Version DSJS - Consultation Automne 2022

Règlement sur la sécurité de l'information (RSI)

du ...

Actes concernés (numéros RSF):

Nouveau: **???.???**
Modifié(s): 122.0.12 | 122.0.31 | 122.0.51 | 122.96.11 | 184.16
Abrogé(s): 17.15

Le Conseil d'Etat du canton de Fribourg

Vu l'article 118 de la Constitution du canton de Fribourg du 16 mai 2004;
Sur la proposition de la Direction de la sécurité, de la justice et du sport,

Arrête:

I.

1 Dispositions générales

Art. 1 Objet

[1] Le présent règlement vise à assurer la sécurité des informations et des systèmes d'information de l'administration cantonale.

[2] A cette fin, il:

a) met en place une organisation dédiée à la sécurité de l'information;

b) institue le ou la délégué-e à la sécurité de l'information (ci-après: le ou la délégué-e SI);

c) prescrit l'élaboration d'une politique générale de sécurité de l'information (ci-après: la PGSI) pour l'administration cantonale;

d) fixe un socle de règles communes et minimales en matière de sécurité de l'information;

e) énonce certains principes relatifs à la sécurité des moyens informatiques dans la mesure où ils servent à la sécurité de l'information.

Art. 2 Champ d'application

[1] Le présent règlement s'applique à l'ensemble des Directions et des unités administratives de l'administration cantonale, ainsi qu'aux particuliers et aux organes d'institutions privées, lorsqu'ils accomplissent des tâches de droit public.

[2] Les unités autonomes au sens de l'article 2 al. 2 de l'ordonnance sur la gouvernance de la digitalisation et des systèmes d'information de l'Etat y sont également soumises. Elles fixent leur propre organisation et nomment leurs propres personnes responsables de la sécurité de l'information.

[3] Le présent règlement est applicable au Grand Conseil ainsi qu'au pouvoir judiciaire dans la mesure où une convention passée avec le Conseil d'Etat le prévoit.

[4] Les dispositions spéciales fédérales ou cantonales en matière de sécurité de l'information sont réservées.

Art. 3 Application aux communes

[1] Lorsque les communes accèdent à des systèmes d'information cantonaux, les mesures de sécurité à respecter sont définies au moyen d'une convention. L'article 20 est réservé.

Art. 4 Définitions

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

a) sécurité de l'information: l'ensemble des normes, mesures, procédures, stratégies, directives, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies destinées à renforcer le niveau de sécurité des informations détenues et traitées par les organes de l'administration cantonale;

b) système d'information: un ensemble organisé de ressources pour créer, collecter, grouper, classifier, traiter et diffuser de l'information à l'aide de moyens informatiques;

c) moyen informatique: un ensemble de ressources matérielles et logicielles constituées de technologies de l'information et de la communication;

d) journalisation: l'enregistrement, à des fins de contrôle ou de reconstitution, de tout ou partie des activités effectuées dans un système d'information;

e) incident de sécurité: un ou plusieurs événements indésirables ou inattendus liés à la sécurité de l'information et présentant une forte probabilité d'altérer la fiabilité et la qualité des informations qu'une unité administrative traite, de compromettre la poursuite de ses activités et/ou de constituer une menace pour des personnes à l'intérieur ou à l'extérieur de l'administration cantonale;

f) procédure d'appel: le mode de communication automatisée des données par lequel les destinataires, en vertu d'une autorisation du responsable du fichier/traitement, décident de leur propre chef, sans contrôle préalable, du moment et de l'étendue de la communication.

Art. 5 Responsabilités

[1] Tout organe qui détient et traite des informations est responsable de leur sécurité, en particulier leur intégrité, leur disponibilité, leur confidentialité, leur traçabilité, leur pérennité et leur résilience.

[2] Lorsque plusieurs organes traitent conjointement des informations, la répartition de leurs responsabilités est fixée dans une convention écrite, à moins qu'elle ne résulte expressément d'une disposition légale.

