DIRECTIVE TRANSVERSALE

SÉCURITÉ ET USAGE DES RESSOURCES INFORMATIQUES ET DE COMMUNICATION DE L'ADMINISTRATION CANTONALE GENEVOISE	
EGE-10-06_v3	Domaine : Sécurité des systèmes d'information
Date : 09.11.2015 (26.01.2016 : modifications mineures sur la forme, validées par le directeur général DGSI)	Entrée en vigueur : Immédiate
Rédacteur(s): *Comité de sécurité de l'information (ComSec-I)*	**Direction/Service transversal(e):** *ComSec-I*
Responsable(s) de la mise en œuvre : Direction générale des systèmes d'information (DGSI) Départements et entités rattachées **Date : 16.12.2015**	**Approbateur :** Commission de gouvernance des systèmes d'information et de communication (CGSIC) **Date : 16.12.2015**

1. Objet

Sécurité et usage des ressources informatiques et de communication de l'administration cantonale genevoise.

2. Champ d'application

Toute l'administration cantonale, conformément au champ d'application tel que défini dans le ROGSIC, incluant les intervenants des fournisseurs externes agissant directement ou indirectement sur les systèmes d'information ainsi que toute autre personne ayant accepté par voie contractuelle la présente directive.

Toutes les ressources de l'administration sont concernées, y compris le matériel personnel connecté au réseau informatique (BYOD[1]), lorsqu'une telle connexion est dûment autorisée.

3. Exceptions

Non applicable

4. Mots clés

Utilisation, sécurité, ressource, informatique, information, administration, accès, usage, messagerie, internet, donnée, protection, système, moyen, contrôle

5. Documents de référence

- RS 943.03 (SCSE) Loi fédérale sur les services de certification dans le domaine de la signature électronique (loi sur la signature électronique)
- A 2 08 (LIPAD) Loi sur l'information du public, l'accès aux documents et la protection des données personnelles
- A 2.08.01 (RIPAD) Règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles
- B 2 15 (LArch) Loi sur les archives publiques
- B 2 15.01 (RArch) Règlement d'application de la loi sur les archives publiques
- B4 05.10 (ROAC) Règlement sur l'organisation de l'administration cantonale (ROAC)

[1] BYOD : Bring your own device

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.

- B 4 23.03 (ROGSIC) Règlement sur l'organisation et la gouvernance des systèmes d'information et de communication
- B 5 05 (LPAC) Loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux
- B 5 05.01 (RPAC) Règlement d'application de la loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux
- B 5 05.13 (RTt) Règlement sur le télétravail
- B 5 10.04 (RStCE) Règlement fixant le statut des membres du corps enseignant primaire, secondaire et tertiaire ne relevant pas des hautes écoles
- F 1 05.01 (RPol) Règlement d'application de la loi sur la police
- F 1 50.01 (ROPP) Règlement sur l'organisation et le personnel de la prison
- Autres lois et règlements relatifs au personnel de l'État
- Politique de sécurité de l'information
- Catalogue de services standards de la DGSI
- Norme internationale ISO/CEI 27002:2013 (ch.7.2, 9.3, 13.2)

6. Directives(s) liée(s)

- Cette directive annule et remplace la version 2 du 18.11.2012
- EGE-09-02 - Partage d'informations couvertes par le secret de fonction
- Toutes les directives transversales relatives aux systèmes d'information et de communication
- La politique de gouvernance et les procédures relatives à l'archivage

SOMMAIRE DE LA DIRECTIVE

L'INFORMATION CONSTITUE POUR L'ETAT DE GENEVE
UN CAPITAL PRECIEUX ET UN BIEN FONDAMENTAL
QUI DOIVENT ETRE PROTEGES PAR DES MESURES DE SECURITE ADEQUATES

1. Préambule

Le recours de plus en plus intensif et diversifié aux ressources informatiques et de communication, et aux services qui y sont associés, permettent à l'État et à ses partenaires d'augmenter leur efficience et la qualité du service fourni. Il induit notamment un accroissement des échanges dématérialisés d'informations, tant à l'intérieur de l'État que vis-à-vis des tiers, ainsi qu'une reproduction facilitée de ces informations.

En parallèle, l'évolution des technologies et de l'usage qui en est fait, pose de nouvelles questions liées à leur utilisation et à la séparation entre monde professionnel et privé, du point de vue de la sécurité et des abus éventuels qui peuvent en découler. Ces moyens concernent en particulier les postes de travail multifonctions, les terminaux mobiles et les espaces de stockage amovibles, les serveurs en réseau et virtualisés, la messagerie électronique et Internet en tant qu'outils de travail professionnel.

