
Règlement d'accès et d'utilisation de la plateforme numérique SIROUT (ReSi)

du 08.07.2026 (état 01.07.2026)

Le Conseil d'Etat du canton du Valais

vu les articles 16 à 19 de la loi d'application de la législation fédérale sur la circulation routière du 12 juin 2025 (LALCR);

vu le règlement de la commission cantonale de signalisation routière du 16 février 2025 (RCCSR);

sur proposition du département en charge de la mobilité,

ordonne: ¹⁾

1 Dispositions générales

Art. 1 **Objet et champ d'application**

¹ Le présent règlement définit les modalités d'accès et d'utilisation de la plateforme numérique SIROUT au sens des articles 16 à 19 de la loi d'application de la législation fédérale sur la circulation routière (LALCR) (ci-après: SIROUT) permettant le traitement des dossiers relatifs aux actes de procédure prévus par les articles 9, 12 et 13 du règlement de la commission cantonale de signalisation routière (RCCSR) par l'autorité compétente au sens de l'article 5 RCCSR (ci-après: autorité compétente).

² Il s'applique à tous les actes de procédure prévus par les articles 9, 12 et 13 RCCSR traités via SIROUT.

³ Tout utilisateur de SIROUT est soumis au présent règlement.

¹⁾ Dans le présent règlement toute désignation de personne, de statut ou de fonction vise indifféremment l'homme ou la femme.

* Tableaux des modifications à la fin du document

Art. 2 Définitions

¹ Au sens du présent règlement, on entend par:

- a) authentification: procédure qui consiste à vérifier et prouver, au moyen des données retenues lors de la procédure d'identification, l'identité d'un utilisateur avant de l'autoriser à accéder à des ressources comme son compte d'utilisateur ou ses documents;
- b) canaux de communication numérique: moyen de transmission des informations numériques entre un expéditeur et un destinataire, notamment, courriel, téléchargement de document, accès par une application web, etc;
- c) compte d'utilisateur: droit d'accès attribué à SIROUT, associé à un nom d'utilisateur, à un rôle et à un mot de passe;
- d) confidentiel: caractère d'une donnée qui doit être protégée contre tout accès indu de tiers, que ce soit en application de la loi ou en raison d'une décision administrative;
- e) identification: procédure permettant d'établir de manière sûre une correspondance entre l'identité physique et l'identité numérique d'un utilisateur et de l'associer à des données qui lui sont propres, en vue de l'authentifier par la suite;
- f) moyen d'identification électronique (MIE): élément électronique utilisé pour l'identification et l'authentification d'un utilisateur, dont il existe deux niveaux:
 - 1. vérifié niveau 1: nécessite une pièce d'identité valable reconnue par le fournisseur du MIE et une adresse email valide,
 - 2. vérifié niveau 2: nécessite un passeport reconnu par le fournisseur du MIE et une adresse email valide;
- g) SIROUT: ensemble de composants matériels et logiciels du système d'information permettant la gestion ou l'utilisation des prestations numériques pour la gestion de demandes en lien avec la signalisation routière et le marquage sur les routes ouvertes au trafic;
- h) sécurité des données: ensemble des mesures organisationnelles (sécurité de l'information) et techniques (sécurité opérationnelle) permettant d'assurer la protection de la confidentialité, de l'intégrité et de la disponibilité des informations, données et systèmes informatiques de l'autorité compétente; d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation, la conformité à la loi et aux standards, ainsi que la fiabilité, peuvent également être concernées; ces mesures intègrent les mesures organisationnelles de protection du patrimoine informationnel, en particulier la gestion des accès;

- i) système de gestion de la protection des données: ensemble des mesures et processus mis en œuvre pour assurer la sécurité des données personnelles et confidentielles;
- j) utilisateur: toute personne physique qui utilise SIROUT à quelque titre que ce soit;
- k) validation: processus par lequel l'utilisateur clique sur le bouton de SIROUT "soumettre".

2 Modalités d'accès et d'utilisation

Art. 3 SIROUT

¹ Tout accès à SIROUT nécessite une connexion internet. Le lien d'accès est disponible sur le site web officiel de l'Etat du Valais et de la commission cantonale de signalisation routière.

² Lors de sa toute première connexion, chaque utilisateur doit effectuer une procédure d'identification grâce à un MIE qu'il a acquis préalablement, ceci lui permettant de créer son compte d'utilisateur et ainsi d'obtenir son identifiant électronique. La liste des MIE acceptés par SIROUT est publiée sur le site web de l'Etat du Valais.

³ Il est nécessaire pour l'utilisateur de disposer:

- a) d'un MIE vérifié niveau 1 pour effectuer toute action au sein de SIROUT, notamment pour le dépôt et la gestion des dossiers;
- b) d'un MIE vérifié niveau 2 pour apposer une signature électronique qualifiée sur les décisions.

⁴ Une fois le processus d'identification terminé, l'identifiant électronique créé par l'utilisateur est associé à un compte utilisateur permettant l'accès à SIROUT.

⁵ Dans le cadre de son activité pour l'Etat du Valais, est exemptée du processus d'identification toute personne employée par l'Etat du Valais possédant déjà un compte d'utilisateur professionnel délivré par le service cantonal en charge de l'informatique.

⁶ Un ou plusieurs rôles sont attribués à l'utilisateur par l'autorité compétente, qui définit les accès et les fonctionnalités de l'utilisateur.

⁷ L'utilisateur peut se voir attribuer, notamment, les rôles suivants:

- a) administrateur;
- b) inspecteur CCSR;

- c) membre CCSR;
- d) requérant Canton;
- e) requérant Commune;
- f) secrétariat;
- g) service cantonal.