[3] En outre, le Service de l'informatique et des télécommunications est responsable de la sécurité des moyens informatiques conformément à l'article 13.

2 Organisation

2.1 Organes stratégiques

Art. 6 Conseil d'Etat

[1] Le Conseil d'Etat a les attributions suivantes:

a) il définit les orientations stratégiques de l'Etat en matière de sécurité de l'information;

b) il adopte la politique générale de sécurité de l'information de l'Etat;

c) il propose dans le cadre du processus budgétaire annuel les moyens nécessaires à la sécurité de l'information;

d) il approuve l'engagement du ou de la délégué-e SI.

Art. 7 Direction de la sécurité, de la justice et du sport (DSJS)

[1] La DSJS a les attributions suivantes:

a) elle porte les projets en matière de sécurité de l'information au sein de l'administration cantonale;

b) elle préavise à l'intention du Conseil d'Etat le contenu et les modifications successives de la PGSI;

c) elle informe le Conseil d'Etat de toutes les affaires importantes en lien avec la sécurité de l'information;

d) elle fixe des orientations portant sur les principes ou les pratiques à favoriser en matière de sécurité de l'information;

e) elle autorise le ou la délégué-e SI à mener des actions ciblées dans le but d'évaluer et/ou d'améliorer le niveau de l'administration cantonale en matière de sécurité de l'information;

f) elle approuve les directives, les recommandations et les modèles de chartes élaborées par le ou la délégué-e SI;

g) elle confie, sur recommandation du ou de la délégué-e SI, des mandats d'audits à des tiers publics ou privés pour évaluer le niveau de sécurité de l'information au sein de l'administration.

Art. 8 Conférence des secrétaires généraux (CSG)

[1] La CSG a les attributions suivantes:

a) elle coordonne les initiatives en matière de sécurité de l'information au sein de l'administration ainsi que leur mise en œuvre;

b) elle préavise les propositions de budget des Directions spécifiques à la sécurité de l'information;

c) elle arbitre les éventuels désaccords entre le ou la délégué-e SI et une Direction.

[2] La personne représentant la DSJS au sein de la CSG assure la préparation et le suivi des dossiers dans le domaine de la sécurité de l'information.

2.2 Organes opérationnels

Art. 9 Directions du Conseil d'Etat

[1] Les Directions ont les attributions suivantes:

a) elles s'assurent que les unités administratives qui leur sont subordonnées appliquent les dispositions du présent règlement et des autres textes adoptés conformément à celui-ci;

b) elles établissent leurs besoins budgétaires spécifiques à la sécurité de l'information;

c) elles arbitrent les éventuels désaccords entre le ou la délégué-e SI et une unité administrative subordonnée.

d) elles veillent au besoin de formation et de sensibilisation du personnel qui leur est rattaché.

[2] En outre, chaque Direction désigne au moins un correspondant ou une correspondante à la sécurité de l'information. En cette qualité, cette personne:

a) conseille et aide les unités administratives dans la mise en oeuvre de leurs obligations en vertu du présent règlement;

b) s'assure auprès des unités administratives qu'elles ont mis en place des mesures de sécurité adaptées et que ces mesures soient appliquées;

c) est l'interlocuteur ou l'interlocutrice principal-e au sein de la Direction pour toutes les questions relatives à la sécurité de l'information;

d) fait partie du réseau des correspondants et correspondantes à la sécurité de l'information.

[3] La fonction de correspondant ou correspondante à la sécurité de l'information peut être attribuée à la personne désignée comme correspondant ou correspondante à la protection des données.

Art. 10 Délégué-e à la sécurité de l'information – Tâches

[1] Le ou la délégué-e SI accomplit ses tâches de manière transversale pour l'ensemble des Directions.

