l'expression de besoins généraux, puis à leur mise en place,
   3° l'élaboration des règlements et directives en matière de sécurité de l'information,
   4° la cartographie des risques relatifs aux systèmes d'information et de communication,
   5° la gestion du système de contrôle interne des systèmes d'information et de communication, pour la part consacrée à la sécurité de l'information.

Art. 25 Composition

1 Le comité est composé :
a) pour chaque département, du responsable départemental de la sécurité de l'information;
b) d'un membre de chaque pouvoir qui dispose d'une convention spéciale, en référence à l'article 2, alinéa 2, si la convention spéciale le prévoit;
c) de 2 représentants de l'office cantonal(5), désignés par le directeur général des systèmes d'information et du numérique(4);
d) du directeur chargé de la sécurité de l'information à l'office cantonal(5).

2 Un membre absent peut se faire remplacer par un autre représentant de son organisation.

3 Le comité est présidé par le directeur chargé de la sécurité de l'information à l'office cantonal(5).

4 Sont systématiquement invités aux séances du comité, mais s'abstiennent lors des prises de décision :
a) les responsables de la sécurité de l'information de la police et de l'informatique pédagogique;
b) le président du groupe interdépartemental des responsables LIPAD, ou une personne désignée par ledit groupe;
c) le directeur général des systèmes d'information et du numérique(4).

5 Le comité invite toute autre personne utile à ses travaux, au gré des sujets à l'ordre du jour.

Art. 26 Groupe de travail

1 Le comité peut mettre sur pied des groupes de travail pour étudier et ainsi anticiper l'évolution de la demande au sein de l'administration cantonale en matière de systèmes d'information et de communication, en évitant néanmoins toute considération technique, sauf lorsqu'aucun autre moyen de description suffisamment précis n'existe.

2 Le résultat de ces travaux fait l'objet d'expressions des besoins, transmises à l'office cantonal(5) dans le cadre du processus de gouvernance relatif à la priorisation des besoins, tel que spécifié à l'article 28.

Art. 27(3)

Chapitre III Gouvernance

Section 1 Priorisation des besoins

Art. 28 Principes

[1] Les besoins de l'administration cantonale en matière de systèmes d'information et de communication sont priorisés par le collège des secrétaires généraux, en adéquation avec :[7]

a) les objectifs de politiques publiques et les décisions du Conseil d'Etat;
b) la stratégie des systèmes d'information et de communication de l'administration cantonale ainsi que la politique de sécurité de l'information, validées par le Conseil d'Etat;
c) les dispositions légales et réglementaires,

selon une méthode validée par le Conseil d'Etat, sur proposition du conseiller d'Etat chargé des systèmes d'information et de communication.

[2] Le processus de priorisation des besoins de l'administration cantonale en matière de systèmes d'information et de communication fait l'objet d'une directive validée par le collège des secrétaires généraux.[7]

[3] Sont prises en charge directement par l'office cantonal[5], selon son appréciation de l'opportunité et dans la limite des ressources humaines et financières à sa disposition :

a) la concrétisation des besoins :
   1° correspondant à une demande de service déjà industrialisée,
   2° relatifs aux actifs mutualisés,[7]
   3° dont le coût est en dessous d'une valeur-seuil précisée dans la directive validée par le collège des secrétaires généraux, sur proposition du directeur général des systèmes d'information et du numérique;[7]
b) la maintenance des systèmes d'information et de communication.[3]

[4] Dans tous les cas, l'office cantonal[5] prend sans délai les mesures adéquates pour remédier aux urgences avérées (catastrophe naturelle, incendie, dégâts d'eau, faille de sécurité majeure, etc.) et informe immédiatement le conseiller d'Etat chargé des systèmes d'information et de communication.