⁸ Un utilisateur peut créer plusieurs identifiants électroniques, privés et professionnels. Les employés de l'Etat et des communes ainsi que les membres des autorités cantonales et communales utilisent, dans l'exercice de leurs fonctions, leur compte d'utilisateur professionnel.

Art. 4 Dossier

¹ Le dossier regroupe toutes les pièces relatives aux actes de procédure prévus par les articles 16 à 19 LALCR et les articles 9, 12 et 13 RCCSR.

² Le dossier est reconnu comme constitué et la procédure débutée lorsque la validation a été opérée par le requérant.

³ Si une validation n'a pas été opérée dans un délai de 1 an après la création du dossier, celui-ci sera supprimé définitivement.

⁴ Toutes les communications relatives au traitement du dossier sont effectuées via SIROUT.

⁵ Chaque dossier possède un numéro de référence unique généré par SIROUT.

⁶ L'autorité compétente est responsable de la gestion des accès aux dossiers.

3 Relations entre SIROUT et les utilisateurs

Art. 5 Canaux de communication électronique

¹ La communication électronique s'effectue par tout canal électronique proposé sur SIROUT et accepté par l'utilisateur lors de la première connexion via SIROUT. L'acceptation vaut pour toutes les demandes créées ultérieurement.

Art. 6 Dépôt et validation des documents

¹ Tous les documents sont déposés sur SIROUT au format PDF.

² Il est de la responsabilité de l'utilisateur de prévoir l'infrastructure nécessaire notamment au dépôt, à l'ouverture et à la lecture de documents supportés par SIROUT.

³ Tous les documents déposés sur SIROUT sont validés par les rôles désignés par l'autorité compétente.

⁴ Si un document ne peut être ouvert ou lu par l'autorité compétente, cette dernière impartit un délai à l'utilisateur qui a déposé le document pour lui transmettre le document en question au format et par les canaux de communication qu'elle spécifie.

Art. 7 Consultation des organes cantonaux

¹ Le processus de consultation des organes cantonaux se fait, à défaut d'une base légale impérative contraire, par le biais de SIROUT.

4 Notification des décisions

Art. 8 Notification électronique

¹ La notification des décisions relevant du présent règlement s'effectue par voie électronique via SIROUT.

² Chaque utilisateur peut consulter sur SIROUT la date et l'heure de la notification.

Art. 9 Format

¹ La décision est notifiée au format PDF.

² Il est de la responsabilité de l'utilisateur de prévoir l'infrastructure nécessaire, notamment au dépôt, à l'ouverture et à la lecture du format PDF.

5 Protection des données et archivage

Art. 10 Système de gestion de la protection des données

¹ Les dispositions en matière de protection des données de la loi sur l'information du public, la protection des données et l'archivage (LIPDA) sont applicables.

Art. 11 Communication de données

¹ Les données SIROUT peuvent être communiquées aux organes cantonaux consultés dans le cadre du processus de consultation.

Art. 12 Sauvegarde et archivage

¹ Les dossiers sont sauvegardés de façon périodique sur un support adéquat. L'accès au dossier doit être garanti en tout temps et l'intégrité des documents doit être assurée.

² L'archivage et l'accès aux archives sont coordonnés avec les archives cantonales de l'Etat du Valais et doivent être conformes à la LIPDA.

6 Obligations et responsabilités

Art. 13 Obligations et responsabilités de l'utilisateur

¹ En accédant à SIROUT, l'utilisateur accepte expressément que ses données personnelles soient traitées et utilisées dans la mesure où cela est nécessaire au traitement de tous les actes de procédure prévus par la LALCR et le RCCSR.

² L'utilisateur est responsable de la mise à jour constante de ses données qu'il a déclarées sur SIROUT.

³ L'utilisateur qui reçoit de la part de l'autorité compétente une communication qui ne lui est pas destinée doit le signaler immédiatement à l'expéditeur.

⁴ L'utilisateur est responsable des actes qui sont exécutés sous couvert de son propre compte d'utilisateur.

Art. 14 Responsabilité de l'Etat

¹ La responsabilité de l'autorité compétente est exclusivement régie par la loi sur la responsabilité des collectivités publiques et de leurs agents.

² L'autorité compétente n'est pas tenue responsable d'éventuelles atteintes, directes ou indirectes, de quelque nature que ce soit, à la confidentialité ou à la qualité des données étrangères à SIROUT. L'autorité compétente met toutefois en œuvre les moyens opérationnels et organisationnels adéquats afin d'assurer la sécurité des données traitées par ses systèmes d'information.

³ L'autorité compétente ne garantit pas un accès continu à SIROUT. L'accès à SIROUT peut être suspendu, notamment – mais pas exclusivement – en cas d'avarie technique, d'acte de malveillance, d'opérations de maintenance ou de tout autre cas de force majeure. L'autorité compétente n'est pas tenue responsable des conséquences découlant d'une suspension de l'accès à SIROUT.

Art. 15 Utilisation abusive de SIROUT

¹ L'accès à SIROUT est bloqué en cas d'utilisation abusive de celle-ci.

² Les documents n'ayant pas de rapport avec le dossier au sens de l'article 4 alinéa 1 dans lequel ils ont été déposés sont supprimés par l'autorité compétente.

³ Le blocage est communiqué par le canal électronique de l'utilisateur et un délai lui est octroyé pour respecter le règlement et rétablir un état conforme au droit.

⁴ Le droit pénal demeure réservé.

Tableau des modifications par date de décision

Adoption	Entrée en vigueur	Elément	Modification	Source publication
08.07.2026	01.07.2026	Acte législatif	première version	RO/AGS 2026-094

Tableau des modifications par disposition

Élément	Adoption	Entrée en vigueur	Modification	Source publication
Acte législatif	08.07.2026	01.07.2026	première version	RO/AGS 2026-094