[2] En particulier, il ou elle:

a) conseille le Conseil d'Etat, les Directions et les unités administratives sur les questions liées à la sécurité de l'information et les mesures à prendre dans ce domaine;

b) élabore la PGSI et d'autres directives en matière de sécurité de l'information, veille à leur mise en oeuvre et en coordonne l'exécution;

c) fait rapport régulièrement à la DSJS sur l'état de situation de la sécurité de l'information dans l'administration cantonale, les menaces existantes et nouvelles, ainsi que les mesures à prendre pour y faire face;

d) organise des audits sur la sécurité de l'information dans les limites de ses compétences;

e) participe à la conception du dispositif de gestion des incidents;

f) organise conjointement avec le ou la préposé-e à la protection des données les séances du réseau des correspondants et correspondantes à la sécurité de l'information et à la protection des données;

g) accomplit les autres tâches que lui confie la DSJS dans le domaine de la sécurité de l'information.

[3] Le ou la délégué-e SI est intégré-e au secrétariat général de la DSJS. Toutefois, dans l'exercice des tâches qu'il ou elle assume pour l'ensemble de l'administration, le ou la délégué-e SI est soumis aux instructions du Conseil d'Etat. L'article 51 al. 2 de la loi sur l'organisation du Conseil d'Etat et de l'administration est applicable par analogie.

Art. 11 Délégué-e à la sécurité de l'information – Collaboration

[1] Dans l'accomplissement de ses tâches, le ou la délégué-e SI collabore et échange des informations avec:

a) la Conférence des secrétaires généraux;

b) la ou les personnes responsables de la sécurité informatique au sein du Service de l'informatique et des télécommunications (ci-après: le SITel);

c) les personnes responsables de la sécurité de l'information de l'administration et celles des unités autonomes au sens de l'article 2 al. 2;

d) les responsables du fichier/traitement;

e) le ou la préposé-e à la protection des donnée sur toutes les questions de sécurité concernant le traitement de données personnelles;

f) les autres autorités en Suisse chargées de la sécurité de l'information.

[2] Le ou la délégué-e SI recueille les informations nécessaires à l'accomplissement de ses tâches. Il ou elle peut notamment demander des renseignements, exiger la production de documents, procéder à des inspections et se faire présenter des systèmes d'information. Le secret de fonction ne peut lui être opposé.

Art. 12 Réseau des correspondants et correspondantes à la sécurité de l'information et à la protection des données

[1] Le réseau est un comité interdisciplinaire réunissant dans la mesure du possible des compétences juridiques, techniques et managériales.

[2] Le réseau a les tâches suivantes:

a) il promeut l'exécution harmonisée du présent règlement et de la PGSI au sein de l'administration cantonale;

b) il participe à l'échange d'informations, notamment sur la gestion des risques, sur les meilleures pratiques et sur les problèmes et les incidents dans le domaine de la sécurité de l'information et de la protection des données;

c) il assiste le ou la délégué-e SI dans l'élaboration des différents documents qu'il ou elle doit rédiger en vertu du présent règlement.

[3] Le réseau, présidé par le ou la délégué-e SI, est composé du ou de la préposé-e à la protection des données et d'au moins un représentant ou une représentante par Direction. Il peut également accueillir des personnes responsables de la sécurité de l'information des unités autonomes au sens de l'article 2 al. 2 et des communes.

2.3 Organes spécialisés

Art. 13 Service de l'informatique et des télécommunications

[1] Le SITel est responsable de la sécurité des moyens informatiques qu'il gère et met à disposition de l'administration cantonale.

Art. 14 Service du personnel et d'organisation

[1] Le Service du personnel et d'organisation organise des cycles de formation au profit du personnel de l'Etat pour développer et renforcer les capacités de l'administration cantonale en matière de sécurité de l'information.

[2] Il bénéficie dans cette tâche du soutien du ou de la délégué-e SI, du ou de la préposé-e à la protection des données et du SITel.