D'une part, l'ouverture de l'administration cantonale, quelle que soit son activité, sur le monde grâce à Internet, ainsi que l'utilisation des réseaux d'information et collaboratifs, la rend plus vulnérable à des attaques informatiques depuis l'extérieur. D'autre part, ces technologies qui sont tout à la fois ergonomiques, faciles d'emploi et parfois ludiques, peuvent conduire à une sous-estimation des dangers et des utilisations abusives ayant un impact sur la sécurité.

Le Conseil d'Etat, dans son règlement sur l'organisation et la gouvernance des systèmes d'information et de communication (ROGSIC, B 4 23.03), a chargé la direction générale des systèmes d'information (DGSI), en collaboration avec les départements, offices et autres acteurs désignés, d'élaborer et de concrétiser une politique de sécurité de l'information qui définit les intentions et les dispositions générales relatives à la sécurité de l'information. Le présent document découle de cette politique.

Il vise à fournir des consignes quant aux modalités d'usages des ressources informatiques et de communication, tant matérielles qu'immatérielles, mises à disposition par l'administration ou autorisées par celle-ci.

Ce document vise également à informer officiellement les utilisateurs des ressources informatiques et de communication de l'administration que, pour des raisons d'exploitation, de sécurité, de contrôle ou liées aux intérêts de l'État, des mesures techniques sont prises afin d'assurer l'enregistrement régulier de données.

2. Définitions

On entend par :

- Activité professionnelle : celle prévue par les lois et règlements auxquels se réfère l'Etat, à savoir toutes les activités éducatives, administratives, de gestion et de soutien nécessaires à l'accomplissement des tâches de l'Etat.
- Administration cantonale : tous les offices et services des départements selon le règlement sur l'organisation de l'administration cantonale (B 4 05.10).
- Classement : action de mettre en ordre et de ranger en faisant référence à un plan de classement.
- Classification : attribution d'un niveau de protection adapté à la valeur et l'importance d'une donnée ou d'un bien détenu par une organisation.

- Incident : tout événement indésirable ou inattendu, qui ne fait pas partie du fonctionnement recherché d'un service, qui cause ou peut compromettre les opérations liées à l'activité de l'organisation et/ou menacer la sécurité de l'information.
- Protection de la sphère privée : protection de la personnalité et des droits fondamentaux des personnes, intégrant la protection des données personnelles[2], par un traitement des données selon, notamment, les principes de licéité (conformité au droit), de finalité (but indiqué, prévu par la loi ou ressortant des circonstances), de proportionnalité (adéquation des moyens à un but recherché) et de transparence.
- Ressources informatiques et de communication (ci-après "ressources") : les moyens informatiques et de communication (matériel, logiciels, outils et services) mis à disposition par l'administration ou autorisées par celle-ci (ci-après "ressources de l'administration").
- Système d'information : ensemble de moyens techniques, humains et organisationnels permettant à l'administration de recueillir, conserver, traiter, distribuer et présenter les informations relatives à son activité quelles que soient les formes et les supports.

3. Principes généraux

[1] L'utilisation d'une information doit respecter les principes de disponibilité, d'intégrité et de confidentialité de celle-ci, tels que définis par les lois, règlements et directives en vigueur.

[2] L'utilisation des ressources ne doit pas compromettre la sécurité de l'information.

[3] Toute demande d'exception aux principes décrits dans cette directive doit être traitée selon une procédure spécifique et validée, qui doit comporter :

- une justification basée sur un besoin métier reconnu et conforme à la loi,
- une autorisation documentée,
- des instances d'autorisation clairement identifiées, dont au moins le responsable hiérarchique, le responsable départemental de la sécurité de l'information (RSI) et la direction générale des systèmes d'information (DGSI).

[4] Demeurent réservées les règles spécifiques[3] édictées par le Conseil d'État.

3.1. Droits d'accès

[1] Tout accès à l'information et aux ressources de l'administration fait l'objet d'une autorisation motivée et documentée. L'accès accordé est strictement personnel, confidentiel, lié à la fonction et intransmissible.

[2] Les autorisations d'accès sont délivrées selon les principes du moindre privilège[4] et de la séparation des rôles et responsabilités.