Section 2 Planification et réalisation des projets

Art. 29 Planification des projets

[1] Sur la base des priorités édictées par le collège des secrétaires généraux, l'office cantonal :[7]

a) met à jour le portefeuille de ses services;
b) planifie la réalisation des projets pour répondre aux demandes selon les disponibilités des ressources humaines et financières à sa disposition, et d'entente avec les offices demandeurs;
c) communique aux offices demandeurs et aux offices responsables de l'organisation de l'information au sein des départements le statut de leurs expressions de besoins.

[2] Il est toutefois admis qu'un projet peut s'intercaler entre 2 projets plus importants pour maximiser l'efficience du plan de charge de l'office cantonal[5].

Art. 30 Réalisation des projets

[1] Le projet pour concrétiser une expression de besoins ne débute que lorsque toutes les ressources humaines et financières nécessaires sont assurées, pour toute la durée du cycle de vie du service concerné.

[2] En particulier, la concrétisation d'un crédit d'ouvrage ne débute que lorsque les ressources nécessaires à son exploitation et à son entretien sont intégrées au budget de fonctionnement, le cas échéant en retirant d'autres services fournis par l'office cantonal[5].

Section 3 Conduite des projets

Art. 31 Méthode de gestion de projet

Le directeur général des systèmes d'information et du numérique[4] :

a) spécifie, après concertation avec le collège spécialisé, la méthode standard de gestion de projet dans le domaine des systèmes d'information et de communication, qui doit prendre en compte les besoins et les particularités de l'administration cantonale;
b) précise les modalités d'application de la méthode.

Art. 32 Gouvernance des projets

[1] Les projets prévoient la mise en place d'un comité de pilotage, dont l'organisation est adaptée à la taille du projet.

[2] Dans tous les cas, le comité de pilotage est composé :

a) d'une personne désignée par les départements ou les offices bénéficiaires, qui assume le rôle de « mandant » – dépositaire des besoins et responsable des ressources qui appartiennent au domaine spécialisé;
b) d'une personne désignée par le directeur général des systèmes d'information et du numérique[4], qui assume le rôle de « sponsor » – responsable des ressources humaines, financières et matérielles en matière de systèmes d'information et de communication mises à disposition du projet.

3 Le comité de pilotage est complété par :
a) le chef de projet;
b) un représentant de la direction départementale, qui assume le rôle de gestionnaire de la qualité et des risques.[3]

4 La composition du reste du comité de pilotage est fixée d'entente entre le mandant et le sponsor, en veillant à respecter la méthode de gestion de projet.

5 Le comité de pilotage est présidé par le mandant.

6 Aussi bien le mandant que le sponsor disposent d'un droit de veto en cours de projet, en particulier s'ils ne disposent plus de ressources humaines, financières ou matérielles en suffisance pour réaliser le projet ou si les risques ne sont pas suffisamment maîtrisés.

Art. 33 Conduite des projets

1 Le chef de projet est désigné par l'office cantonal[5], en principe dans son organisation.

2 Le choix est validé par le mandant.

3 Lorsque le périmètre d'un projet dépasse substantiellement la mise en place d'un système d'information et de communication :
a) il est transformé en programme et les grands domaines qui le composent deviennent des projets à part entière, et
b) les projets correspondant au système d'information et de communication sont organisés selon les dispositions de la présente section.[3]

Section 4 Sécurité de l'information

Art. 34 Principes

Les principes directeurs de la sécurité de l'information 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.

Art. 35 Elaboration d'une politique de sécurité de l'information

1 Les principes directeurs de la sécurité de l'information sont déclinés en objectifs et en mesures générales dans une « politique de sécurité de l'information ».

2 La politique de sécurité de l'information doit notamment :
a) constituer le cadre de gouvernance, de référence et de cohérence de la sécurité de l'information au sein de l'administration cantonale;
b) être conforme à la législation et à la réglementation en vigueur;
c) s'appuyer sur des normes internationales reconnues;
d) être en adéquation avec les besoins de l'administration cantonale;
e) définir les responsabilités dans le domaine de la gestion de la sécurité de l'information, traitant en particulier de la remontée d'incidents de sécurité;
f) présenter les besoins de communication, de formation et de sensibilisation.