Art. 15 Autorité de la transparence, de la protection des données et de la médiation

[1] Les compétences de conseil et de contrôle de l'Autorité de la transparence, de la protection des données et de la médiation en matière de protection des données personnelles sont réservées.

2.4 Organes-métiers

Art. 16 Unités administratives

[1] Les unités administratives procèdent à une évaluation des risques pertinents de leurs systèmes d'information et prennent les mesures propres à assurer leur sécurité conformément au présent règlement et à la PGSI.

[2] Elles veillent à la formation de leur personnel et vérifient régulièrement l'application, par les collaborateurs et collaboratrices, des mesures prescrites.

[3] L'article 5 al. 3 est réservé.

Art. 17 Utilisateurs et utilisatrices

[1] Les collaborateurs et les collaboratrices qui utilisent des systèmes d'information mis à disposition par l'Etat sont responsables de l'application des mesures prescrites en vertu du présent règlement.

[2] Lorsque les utilisateurs et utilisatrices sont des mandataires non soumis aux dispositions du présent règlement, leurs responsabilités en matière de sécurité sont définies au moyen d'un contrat.

[3] Les utilisateurs et utilisatrices qui, dans l'accomplissement de leurs tâches, constatent des lacunes en matière de sécurité de l'information en informent leur hiérarchie. Celle-ci prend les mesures utiles.

3 Politique générale de sécurité de l'information de l'Etat

Art. 18 Principes

[1] L'Etat se dote d'une politique générale de sécurité de l'information.

[2] Les principes directeurs de la PGSI sont les suivants:

a) la gestion des risques;

b) la préservation du capital informationnel de l'Etat;

c) la préservation des ressources matérielles et immatérielles;

d) la préservation de la continuité des activités de l'administration cantonale;

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

f) l'adéquation avec les besoins de l'administration cantonale.

[3] La PGSI est publiée sur le site Internet de l'Etat.

Art. 19 Contenu

[1] En application des principes directeurs, la PGSI 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 les bonnes pratiques et les normes internationales reconnues;

d) préciser les responsabilités dans le domaine de la gestion de la sécurité de l'information;

e) prévoir des règles concernant l'identification, le suivi et la résolution des incidents;

f) prévoir un plan de continuité pour les activités indispensables au fonctionnement de l'Etat en cas d'incident de sécurité;

g) inclure les besoins en matière de formation et de sensibilisation du personnel.

[2] La PGSI définit également les règles pour sa mise en oeuvre et son contrôle.

[3] La PGSI est mise à jour périodiquement.

Art. 20 Application aux communes

[1] La PGSI est applicable aux communes lorsqu'elles utilisent des systèmes d'information de l'administration cantonale.

Art. 21 Directives sectorielles relatives à la sécurité de l'information

[1] Les Directions et les unités autonomes établissent leurs propres directives relatives à la sécurité de l'information et à la protection des données dans les secteurs où cela leur paraît nécessaire.

[2] Une directive sectorielle peut déroger à la PGSI sur des points spécifiques.

[3] Le ou la délégué-e SI ainsi que le ou la préposé-e à la protection des données sont consultés lors de l'élaboration d'une directive sectorielle.

Art. 22 Chartes de service relatives à la sécurité de l'information

[1] Les unités administratives qui traitent de grandes quantités de données peuvent se doter d'une charte relative à la sécurité de l'information. Elles consultent le correspondant ou la correspondante à la sécurité de l'information et/ou à la protection des données dont ils dépendent.

4 Règles minimales de sécurité

4.1 Principes généraux

Art. 23 Evaluation des risques

[1] L'organe public évalue les risques d'atteintes aux informations qu'il traite du point de vue de la disponibilité, de l'intégrité, de la confidentialité, de la traçabilité, de la pérennité et de la résilience.

[2] Dans son évaluation des risques, l'organe public tient compte des facteurs humains, techniques et juridiques.