[3] Chaque utilisateur :

- choisit des mots de passe conformément à la directive sur les comptes et mots de passe (EGE-10-13),

[2] Protection des données personnelles au sens de la LIPAD et, lorsque l'administration cantonale agit en délégation de la Confédération, à loi fédérale sur la protection des données (LPD, RS 235.1).
[3] Par exemple, l'arrêté du CE du 25.6.2014 sur la communication syndicale.
[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.

- s'abstient de mettre à la disposition de personnes non autorisées un accès aux informations et/ou aux ressources de l'administration à travers les outils et moyens dont il a l'usage,
- assure la protection de ses informations et est responsable des droits donnés à d'autres personnes dûment autorisées,
- est personnellement responsable du bon usage de ses droits d'accès aux ressources, notamment son poste de travail, la messagerie et Internet. Comme pour toute opération informatique, une action effectuée sous une authentification est présumée attribuée à la ou au propriétaire du compte,
- signale à sa hiérarchie toute tentative de violation ou d'usurpation de son compte et, de façon générale, toute anomalie constatée.

3.2. Confidentialité

[1] Toute information fait l'objet d'une classification avant tout autre traitement. Cette classification est définie selon les règles de la directive transversale sur la classification des informations EGE-10-12 (ci-après "directive classification") qui établit les mesures de protection adaptées au niveau de classification. Par défaut, toute information non classifiée est considérée comme de niveau de protection "non public".

[2] L'utilisation, l'enregistrement et la diffusion de l'information sont soumis au secret de fonction tel que défini dans le code pénal suisse[5] et aux dispositions légales cantonales applicables, notamment la LIPAD et son règlement d'application. Le secret de fonction est également applicable pour toutes informations portées à la connaissance des membres du personnel à l'occasion de l'exercice de leur fonction, dans la mesure où une disposition légale en vigueur ne permet pas de les communiquer à autrui.

[3] La sortie d'information hors du périmètre physique de l'administration et/ou à l'extérieur du réseau informatique de l'État est assujettie à l'autorisation des hiérarchies ou responsables concernés, dans le respect du cadre légal (LIPAD et RIPAD notamment) applicable.

[4] Le partage d'une information au sein de l'administration, doit également prendre en compte les autres secrets de fonctions spéciaux (qualifiés), en respectant la directive sur le partage d'informations couvertes par le secret de fonction (EGE-09-02).

[5] Il convient d'adopter une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l'écran vide pour les moyens de traitement de l'information. De même, les documents papier comportant des données personnelles doivent être broyés et non simplement jetés à la poubelle.

[6] L'usage de certaines ressources peut être restreint, voire interdit, par les offices traitant des données confidentielles ou secrètes.

3.3. Utilisation professionnelle et privée

[1] Les ressources de l'administration sont destinées à un usage professionnel.

[2] L'utilisation à des fins privées n'est tolérée que si [6]:

- elle est minime en temps et en fréquence,
- elle n'entraîne qu'une utilisation négligeable des ressources,
- elle ne compromet ni n'entrave l'activité professionnelle ou celle du service,

[5] Cf. art. 320 et 110 ch. 3 CPS - 311.0
[6] Cf. art.23A al.2 RPAC

- elle ne relève pas d'une activité lucrative privée, de propagande politique ou religieuse,
- elle n'est ni illicite, ni contraire à la bienséance ou à la décence,
- elle ne met pas en danger la sécurité du système d'information.

[3] Toute propagande politique ou religieuse est interdite[7].

[4] Dans le cadre d'une utilisation privée des ressources de l'administration, on n'émettra pas d'opinions personnelles susceptibles de porter préjudice à l'Etat de Genève. Si des opinions personnelles sont exprimées, il sera explicitement précisé que ces opinions sont personnelles et qu'elles n'engagent en aucune manière la responsabilité de l'employeur.

3.4. Moyens de contrôle et protection de la sphère privée

[1] L'État met en place, conformément au cadre légal en vigueur - notamment l'article 23A al.4 et 5 RPAC (B 5 05.01) - et dans le respect de la sphère privée des collaborateurs, tous les moyens de contrôle, d'analyse et de collecte de preuves qu'il juge nécessaires à la défense de ses intérêts, de son image, de ses informations et de ses ressources[8]. Ces mesures s'appliquent également aux informations professionnelles stockées sur des ressources privées.

[2] Des contrôles automatisés, statistiques et non individualisés de l'utilisation des ressources de l'administration par le personnel peuvent être effectués[9].

