Directive d'utilisation des systèmes d'information

du 27.10.2021

Actes législatifs concernés par ce projet (RS numéros)

Nouveau: **-**
Modifié: –
Abrogé: –

Le Conseil d'Etat du canton du Valais

vu la loi sur le personnel de l'Etat du Valais du 19 novembre 2010 (LcPers),

vu la loi sur l'information du public, la protection des données et l'archivage du 9 octobre 2008 (LIPDA),
sur la proposition du Département des finances et de l'énergie,

arrête:

I.

Art. 1 But

[1] La directive d'utilisation des systèmes d'information de l'Etat du Valais établit les règles en vue de préserver le bon fonctionnement de ceux-ci.

[2] Cette directive entend également prévenir l'utilisation abusive des systèmes d'information de l'Etat du Valais, elle précise les sanctions dans le respect des lois et réglementations en vigueur.

[3] A ce titre, elle définit les droits et obligations des utilisateurs internes concernant l'usage des systèmes d'information de l'Etat du Valais.

Art. 2 Définitions

[1] On entend par:

a) données personnelles: toute information se rapportant à une personne physique, morale ou à un groupe de personnes identifiées ou identifiables (art. 3 al. 3 LIPDA);

b) données sensibles: données personnelles concernant les opinions ou activités religieuses, idéologiques, politiques ou syndicales; la santé, la sphère intime ou l'origine raciale; des mesures d'aide sociale; des poursuites ou sanction pénales et administratives (art. 3 al. 7 LIPDA);

c) données confidentielles: toute information soumise au secret de fonction au regard des articles 21 LcPers et 320 CP;

d) fonction informatique: la fonction informatique de l'Etat du Valais regroupe les dispositifs informatiques du SCI, de la police cantonale et d'ICT-VS (informatique des écoles);

e) fonction sécurité de l'information : la fonction sécurité de l'information est représentée par les responsables sécurité des trois dispositifs informatiques cités ci-dessus;

f) VPN: connexion sécurisée entre un appareil distant et le réseau cantonal.

Art. 3 Champ d'application

[1] Cette directive s'applique à tous les utilisateurs des systèmes d'information de l'Etat du Valais. Elle ne s'applique pas aux utilisateurs des prestations de cyberadministration, ni aux écoles du canton, hormis celles hébergées et/ou gérées par le SCI, notamment les écoles d'agriculture.

[2] On comprend par:

a) utilisateurs: les usagers internes, à savoir les magistrats, les employés, les stagiaires, les apprentis, mais également les prestataires de l'Etat du Valais ou toutes les personnes ayant/exécutant un mandat pour/avec l'Etat du Valais;

b) systèmes d'information: l'ensemble des outils informatiques et de télécommunications.

Art. 4 Conditions d'utilisation

[1] Chaque utilisateur porte la responsabilité d'utiliser correctement les systèmes d'information mis à sa disposition.

[2] Les systèmes d'information sont mis à disposition des utilisateurs pour leurs activités professionnelles. Le choix des moyens informatiques et les limitations spécifiques d'utilisation sont arrêtés par le chef de département sur proposition du chef de service, sous réserve de l'accord de la fonction informatique, notamment en ce qui concerne les aspects techniques et sécuritaires. Demeurent, en sus, réservées les dispositions concernant la gestion financière.

[3] Un usage privé limité et raisonnable des systèmes d'information est toléré, dès lors qu'il est réalisé dans un but non lucratif et dans la mesure où il n'entraîne que des coûts minimes pour l'employeur, qu'il ne nuit pas au travail de l'utilisateur, qu'il ne porte pas atteinte aux intérêts de l'Etat et qu'il ne contrevient aucunement aux lois et réglementations en vigueur.

[4] Lors d'usage privé, l'utilisateur doit faire en sorte que ce qu'il traite soit clairement perçu comme tel et n'engage d'aucune façon la responsabilité de l'Etat.

[5] Le stockage de données privées n'est toléré que sur les supports de données locaux qui ne sont pas synchronisés avec le système central, l'Etat du Valais ne pourra en aucun cas être tenu pour responsable de la perte de ces données.

Art. 5 Règles générales d'utilisation

[1] Les données confidentielles (toutes les données non publiques) doivent être traitées selon les dispositions régissant le respect du secret de fonction et toutes les précautions doivent être prises pour en réserver l'accès aux seuls ayants droits. Les intervenants techniques internes et externes doivent être particulièrement vigilants à cet égard.