Art. 24 Définition des mesures

[1] L'organe public définit, en fonction de l'étendue des risques et du degré de confidentialité des données, les mesures organisationnelles et techniques appropriées, dans le but de réduire les risques; ces mesures peuvent porter aussi bien sur les processus, les personnes, les locaux ainsi que sur le matériel et la sécurité des moyens informatiques.

[2] Les mesures doivent être proportionnées aux circonstances, techniquement adaptées, économiquement supportables et applicables en pratique.

Art. 25 Conception et évolution

[1] Les exigences liées à la sécurité des informations, notamment leurs coûts, doivent être prises en considération dès la conception et lors de l'évolution des systèmes d'information.

Art. 26 Risques résiduels

[1] L'organe public met en évidence et documente les risques qui ne peuvent être réduits ou qui ne peuvent l'être que de manière insuffisante (risques résiduels).

[2] La décision d'assumer ou non les risques résiduels connus appartient au ou à la responsable de l'organe public concerné. Au besoin, elle est discutée avec la Direction concernée.

Art. 27 Réévaluation périodique

[1] Les mesures mises en oeuvre en matière de sécurité de l'information doivent être réévaluées périodiquement mais au plus tard lors de chaque révision de la PGSI, afin de tenir compte des changements juridiques, organisationnels et technologiques, ainsi que de l'évolution des menaces et des risques.

4.2 Classification des informations

Art. 28 Principe

[1] L'organe public détermine le niveau de classification des informations dont il est responsable en fonction de leur confidentialité selon l'échelle suivante:

a) non-classifiées;

b) à usage interne;

c) confidentielles;

d) secrètes.

[2] Cette classification tient compte de la nature des informations traitées, de leur valeur, de leur sensibilité ainsi que du préjudice que pourrait causer leur divulgation non autorisée que ce soit à l'Etat ou aux personnes auxquelles elles se rapportent.

[3] Les dispositions en matière de droit d'accès prévues dans la loi sur l'information et l'accès aux documents sont réservées.

Art. 29 Informations confidentielles ou secrètes

[1] Les informations classées confidentielles ou secrètes doivent être protégées par des mesures de sécurité renforcées lors de leur transmission et de leur stockage.

[2] En outre, l'organe public détermine, en fonction des tâches à accomplir, les personnes autorisées à accéder aux informations classées confidentielles ou secrètes, ainsi que l'étendue de leurs accès.

4.3 Mesures de sécurité particulières

Art. 30 Authentification et contrôle des accès

[1] L'accès aux systèmes d'information de l'administration cantonale doit être protégé par un dispositif comprenant au moins:

a) une procédure d'authentification comprenant au moins l'identification des utilisateurs et utilisatrices et l'introduction d'un mot de passe ou d'un autre moyen de vérification;

b) un système de contrôle des accès, fondé sur une définition d'autorisations individuelles d'accès.

Art. 31 Journalisation

[1] Lorsque les mesures préventives ne suffisent pas à garantir la sécurité des informations, leur traitement doit faire l'objet d'une procédure de journalisation.

[2] Les fichiers de journalisation sont soumis aux règles de la protection des données, notamment en ce qui concerne la déclaration mentionnée à l'article 19 de la loi du 25 novembre 1994 sur la protection des données (ci-après: LPrD).

[3] La conservation, l'exploitation et la destruction des fichiers de journalisation font l'objet d'instructions dans la PGSI.

Art. 32 Procédure d'appel

[1] Lors de la mise en place d'une procédure d'appel au sens de l'article 10 al. 2 LPrD, les autorisations individuelles d'accès sont définies par le responsable du fichier/traitement au sens de la LPrD, en accord avec les destinataires des données.

[2] Le responsable du fichier/traitement veille à ce que les destinataires ne puissent pas modifier les données ni en entrer de nouvelles et qu'ils n'aient accès qu'aux données correspondant aux autorisations d'accès.