[3] Lorsque les intérêts prépondérants de l'Etat de Genève tels que la sécurité informatique ou le bon fonctionnement du service l'exigent, des contrôles individualisés, et le cas échéant un accès à la liste des appels et à leur durée, au poste de travail informatique ou au compte de messagerie, peuvent être ordonnés par le chef du département ou son secrétaire général. Ces mesures respectent, dans toute la mesure du possible, la sphère privée des membres du personnel concernés[10].

[4] L'administration peut, dans le cadre du contrôle des affaires ou pour assurer la continuité des activités, consulter les messages professionnels reçus par courrier électronique et des fichiers professionnels sauvegardés sur le poste de travail ou sur les espaces de stockage définis dans le catalogue de service de la DGSI, conformément aux directives transversales spécifiques traitant notamment des mesures de contrôles (EGE-10-07) et de continuité d'activité.

[5] En cas d'urgence ou de faille majeure, la DGSI prend toutes les mesures adéquates pour protéger les intérêts de l'État, en respectant autant que possible la sphère privée des collaborateurs. Ces mesures sont prises jusqu'au retour à la normale ou la correction de la faille.

3.5. Responsabilités

[1] Toute ressource est attribuée à un ou une propriétaire qui demeure responsable de la bonne gestion de ce bien tout au long de son cycle de vie.

[2] Chaque utilisateur est personnellement responsable de l'emploi des ressources mises à sa disposition.

[3] Chaque utilisateur a la charge, à son niveau, de contribuer à la sécurité générale.

[7] Cf. al. 3, art. 23A, règlement B 5 05.01
[8] Notamment par rapport aux risques d'erreurs, de négligence ou de malveillance, et en particulier de fraude.
[9] Cf. art.23A al.4 RPAC
[10] Cf. art.23A al.5 RPAC

[4] Chaque entité et chaque utilisateur veillent, en fonction du niveau de confidentialité et d'importance des informations traitées, à leur assurer un niveau de protection adapté et conforme au cadre légal et réglementaire[11].

[5] Il est interdit à l'utilisateur :

- de perturber intentionnellement le bon fonctionnement des ressources de l'administration,
- de se livrer depuis l'infrastructure de l'Etat à des actes mettant sciemment en péril la sécurité ou le bon fonctionnement d'autres sites et réseaux de télécommunication,
- de modifier les paramètres régissant la sécurité (par exemple navigateur, client messagerie, poste de travail, etc.),
- de contourner, de quelque façon que ce soit, les mesures de sécurité,
- de divulguer ses mots de passe et/ou de les communiquer à des tiers,
- de masquer sa véritable identité et/ou d'usurper l'identité d'autrui.

[6] Il est interdit de prendre connaissance, sans y être autorisé par la personne intéressée, d'informations détenues par d'autres utilisateurs, quand bien même celles-ci ne seraient pas explicitement protégées. Reste réservée la section 3.4, alinéas 4 et 5.

[7] Il est également interdit d'enregistrer et de diffuser des informations à caractère contraire à l'honneur, raciste, pornographique, pédophile ou contraire aux mœurs. Est prohibée toute collecte ou diffusion d'informations susceptible de porter atteinte à l'image de l'État, à une minorité ou à un individu. Demeurent réservés les besoins liés aux enquêtes judiciaires et administratives.

[8] L'usage abusif des ressources de l'administration peut donner lieu à des sanctions, voire à un dépôt de plainte pénale ou administrative. Il en est de même de la divulgation inopportune ou malveillante d'informations.

[9] Seules les entités autorisées par l'art 8 al.2 ROGSIC peuvent mandater ou réaliser des audits relatifs à la sécurité de l'information. Pour tout audit technique (test de vulnérabilité ou test d'intrusion par exemple) pouvant avoir un impact sur les ressources de l'Etat, ces entités avertiront la direction de la DGSI. Celle-ci prendra, d'entente avec l'entité, les mesures adéquates.

3.6. Destruction de supports d'information

[1] Les offices prennent les mesures propres à garantir la destruction des supports d'information physiques ou numériques (papier, CD, clé USB, bases de données, etc.) qui contiennent des données obsolètes ou erronées.

[2] Les mesures doivent être prises conformément au cadre légal, notamment la LIPAD et la LArch, ainsi qu'à la directive sur la classification.

[11] Cette responsabilité s'applique aussi bien aux informations de l'office, qu'aux informations provenant d'autres départements ou office, ou sous propriété de ceux-ci.