[2] La législation relative aux droits d'auteur doit être respectée, il est de fait strictement interdit de copier des logiciels appartenant à l'Etat du Valais.

[3] La consultation, le stockage ou la diffusion d'informations qui, sous quelque forme que ce soit, portent atteinte à la dignité de la personne, présentent un caractère violent, pornographique, pédophile, raciste ou criminel sont strictement interdits.

[4] Les utilisateurs ne sont pas autorisés à effectuer ou à faire effectuer des développements informatiques spécifiques, sauf en cas d'accord des instances compétentes de la fonction informatique.

[5] Les utilisateurs sont tenus de traiter leurs mots de passe de manière confidentielle. Aucune transmission de ceux-ci n'est autorisée, sauf cas d'urgence impactant la continuité des affaires du service et selon une procédure validée par la fonction sécurité de l'information.

[6] Tout envoi de données confidentielles ou sensibles doit faire l'objet d'une protection appropriée, notamment par le biais du chiffrement, sous la responsabilité de l'utilisateur. Le service cantonal de l'informatique est à disposition pour indiquer les solutions adéquates.

[7] L'utilisateur doit éteindre ses systèmes informatiques personnels (ordinateur, écran, imprimante, etc.) à la fin de chaque journée de travail.

[8] Le piratage informatique est strictement interdit et pénalement répréhensible.

[9] L'accès aux données informatiques d'un tiers est strictement interdit, sauf sur autorisation formelle de ce dernier ou lorsqu'une procédure pénale l'exige.

[10] L'accès à distance n'est autorisé qu'au travers des solutions mises à disposition par le SCI, toute autre solution est interdite.

[11] L'utilisation de matériel privé (BYOD) n'est pas autorisée hors des utilisations formellement validées par la fonction informatique.

[12] L'accès à des services professionnels en ligne (messagerie étatique, bureau virtuel, etc.) à l'aide d'un appareil privé (smartphone, ordinateur, etc.) ne donne droit à aucune prétention financière, horaire ou de quelque autre ordre, y compris en cas de dommage ou de perte de l'appareil concerné, sauf si cela a été explicitement prévu et défini à l'avance.

Art. 6 Postes de travail et stockage des données

[1] Le poste de travail est un élément constitutif du système d'information de l'Etat du Valais. La modification de sa configuration et/ou un usage inapproprié peuvent affecter négativement son fonctionnement global.

[2] Seules les entités autorisées de la fonction informatique peuvent installer et désinstaller du matériel et des logiciels informatiques ou en modifier la configuration. Elles peuvent déléguer ces tâches à un fournisseur ou à un utilisateur spécialement instruit.

[3] Sauf autorisation préalable d'une entité informatique habilitée, il est interdit de connecter sur le réseau interne de l'Etat (réseau filaire ou WiFi Intranet) tout appareil électronique tiers.

[4] De même, la connexion au poste de travail d'un périphérique tiers est prohibée. A l'exception toutefois, de la connexion temporaire d'unités de stockage USB dans le but d'y récupérer des données de partenaires, après s'être préalablement assuré auprès de ce dernier que le périphérique en question ne constitue aucunement un danger (libre de tout logiciel malveillant).

[5] L'Etat du Valais se réserve le droit de supprimer sans préavis toute modification ou installation effectuée en violation des présentes directives.

[6] Des espaces de stockage sont mis à disposition sur les infrastructures centrales afin de permettre le stockage des documents professionnels. Ces espaces sont sauvegardés quotidiennement. L'utilisateur est tenu d'épurer régulièrement les données obsolètes.

Art. 7 Mobilité

[1] Les équipements nomades fournis par l'Etat du Valais sont placés sous la responsabilité de leur détenteur, ils ne doivent jamais rester sans surveillance (véhicule, soute à bagages, lieux publics, etc.). En cas de perte ou de vol, le collaborateur est tenu d'en avertir immédiatement le responsable sécurité de l'information compétent.

[2] Le détenteur d'équipements nomades est tenu de les protéger des éléments environnementaux inadéquats (soleil, chaleur, eau, sable, etc.).

[3] Les informations à caractère non public doivent obligatoirement être chiffrées sur tout élément de stockage quittant l'administration cantonale. De plus, les informations confidentielles ou sensibles ne doivent en aucun cas être transférées sur un espace de stockage privé (smartphone, tablette, clé USB, stockage en ligne, etc.), ni déposées sur une boîte vocale.