3 La politique de sécurité de l'information définit également :
a) les règles pour sa mise en œuvre;
b) les mesures et les contrôles;
c) les règles de révision et de mise à jour.

4 Elle est publiée à l'intention de l'ensemble des utilisateurs des systèmes d'information et de communication de l'administration cantonale.

Chapitre IV Dispositions finales et transitoires

Art. 36 Clause abrogatoire

Sont abrogés :

a) le règlement concernant la protection des applications et des systèmes informatiques dans l'administration cantonale, du 5 avril 2000;
b) le règlement du centre des technologies de l'information, du 22 décembre 2004;
c) le règlement sur l'organisation de la gestion des systèmes d'information, du 6 avril 2011.

Art. 37 Entrée en vigueur

Le présent règlement entre en vigueur le lendemain de sa publication dans la Feuille d'avis officielle.

RSG	Intitulé	Date d'adoption	Entrée en vigueur
B 4 23.03	**R sur l'organisation et la gouvernance des systèmes d'information et de communication**	26.06.2013	03.07.2013
Modifications :			
1.	***n.t.*** : 8/2, 12/2b 2°	28.05.2014	01.06.2014
2.	***n.t.*** : rectification selon 7C/1, B 2 05 (2/1)	01.09.2014	01.09.2014
3.	***n.*** : 3/4k, 10/3; ***n.t.*** : 6/1h, 10/1e, 11, 12/1, 12/2 phr. 1, 12/2b 2°, 13/4j, 18/5, 20, 21/1a, 28/3b, 32/3b, 33/3; ***a.*** : 12/3, 12/4, 19, 23, 27, 38, 39	16.05.2018	23.05.2018
4.	***n.t.*** : rectification selon 7C/1, B 2 05 (2/2 phr. 1, 2/3, section 2 du chap. II, 16/1c, 16/2, 17/4, 21/1c, 21/1e, 21/2, 25/1c, 25/4c, 28/3a 3°, 31 phr. 1, 32/2b)	04.09.2018	04.09.2018
5.	***n.t.*** : rectification selon 7C/1, B 2 05 (2/1, 2/2 phr. 1, 2/3, 3/4b, 3/4f, section 2 du chap. II, 5, 6/1 phr. 1, 6/2, 7/1 phr. 1, 7/4, 7/5, 8/1 phr. 1, 8/2, 9/1, 9/2, 9/4, 10/1a, 10/1e, 10/1f 1°, 10/1g, 10/2d, 10/3, 11/2b 2°, 11/2c 2°, 11/2c 3°, 11/2d, 11/2e phr. 1, 11/2e 1°, 12/2a 2°, 12/2a 4°, 12/2a 6°, 12/2b phr. 1, 12/2c, 12/2d, 13/1, 13/4g, 13/4j, 15/a, 18/1b, 18/5, 20/a phr. 1, 20/c phr. 1, 21/1c, 21/1d, 21/2, 22/2, 24/a phr. 1, 24/b phr. 1, 25/1c, 25/1d, 25/3, 26/2, 28/3 phr. 1, 28/4, 29/1 phr.1, 29/2, 30/2, 33/1)	15.11.2018	15.11.2018
6.	***n.t.*** : 12/2a 6°	28.08.2019	04.09.2019
7.	***n.t.*** : 3/3, 13/6, section 4 du chap. II, 14, 15, 28/1 phr. 1, 28/2, 28/3a 2°, 28/3a 3°, 29/1 phr. 1; ***a.*** : 3/4f (*d.* : 3/4g-k >> 3/4f-j), 4/2b 2° (*d.* : 4/2b 3°-6° >> 4/2b 2°-5°), 13/7, 16, 17, 18	04.11.2020	11.11.2020
8.	***n.t.*** : rectification selon 7C/1, B 2 05 (2/1)	14.11.2023	14.11.2023