4. Mesures de protection spécifiques

4.1. Matériel informatique et logiciels

[1] Afin de garantir une maîtrise et une protection complètes et continues du matériel informatique et des logiciels fournis par l'administration, en particulier du poste de travail :

- toute intervention sur ces ressources ne peut être réalisée que par une personne habilitée,
- les consignes d'utilisation du matériel sont respectées,
- le poste de travail est verrouillé, voire éteint, lors de toute pause ou éloignement,
- les postes de travail mobiles sont connectés au minimum une fois par mois au réseau de l'État afin d'effectuer les mises à jour nécessaires,
- les postes de travail sont éteints en fin de journée.

[2] Les postes de travail fournis par la DGSI, mais non maintenus par elle, ne sont pas connectés au réseau de l'État.

4.1.1. Matériel informatique

[3] L'État définit les ressources standards de l'administration et leur configuration, et met en place le dispositif de sécurité requis adapté à l'usage prévu (par ex. chiffrement des disques durs des PC portables).

[4] Il est strictement interdit à un utilisateur de modifier ou de reconfigurer le matériel fourni par l'État.

[5] Tout matériel privé ou fourni par une personne tierce et connecté au poste et au réseau de l'Etat doit faire l'objet d'une autorisation écrite de la hiérarchie[12].

[6] L'utilisation de matériel privé doit respecter les instructions et contraintes de sécurité, en particulier dans le domaine de la confidentialité des données. Lorsque l'utilisateur se sépare de ce matériel, il supprime toute donnée professionnelle.

[7] L'utilisateur doit avertir les instances compétentes en cas de dysfonctionnement du matériel, d'alertes de sécurité, ou de tout autre incident mettant en péril la confidentialité, l'intégrité et la disponibilité des ressources ou des données. Cette disposition s'applique également au matériel privé utilisé à des fins professionnelles.

[8] Lors de l'usage de matériel non standard fourni par la DGSI, les conditions de sécurité sont définies par une charte ou une convention spécifique.

4.1.2. Applications et logiciels

[9] Il est strictement interdit à un utilisateur d'installer ou d'utiliser sur les ressources de l'administration d'autres logiciels que ceux agréés par la DGSI, ou par délégation les organes autorisés, et régulièrement acquis conformément au processus d'acquisition en vigueur à l'Etat.

[10] Le développement et l'installation des logiciels sont réservés aux personnes qui y sont habilitées. La création et l'utilisation de code exécuté dans les applications bureautiques (script, macro, formulaire interactif, etc.) sont déconseillées. Des restrictions peuvent être mises en place.

[12] Dans le domaine pédagogique, le SEM est l'instance habilitée à délivrer cette autorisation.

[11] Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le contrat d'achat.

[12] L'auteur d'une contrefaçon engage directement sa responsabilité.

[13] L'usage de licences privées sur des postes professionnels est interdit.

[14] Le domaine pédagogique règle les points ci-dessus dans le respect des droits de licence et selon ses dispositions spécifiques.

4.2. Messagerie

[1] Dans le cadre de cette directive, on entend par messagerie l'ensemble des fonctionnalités liées à celle-ci selon le catalogue de services standards de la DGSI : boîte aux lettres, agenda, tâches, contacts, notes, archivage, sms, fax, etc.

4.2.1. Utilisation

[2] L'expéditeur doit porter une attention particulière à la liste des destinataires, notamment en contrôlant leur nombre et leur identité.

[3] Les envois de masse sont régis par des procédures internes aux départements ou aux offices, en accord avec la DGSI.

[4] Sont interdits les envois de masse à des fins privées, la propagation de messages " chaînés " et de fausses rumeurs (hoax).

[5] Les abonnements à des " Newsletters " ou listes de distribution doivent être en rapport avec l'activité professionnelle.

[6] La diffusion ou la redistribution de tout ou partie des annuaires électroniques de l'État est interdite.

[7] La réception de messages ou de pièces jointes doit éveiller tout particulièrement l'attention, notamment si l'expéditeur du message est inconnu, si l'extension de la pièce jointe est inusitée ou si le contenu du message est peu plausible. En cas de message suspect, il est absolument prohibé d'ouvrir la pièce jointe, et il faut en référer sans délai au Super-U, ou à une personne exerçant une fonction équivalente, de son service. Dans tous les cas, un ticket d'incident doit être ouvert.