[4] Les codes d'accès, calculette, token et autres éléments servant à l'authentification doivent être tenus à l'écart de l'équipement de base qu'ils sécurisent.

[5] L'utilisation du matériel nomade de l'Etat du Valais à des fins privées est tolérée, en sus des précédentes conditions, uniquement si le matériel est utilisé par son propre détenteur et qu'aucune modification n'affecte le système.

[6] Lors de travail externe, il est de la responsabilité de l'utilisateur de s'assurer que l'information ne puisse être ni vue ni entendue par un tiers. Dans le cadre d'une telle utilisation, l'utilisateur est préalablement tenu de se renseigner sur les réglementations en vigueur à l'étranger (tout appareil électronique peut être confisqué sans aucune justification par certaines douanes).

Art. 8 Messagerie électronique professionnelle

[1] L'usage de la messagerie électronique professionnelle est réservé aux besoins professionnels. Un usage privé, limité et raisonnable, est toléré; le cas échéant, les messages n'apparaissant pas d'emblée comme privés pourront être consultés.

[2] L'utilisation de l'adresse de messagerie étatique comme identifiant sur des sites tiers n'est autorisée qu'en lien avec des besoins professionnels.

[3] L'expéditeur d'un courrier électronique (ci-après: courriel) est responsable de son envoi et en assume les éventuelles conséquences. Il est notamment interdit de:

a) transférer des courriels à caractère professionnel sur une adresse privée;

b) diffuser des informations pouvant porter atteinte à la réputation de l'Etat du Valais;

c) diffamer des personnes, des entreprises ou porter atteinte à la personnalité d'autrui.

[4] L'utilisateur est tenu d'assurer l'acheminement des courriels reçus par erreur ou de les retourner à l'expéditeur, exception faite des envois de masse de type spam.

[5] Tout courriel en rapport avec des chaînes de lettres ou du spamming doit être détruit.

[6] L'utilisateur supprime régulièrement les courriels obsolètes et classe les courriels à conserver. La corbeille est vidée régulièrement de façon automatisée.

[7] En cas d'absence supérieure à un jour, l'utilisateur prend les mesures nécessaires pour assurer une notification à ses courriels entrants. Celle-ci doit mentionner la durée de l'indisponibilité et mentionner qui contacter en cas d'urgence. Le cas échéant, sur demande du chef de service, la fonction informatique peut insérer un message d'absence.

[8] Les courriels sortants doivent être accompagnés de la signature et du titre officiel selon les prescriptions mises en place par IVS.

[9] L'utilisateur est rendu attentif au fait qu'un courriel n'offre pas plus de confidentialité qu'une carte postale. De ce fait, les courriels contenant des données personnelles, sensibles ou confidentielles doivent être chiffrés au moyen d'une solution expressément autorisée par la fonction sécurité de l'information.

[10] La mise en place de règles de transfert automatique des courriels vers une messagerie tierce est prohibée, toute exception nécessite une autorisation préalable du responsable de la sécurité de l'information compétent.

[11] La synchronisation de la messagerie sur smartphone ou tablette est uniquement autorisée au travers des solutions mises à disposition par la fonction informatique.

[12] L'accès à la messagerie professionnelle depuis Internet (webmail) ne doit être effectué que depuis un poste de confiance, les Internet cafés ou bornes d'aéroport sont notamment à proscrire.

[13] L'utilisateur doit adopter la plus grande vigilance vis-à-vis des courriels entrants, il doit s'assurer de la plausibilité du message, de l'identité de l'émetteur. Dans tous les cas il agit avec prudence avant d'ouvrir tout fichier joint. Il pourra être tenu pour potentiel responsable des dégâts qu'il aura engendré par un comportement inapproprié ou par négligence grave ou répétée.

[14] L'utilisation de messageries privées (Google, Microsoft, Yahoo!, etc.) est formellement prohibée, sauf autorisation préalable de sa hiérarchie (chef de service ou de département).

Art. 9 Internet, réseaux sociaux et cloud computing

[1] L'utilisation d'Internet à titre privé est tolérée dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (espaces de stockage, bande passante), ni ne viole le devoir de fidélité et de diligence de l'utilisateur.

[2] L'accès à Internet est filtré et journalisé. L'accès aux sites non autorisés, notamment ceux portant atteinte au fonctionnement ou à la sécurité du système d'information de l'Etat, ainsi que ceux correspondants à la description faite dans l'article 5, alinéa 3 de la présente directive est bloqué par la fonction sécurité de l'information. Le fait qu'un site qui devrait être bloqué puisse malgré tout être consulté ne diminue en rien la responsabilité de l'utilisateur et l'importance des éventuelles sanctions qui pourraient être prises.