[3] La procédure d'appel doit être documentée dans un règlement d'utilisation, qui précise notamment les personnes autorisées à accéder aux données, les données mises à leur disposition, la fréquence des interrogations, la procédure d'authentification, les autres mesures de sécurité ainsi que les mesures de contrôle. Une copie du règlement est transmise à l'autorité cantonale ou communale de surveillance en matière de protection des données.

Art. 33 Appareils privés

[1] Des mesures spéciales doivent être prises pour éviter toute atteinte à la confidentialité et tout traitement non autorisé lors de l'utilisation d'appareils privés.

Art. 34 Systèmes d'information transversaux ou ouverts au public

[1] Tout système d'information transversal ou ouvert au public doit, avant sa mise en exploitation, faire l'objet d'un audit de sécurité.

Art. 35 Archivage et destruction

[1] La sécurité des informations figurant dans les archives intermédiaires doit être assurée.

[2] Les informations qui ne sont pas destinées à être versées aux archives sont détruites de façon appropriée. Une attention particulière est apportée aux informations classées confidentielles ou secrètes afin d'éviter qu'elles puissent être reconstituées.

Art. 36 Protection des locaux et du matériel informatique

[1] Tous les locaux où sont conservées des informations qui ne sont pas librement accessibles au public doivent être fermés ou surveillés.

[2] Le matériel informatique doit être protégé conformément aux dispositions de la PGSI qui se base à cet effet sur les recommandations et les normes reconnues en la matière.

Art. 37 Incidents de sécurité

[1] Le ou la délégué-e SI élabore une directive sur la gestion des incidents de sécurité. Dans cette tâche, il ou elle collabore avec le SITel pour les aspects relatifs à la sécurité des moyens informatiques.

[2] Cette directive traite en particulier des points suivants:

a) les processus de détection, de signalement et d'évaluation des incidents liés à la sécurité de l'information;

b) les mesures d'intervention et de traitement à prendre en cas d'incident;

c) la répartition des rôles et des responsabilités;

d) les échanges et la coordination avec le ou la préposé-e à la protection des données;

e) l'information du public.

[3] L'ATPrDM est consultée dans le cadre de l'élaboration de la directive sur la gestion des incidents de sécurité.

5 Sécurité des moyens informatiques

Art. 38 Directive de sécurité des moyens informatiques

[1] le SITel élabore une directive de sécurité des moyens informatiques.

[2] Cette directive définit au moins:

a) les standards et normes minimaux en matière de sécurité des moyens informatiques;

b) les modalités de mise en œuvre des mesures de sécurité et leur contrôle.

[3] Le SITel applique la directive de sécurité des moyens informatiques. Lorsque cela est nécessaire, il donne les instructions à suivre aux organes responsables.

Art. 39 Niveaux de sécurité

[1] Le niveau de sécurité des moyens informatiques varie en fonction de la classification des informations traitées.

[2] Par défaut, le niveau de sécurité standard est appliqué.

[3] Un niveau de sécurité renforcé est appliqué lorsque:

a) une violation de la confidentialité, de la disponibilité, de l'intégrité, de la traçabilité, de la pérennité ou de la résilience des informations est susceptible de nuire aux intérêts supérieurs de l'Etat; ou

b) l'utilisation abusive des informations ou leur perturbation sont susceptibles de nuire aux intérêts supérieurs de l'Etat.

[4] La sécurité des infrastructures et des applications critiques fait l'objet de règles spécifiques, validées par le Conseil d'Etat.

Art. 40 Mesures techniques de sécurité

[1] Le SITel fixe les exigences techniques applicables aux niveaux de sécurité définis à l'article 39.

[2] Le SITel s'assure que les mesures techniques de sécurité applicables au niveau de sécurité renforcé fassent l'objet de contrôles périodiques.