[8] Le transfert automatique de messages depuis la messagerie de l'État vers une adresse de messagerie externe est interdit.

[9] En cas d'absence pouvant impacter la bonne marche de l'office, l'utilisateur veillera à mettre un message d'absence sur sa boîte-aux-lettres.

4.2.2. Droits d'accès

[10] Exceptés les cas prévus aux alinéas 4 des sections 3.4 et 3.5 de la présente directive, nulle autre personne que son propriétaire ne peut accéder à une boîte aux lettres, personnelle ou de service, si elle n'est pas au bénéfice d'une délégation des droits nécessaires accordée par le propriétaire.

4.2.3. Utilisation privée et des systèmes de messagerie tiers

[11] L'utilisateur veillera à une séparation stricte de l'usage de la messagerie à des fins professionnelles et de celui à des fins privées. Il n'utilisera pas d'agrégateur ou de fédérateur de messagerie ou d'autres utilitaires recourant à un stockage délocalisés ou dématérialisés externes (« cloud »).

[12] L'utilisation de systèmes de messageries personnelles disponibles à travers des services de messageries non officielles (par exemple : Gmail, Hotmail, Bluewin) est tolérée depuis le réseau de l'administration avec les réserves émises par rapport à l'usage privé (section 3.3).

[13] En coordination avec la DGSI, le DIP spécifie les systèmes de messagerie pédagogiques et en fixe les règles d'usage.

[14] L'utilisation d'une messagerie privée pour un usage professionnel est interdite.

4.2.4. Confidentialité

[15] Les informations classifiées confidentielles ou secrètes doivent être protégées conformément aux recommandations de la directive classification, notamment en chiffrant ces informations et en limitant leur diffusion.

4.2.5. Engagement de l'Etat

[16] Les messages qui contiennent un engagement juridique ou financier de l'Etat doivent émaner d'une personne habilitée à engager l'Etat.

4.3. Stockage et bureautique

[1] Afin d'assurer la maîtrise de l'information, l'utilisation efficiente des ressources bureautiques et de stockage (poste de travail, serveurs de fichiers, outils collaboratifs, etc.), ainsi que la conformité de son traitement :

- l'information est classée, classifiée et archivée selon les exigences légales, réglementaires et normatives,
- les droits d'accès à l'information doivent être précisément définis et régulièrement contrôlés,
- les informations doivent être stockées sur des espaces sauvegardés et sécurisés par l'État; les espaces de stockage locaux n'étant ni sauvegardés ni sécurisés,
- les espaces de stockage ne sont pas encombrés par des fichiers n'ayant pas de caractère professionnel.

[2] Le recours à des systèmes informatiques délocalisés ou dématérialisés externes (informatique en nuage dite "cloud") est interdit, sous réserve d'un accord préalable du directeur de la DGSI.

[3] En coordination avec la DGSI, le DIP spécifie les règles d'usage des systèmes "cloud" pédagogiques.

4.4. Téléphonie et réseau

[1] L'échange de données au travers d'un service téléphonique (téléphone, fax, SMS, etc.), d'un outil de communication électronique, d'un réseau informatique ou de télécommunication doit être fait avec prudence en prenant en compte l'environnement, le lieu et le contexte. La directive classification est applicable.

[2] Les règles et instructions d'utilisation de la DGSI doivent être respectées.

4.4.1. Téléphonie

[3] La téléphonie mobile comporte des vulnérabilités et des risques importants pour l'environnement professionnel de l'Etat; en conséquence :

- dans tous les cas, les collaborateurs privilégient les appels depuis et vers les postes fixes,

- les collaborateurs s'assurent de l'identité de l'interlocuteur. Selon la nature des informations à traiter, il est recommandé de proposer à son interlocuteur externe à l'Etat de le rappeler au numéro de téléphone qu'il indiquera,
- la déviation systématique d'appels sur un téléphone mobile est à proscrire.

[4] Dans le cadre de l'activité professionnelle, l'utilisateur d'un appareil de téléphonie mobile doit s'assurer que son appareil est protégé de manière adéquate. Cette protection concerne notamment l'activation du verrouillage de l'appareil après chaque utilisation et l'installation des mises à jour de sécurité.

[5] La synchronisation sur l'appareil de téléphonie de services informatiques et de communication de l'État, notamment des services de messagerie, fait l'objet d'une autorisation par la hiérarchie.

4.4.2. Réseau

[6] L'extension de réseaux par des moyens techniques non mis en place par la DGSI, dont les appareils mobiles, est interdite.