[3] La diffusion d'informations relatives à l'Etat du Valais sur Internet est encadrée par les règles établies par IVS.

[4] La présence et l'activité des utilisateurs sur les réseaux sociaux est régie par les règles établies par IVS.

[5] L'utilisateur s'engage à ne pas diffuser d'informations appartenant à des tiers sans leur autorisation, à mentionner ses sources lors de l'utilisation d'informations récupérées sur Internet et à respecter la législation sur le droit d'auteur.

[6] L'utilisateur n'est pas autorisé à s'abonner à des services d'information payants, sauf autorisation préalable de sa hiérarchie (chef de service ou de département).

[7] L'accès aux sites de réseaux sociaux depuis le réseau de l'Etat du Valais est assujetti à autorisation formelle et préalable.

[8] L'utilisation de services informatiques dans le nuage ou cloud (partage de fichiers en ligne, collaboration en ligne, etc.) est sujette à autorisation, exception faite des services officiellement autorisés ou proposés par la fonction informatique.

Art. 10 Téléphonie

[1] L'utilisation de la téléphonie fixe pour un usage privé est tolérée, à titre exceptionnel.

[2] La déviation d'un poste fixe vers un appareil mobile hors convention avec l'Etat du Valais n'est pas autorisée.

[3] Les forfaits téléphoniques sont régis par la directive spécifique émise par le SCI.

[4] Le collaborateur est tenu de répondre au téléphone lorsqu'il se trouve sur sa place de travail.

[5] La définition de la zone géographique d'appel relève de la compétence du chef de service.

[6] L'utilisation de la téléphonie fixe comme moyen de connexion à un réseau externe est strictement interdite.

[7] L'utilisation de services payants, ainsi que la commande de biens portée directement en débit sur la facture téléphonique sont interdites, sauf autorisation formelle et préalable.

[8] Les solutions de téléphonie Internet non fournies par la fonction informatique sont prohibées.

Art. 11 Départ du collaborateur

[1] Au départ (dernier jour de travail) d'un collaborateur, et sans dispositions expresses contraires, l'ensemble de ses comptes informatiques sont immédiatement désactivés.

[2] Le collaborateur doit supprimer, avant son départ, toutes les données privées.

[3] Une fois que le collaborateur a quitté son poste, son service peut disposer et consulter toutes les données résultantes et si besoin mettre en place une réponse automatique pendant un mois.

[4] Sauf demande expresse contraire, la boîte de messagerie et l'espace de stockage personnel seront définitivement effacés un mois après le départ du collaborateur.

[5] Le collaborateur doit retourner l'ensemble du matériel mis à sa disposition par l'Etat du Valais dans le cadre de son activité (ordinateur portable, téléphone cellulaire, clés, badges, systèmes de stockage externes, documentation, etc.).

[6] En cas de départ immédiat d'un collaborateur, la fonction informatique bloque immédiatement ses accès et insère un message d'absence sur sa messagerie. Les procédures liées à la démission ou résiliation ordinaire sont aussi appliquées, cependant, la suppression des données privées s'effectue sous supervision hiérarchique, le cas échéant, et sauf urgence, en présence du collaborateur qui y est invité.

[7] En cas d'absence non planifiée d'un collaborateur (décès, accident ou maladie), lorsque l'autorisation d'accès de ce dernier ne peut être obtenue alors que la bonne marche du service l'exige, l'accès aux informations professionnelles de sa messagerie peut tout de même être obtenu dans le respect strict des conditions ci-après:

a) l'aval officiel de sa hiérarchie est obligatoire (chef de service ou de département);

b) l'accès ne peut qu'être temporaire;

c) la présence d'un collaborateur du SRH (membre de la direction ou collaborateur en charge du service) ou de la fonction sécurité de l'information est requise.

[8] La tenue d'un protocole horodaté, signé par les intervenants, indiquant tout ce qui a été entrepris, est indispensable.

[9] En cas de décès, il sera procédé à une pondération des intérêts en présence avant d'accéder à toute demande des proches du défunt.

Art. 12 Mesures de surveillance

[1] La fonction informatique est chargée d'effectuer, dans le respect de la LIPDA, des contrôles statistiques anonymisés de l'utilisation des systèmes d'information (messagerie, accès Internet, etc.) mis à disposition des collaborateurs, ceci pour d'une part assurer la sécurité et le bon fonctionnement technique de ces systèmes, et d'autre part, vérifier de manière générale l'application des présentes directives.