Art. 41 Procédure en cas de désaccord

[1] En cas de désaccord sur le niveau de sécurité à appliquer entre l'organe responsable et le SITel, la Délégation du Conseil d'Etat en matière de digitalisation et de systèmes d'information tranche.

[2] Le ou la délégué-e SI est consulté-e.

6 Collaboration avec la Confédération et les autres cantons

Art. 42 Collaboration dans le domaine de la sécurité de l'information

[1] Le ou la délégué-e SI et le SITel collaborent avec la Confédération et les autres cantons sur les différents aspects liés à la sécurité de l'information et des moyens informatiques.

[2] Ils peuvent dans ce cadre échanger des informations et des données personnelles avec les organes spécialisés de la Confédération et des cantons.

II.

1.
L'acte RSF 122.0.12 (Ordonnance fixant les attributions des Directions du Conseil d'Etat et de la Chancellerie d'Etat (OADir), du 12.03.2002) est modifié comme il suit:

Art. 3 al. 1

[1] La Direction de la sécurité, de la justice et du sport a dans ses attributions:

r) *(nouveau)* la sécurité de l'information,

et les autres tâches placées dans sa compétence.

2.
L'acte RSF 122.0.31 (Règlement de la Conférence des secrétaires généraux, du 11.12.1990) est modifié comme il suit:

Art. 1 al. 2

[2] Elle donne son avis, en particulier sous l'angle de la planification, de la coordination et de la mise en œuvre, sur les projets et questions qui concernent:

b1) *(nouveau)* la sécurité de l'information;

3.
L'acte RSF 122.0.51 (Ordonnance relative à l'information sur les activités du Conseil d'Etat et de l'administration (OInf), du 14.12.2010) est modifié comme il suit:

Art. 34 al. 3 *(modifié)*

[3] Ils répondent aux exigences en matière de sécurité de l'information et de protection des données personnelles.

Art. 36 al. 2

[2] Le Service de l'informatique et des télécommunications assume les responsabilités qui découlent de son statut de service spécialisé de l'Etat en matière informatique; en particulier:

c) *(modifié)* il veille au respect du plan directeur ainsi que du schéma directeur de la digitalisation et des systèmes d'information, conformément aux dispositions en la matière;

4.
L'acte RSF 122.96.11 (Ordonnance sur la gouvernance de la digitalisation et des systèmes d'information de l'Etat, du 28.06.2021) est modifié comme il suit:

Art. 4 al. 1

[1] Le Conseil d'Etat exerce notamment les attributions suivantes:

b) *(modifié)* il fixe le cadre politique et réglementaire dans lequel doivent évoluer la digitalisation et les systèmes d'information de l'Etat en accordant une attention particulière à la sécurité de l'information et des moyens informatiques;

Art. 21

Sécurité des moyens informatiques et protection des données *(titre médian modifié)*

Art. A7-3 al. 1

[1] La CIInfra a les attributions spécifiques suivantes:

a) *(modifié)* elle préavise le concept général du SITel se rapportant aux infrastructures de la digitalisation et des systèmes d'information de l'Etat, en veillant à assurer la cohérence et à promouvoir toutes les synergies possibles, tout en portant une attention particulière à la sécurité des moyens informatiques et aux risques liés à l'obsolescence technologique;

5.

L'acte RSF 184.16 (Ordonnance concernant la mise en œuvre du Référentiel cantonal de données de personnes, organisations et nomenclatures (projet pilote), du 24.06.2019) est modifié comme il suit:

Art. A5-1 al. 1 *(modifié)*

[1] La protection des données du Référentiel cantonal est harmonisée avec les mesures visant à assurer la sécurité de l'information en général. Les mesures prises à titre de sécurité des moyens informatiques sont proposées et mises en œuvre par le SITel en fonction des risques et des technologies existantes.

III.

L'acte RSF 17.15 (Règlement sur la sécurité des données personnelles (RSD), du 29.06.1999) est abrogé.

IV.

Le présent règlement entre en vigueur le

[Signatures]