[7] La connexion simultanée à plusieurs réseaux (réseau de l'État et réseau WiFi par exemple) est interdite.

[8] Tout usage d'un accès distant[13] aux ressources de l'État, quels que soient le moyen utilisé et l'utilisateur (interne ou externe), fait l'objet d'une autorisation documentée[14].

[9] L'accès distant est réservé à l'usage pour lequel il a été accordé.

4.5. Moyens d'impression et numérisation

[1] L'utilisation des moyens d'impression, de numérisation, de télécopies (fax) et des appareils multicopieurs (mopieurs), doit garantir la confidentialité des informations.

[2] Les offices s'assurent que l'activation des fonctionnalités de sécurité (chiffrement et/ou suppression de données, effacement de la mémoire, récupération du disque dur, connexion à distance, etc.) répond aux exigences métier.

[3] Les dispositions de sécurité ci-dessous sont prises en fonction du niveau de classification des informations.

4.5.1. Document imprimé

[4] Toute impression ou copie de documents nécessite le suivi du traitement du document "papier" concerné. Les mesures suivantes doivent être appliquées :

- mettre en œuvre la politique du bureau propre pour les documents imprimés et assurer leur classement et leur protection de manière adéquate,
- marquer le niveau de classification, ainsi que des informations permettant de retrouver l'auteur de façon visible sur le document,
- assurer le suivi et la prise en charge des documents imprimés notamment en retirant immédiatement des moyens d'impression les documents contenant de l'information non publique, confidentielle ou secrète,

[13] Permet à l'utilisateur de se connecter sur une ressource ou une information de l'État alors qu'il est connecté en dehors du réseau de l'administration (en utilisant un WiFi public ou depuis son domicile par exemple).

[14] Cette autorisation peut explicitement découler d'une permission accordée dans un système de gestion des identités et des autorisations (par ex. GINA Manager)

- retirer les originaux imprimés lors de copies, de numérisation ou de télécopie, ainsi que tout document issu de ces opérations (journaux, confirmation d'envoi, accusés de réception),
- assurer l'archivage et/ou la destruction du document imprimé selon les règles d'archivage et de classification des informations.

[5] Les options d'impression sécurisée mises à disposition par les moyens d'impression (protection de l'impression par mot de passe) doivent être utilisées en fonction du niveau de classification et de protection de l'information et du lieu d'impression (par exemple imprimantes dans un espace public).

[6] Pour des raisons de confidentialité et de protection de l'environnement, il est recommandé de restreindre les impressions au strict nécessaire.

4.5.2. Document numérisé

[7] Toute numérisation de documents crée des fichiers et des sauvegardes, sur des espaces de stockage dédiés, qu'il convient de protéger de manière adéquate. L'utilisateur est en charge de :

- traiter les documents numérisés conformément aux règles de la section 4.3,
- supprimer les fichiers sur les espaces de numérisation après copie sur les espaces de stockage métier,
- purger les fichiers, pour les documents confidentiels et secrets, sur les espaces de numérisation (dossiers "scan").

4.5.3. Document faxé :

[8] L'usage de la télécopie (fax) nécessite les mesures suivantes :

- placer de préférence les machines fax dans une zone non publique, dans des endroits discrets, à proximité et sous la surveillance des services qui en ont besoin,
- vérifier attentivement les coordonnées du destinataire avant l'envoi,
- récupérer l'original du fax envoyé, ainsi que l'accusé d'envoi.

4.6. Sécurité de l'information nomade et télétravail

[1] Hors des locaux de l'État (domicile, voie publique, transports, cybercafé, hôtel, gare, etc.) l'utilisation des ressources informatiques et de réseaux publics, en particulier WiFi, offre de moindres garanties de sécurité. Ce constat concerne notamment le risque d'interception de communication, la perte ou le vol de matériel et d'informations et la sécurité physique du matériel. Il convient dès lors de prendre des mesures de sécurité adaptées.

4.6.1. Télétravail

[2] Le télétravail est régi par le règlement ad hoc[15].

4.6.2. Utilisation

[3] Tout traitement, échange ou transport d'information doit respecter le cadre légal, réglementaire ou contractuel en vigueur en Suisse ou, le cas échéant, à l'étranger.

[4] Les informations classées secrètes ne doivent en aucun cas sortir de l'administration.