[2] Lorsqu'un dérangement technique perturbe ou met en péril le bon fonctionnement des systèmes d'information et de télécommunication, la fonction informatique est autorisée à prendre toutes les mesures nécessaires pour rétablir une situation normale, à l'exclusion de la prise de connaissance des données ressortant comme étant d'ordre privé. Les fichiers journaux peuvent être analysés afin d'établir le diagnostic des problèmes techniques.

[3] Les chefs de service et d'établissement peuvent demander, en cas de soupçons, à la fonction informatique d'effectuer des contrôles anonymisés de l'utilisation des systèmes d'information faite par leurs collaborateurs.

[4] La même compétence est attribuée aux chefs de département pour les services rattachés à leur département.

[5] En cas de non-respect présumé des présentes directives, révélé par les contrôles précités, ou d'autres éléments, les chefs de service et d'établissement, respectivement les chefs de département, peuvent demander à la fonction informatique de procéder à des contrôles individualisés portant sur l'utilisation des Systèmes d'information.

[6] Ce contrôle ne pourra pas porter sur les fichiers et messages apparaissant comme de nature exclusivement privée.

[7] Les utilisateurs doivent être informés préalablement de la tenue de ces contrôles individualisés, hormis s'il y a suspicion d'actes relevant du droit pénal.

[8] Si les soupçons de non-respect des présentes directives sont avérés, le contrôle pourra être étendu à la période antérieure à l'information.

[9] En cas de confirmation des soupçons de non-respect des présentes directives, sont applicables, sous réserve des cas bagatelle, les dispositions du chapitre 4 «Conséquences des violations des devoirs de service» de la Lc-Pers

[10] Lorsqu'il y a suspicion d'actes pouvant relever du droit pénal, la fonction informatique informe le chef de département concerné, lequel décide des mesures à prendre.

[11] S'il y a constat ou forte suspicion d'une infraction pénale qui se poursuit d'office, la fonction informatique informe immédiatement l'autorité compétente, le chef de département concerné et le Conseil d'Etat.

[12] Le service ou l'établissement concerné, en collaboration avec le responsable sécurité de l'information compétent, prend les mesures forensiques nécessaires pour la sauvegarde des éléments de preuve pertinents, en vue de l'ouverture d'éventuelles procédures administratives ou pénales.

[13] Il traite confidentiellement le résultat et les données recueillies pour les besoins de l'enquête.

[14] Lorsqu'il est certain que les données individualisées ne serviront pas à d'éventuelles procédures, elles devront être détruites dans les quatre semaines.

[15] La surveillance abusive peut donner lieu à enquête sur demande de l'utilisateur contrôlé individuellement.

[16] Le Conseil d'Etat désigne l'organe d'instruction, lequel doit présenter toute garantie d'impartialité.

[17] Demeurent réservées les dispositions concernant la protection des données.

[18] En cas de non-respect des présentes directives, la fonction informatique restreindra ou bloquera l'accès aux systèmes d'information.

Art. 13 Dispositions finales

[1] Les chefs de service et d'établissement informent leurs collaborateurs des droits et obligations arrêtés dans les présentes directives. Lors de l'entrée en vigueur des présentes directives, ils en transmettent une copie à leurs collaborateurs. La même procédure s'applique lors de l'engagement de nouveaux collaborateurs.

[2] Les chefs de service et d'établissement sont responsables de l'application des présentes directives dans leur fonction de conduite, sous réserve des compétences des autres organes.

[3] La fonction informatique est chargée de veiller à la mise à jour des présentes directives en fonction de l'évolution des technologies de l'information et de la communication, ainsi que pour tenir compte des expériences faites. Les propositions de modification par la fonction informatique seront soumises au Conseil d'Etat pour décision.

[4] La Chancellerie d'Etat est chargée de la notification des présentes directives à tous les chefs de service et d'établissements.

II.

Aucune modification d'autres actes.

III.

Aucune abrogation d'autres actes.

IV.

Le présent acte législatif entre en vigueur le 1er novembre 2021.

Sion, le 27 octobre 2021

Le président du Conseil d'Etat: Frédéric Favre
Le chancelier d'Etat: Philipp Spörri

La présente directive remplace les directives concernant les moyens informatiques et la téléphonie du 21 décembre 2005.