[15] Règlement sur le télétravail (RTt – B 5 05.13)

[5] Tout échange d'informations confidentielles (par voie orale ou électronique) dans un espace public ou non contrôlé doit être strictement limité aux cas urgents. A défaut l'utilisateur doit s'assurer que sa conversation ou que le message ne puisse pas être écouté, intercepté ou lu par des entités ou des personnes non autorisées.

[6] L'accès distant aux ressources informationnelles de l'État s'effectue par des moyens (services ou matériel) fournis par l'État et offrant un niveau de sécurité renforcé.

[7] L'accès distant doit être interrompu en fin d'activité ou en cas d'absence momentanée en se conformant aux procédures de déconnexion standards ou documentées.

[8] Tout utilisateur doit veiller à supprimer, sur les systèmes tiers utilisés, toute information et toute trace d'activité (fichiers téléchargés et temporaires, impression, mots-de-passe, historique et cookies de navigation internet, etc.).

[9] Dès que possible, les données enregistrées et traitées en utilisation nomade (PC portable, smartphone, etc.), devront être transférées et sauvegardées sur les espaces partagés de l'État (disques réseau).

[10] A titre exceptionnel, dans le cas où la règle de l'alinéa 9 ci-dessus ne peut être respectée, une sauvegarde temporaire sur un support physique adapté (clé USB par ex.) et sous la responsabilité de l'utilisateur, est tolérée. Les informations sont protégées et effacées, après transfert sur les espaces de stockage partagés de l'État, selon les règles de la "directive classification".

[11] Le niveau de sécurité du matériel de l'État (ordinateur portable) ne doit pas être modifié par l'utilisateur. La configuration du matériel doit être régulièrement mise à jour, en le connectant au réseau de l'État.

[12] Aucun tiers ne doit utiliser l'équipement nomade fourni par l'État.

4.6.3. Protection physique

[13] L'information et son support sont protégés contre la perte, le vol et d'éventuels dommages et ne sont pas laissés sans surveillance (soute à bagage, véhicules, lieux publics, salle de conférence, etc.). Ils sont, dès que possible, entreposés de façon sécurisée (coffre-fort dans les chambres d'hôtel par ex.). Ils sont également protégés des conditions environnementales.

[14] En cas de perte ou de vol, l'utilisateur doit aviser son service et le service d'assistance de la DGSI dont il aura pris soin de prendre les coordonnées; cet avis déclenchera les procédures adéquates. Ces dispositions s'appliquent également en cas de matériel privé utilisé pour l'usage professionnel.

[15] Lors de l'utilisation de matériel privé, en particulier dans le cadre du télétravail, l'utilisateur est responsable de la protection et du niveau de sécurité de son poste et de ses équipements.

[16] En dehors de périodes de travail, afin de bénéficier de la protection mise en place (chiffrement du disque dur) sur les PC portables de l'État, ceux-ci doivent être arrêtés.

[17] Les moyens d'authentification sont conservés séparément du support de l'information.

4.7. Internet

4.7.1. Utilisation

[1] L'accès à Internet est réservé à un usage professionnel. Pour des besoins de sécurité, il peut être limité à des sites de confiance sur la base d'une liste préétablie et régulièrement mise à jour.

[2] Une utilisation à des fins privées est toutefois tolérée, avec les réserves émises sous la section 3.3.

[3] Il est interdit de consulter sciemment des informations à caractère pornographique, pédophile, raciste ou violent, ou des sites mettant potentiellement en danger la sécurité des ressources et de l'information. Demeurent réservés les besoins liés aux enquêtes judiciaires et administratives.

4.7.2. Pages personnelles

[4] La création à des fins non professionnelles de sites ou de pages hébergés sur les ressources de l'État est interdite.

4.7.3. Divulgation d'information

[5] L'utilisateur ne doit pas utiliser les services Internet pour proposer ou rendre accessible à des tiers des données et informations non publiques, confidentielles ou secrètes ou contrevenant à la législation en matière de propriété intellectuelle (droit d'auteur).

[6] Sur les réseaux sociaux et outils de partage d'informations (forums, chats, etc.), le collaborateur doit s'abstenir, dans le cadre de sa fonction mais également dans le cadre privé, de tout propos ou acte qui peut porter préjudice à l'Etat. Il doit aussi prendre soin de s'exprimer avec le tact et la bienséance requis.

4.7.4. Téléchargement

[7] Le téléchargement d'informations depuis Internet est réservé à l'activité professionnelle; il doit être réduit au strict minimum et ne provenir que de sources réputées sûres.