

Loi sur la sécurité de l'information et la cybersécurité (LSIC)

du [date]

Acte(s) législatif(s) de la présente publication :

Nouveau : **???.???**

Modifié(s) : 551.1

Abrogé(s) : –

Le Grand Conseil du canton de Berne,

vu l'article 18, alinéa 3 et l'article 37 de la Constitution cantonale¹⁾,

sur proposition du Conseil-exécutif,

arrête:

I.

L'acte législatif **???.???** intitulé Loi sur la sécurité de l'information et la cybersécurité (LSIC) est publié en tant que nouvel acte législatif.

1 Dispositions générales

Art. 1 *But*

¹ La présente loi vise à garantir la sécurité des informations lors de leur traitement et la sécurité de l'utilisation d'outils TIC par les autorités.

² Elle protège les intérêts publics suivants:

- a* la capacité d'action et de décision des autorités,
- b* la sécurité et l'ordre public,
- c* le respect des obligations légales et contractuelles des autorités en matière de protection des informations.

¹⁾ RSB [101.1](#)

Art. 2 *Champ d'application*

¹ La présente loi s'applique aux autorités cantonales et aux communes au sens de la Constitution cantonale (titres 5 et 7), sous réserve de l'alinéa 2.

² Ne s'appliquent aux autres organisations chargées de tâches publiques et aux communes que les dispositions sur

- a* les informations classifiées, lorsqu'elles traitent des informations classifiées du canton ou de la Confédération;
- b* la sécurité de l'utilisation d'outils TIC, lorsqu'elles se servent d'outils TIC du canton ou de la Confédération.

Art. 3 *Relation avec d'autres lois*

¹ Les articles 27 à 31a de la loi du 2 novembre 1993 sur l'information et l'aide aux médias (LIAM)²⁾ priment la présente loi.

² La présente loi s'applique à titre supplétif

- a* aux informations dont la protection est aussi réglée dans des lois fédérales ou dans d'autres lois cantonales;
- b* pour la protection de données personnelles au sens de l'article 2, alinéa 1 de la loi du 19 février 1986 sur la protection des données (LCPD)³⁾.

Art. 4 *Définitions*

¹ Dans la présente loi, il est entendu par

- a* sécurité de l'information: confidentialité, disponibilité, intégrité et traçabilité des informations
 - 1. confidentialité: les informations ne sont accessibles qu'aux personnes autorisées;
 - 2. disponibilité: les informations sont disponibles lorsqu'elles sont nécessaires;
 - 3. intégrité: les informations ne peuvent pas être modifiées sans autorisation ni par mégarde;
 - 4. traçabilité: la source et l'auteur du traitement des informations sont identifiables;
- b* cybersécurité: sécurité de l'information lors de la transmission de données via des réseaux;
- c* outils TIC: biens et services des technologies de l'information et de la communication (TIC) incluant les logiciels et le matériel.

²⁾ RSB [107.1](#)

³⁾ RSB [152.04](#)

2 Principes

Art. 5 *Obligations des autorités*

¹ Chaque autorité veille à ce que

- a* les besoins de protection des informations relevant de son domaine de responsabilité soient évalués;
- b* la confidentialité, la disponibilité, l'intégrité et la traçabilité des informations au sens de la lettre a soient garanties en fonction de leur besoin de protection;
- c* ses outils TIC soient protégés contre les utilisations abusives et les perturbations et que
- d* la sécurité de l'information soit régulièrement contrôlée.

² Elle assure la gestion des risques

- a* en évaluant constamment les risques pour la sécurité de l'information;
- b* en prenant les mesures nécessaires pour les éliminer ou les réduire à un niveau tolérable et
- c* en documentant son acceptation des risques inévitables.

³ Elle prend en compte les principes d'adéquation, de rentabilité et de facilité d'emploi.

Art. 6 *Tiers mandatés*

¹ L'autorité qui mandate des tiers veille à ce que

- a* ces tiers soient liés par les exigences et les mesures découlant de la présente loi;
- b* la mise en œuvre des exigences et des mesures découlant de la présente loi fasse l'objet d'un contrôle approprié et que
- c* le non-respect des exigences et des mesures découlant de la présente loi soit sanctionné.

Art. 7 *Réactivité et planification préventive*

¹ Les autorités veillent

- a* à détecter rapidement toute atteinte à la sécurité de l'information, à en éliminer les causes et à en réduire les répercussions au minimum;
- b* à concevoir des plans d'action pour les cas d'atteinte grave à la sécurité de l'information pouvant menacer l'accomplissement de tâches cantonales de grande importance pour la population;
- c* à mettre en œuvre et à actualiser régulièrement ces plans d'action.

3 Mesures concernant l'organisation

Art. 8 *Classification*

¹ Les autorités classifient les informations qui sont susceptibles de nuire aux intérêts publics selon l'article 1, alinéa 2, lettres a et b si une personne non autorisée en prend connaissance.

² La classification comporte les échelons suivants:

- a «interne», si l'information dont une personne non autorisée prend connaissance peut nuire aux intérêts publics;
- b «confidentiel», si l'information dont une personne non autorisée prend connaissance peut nuire considérablement aux intérêts publics;
- c «secret», si l'information dont une personne non autorisée prend connaissance peut nuire gravement aux intérêts publics.

³ Elle doit se limiter au strict nécessaire et être si possible temporaire.

⁴ Le Conseil-exécutif règle la classification et la déclassification par voie d'ordonnance.

Art. 9 *Accès aux informations classifiées*

¹ Seules ont accès aux informations classifiées les personnes

- a offrant la garantie qu'elles ne portent pas atteinte aux intérêts publics au sens de l'article 1, alinéa 2 et
- b qui ont besoin de ces informations pour accomplir leurs tâches légales ou contractuelles.

² L'accès à des archives classifiées est régi par les dispositions de la législation sur l'archivage.

Art. 10 *Accès en procédure spéciale*

¹ L'accès à des informations classifiées du Grand Conseil et des Services parlementaires ainsi que des autorités judiciaires et du Ministère public est régi, sous réserve de l'alinéa 2, par les dispositions de la législation spéciale.

² Avant d'autoriser l'accès à une information classifiée au sens de l'alinéa 1, l'autorité parlementaire, administrative ou judiciaire compétente en la matière entend le service qui a classifié ladite information.

4 Mesures techniques

4.1 Procédure de sécurité

Art. 11 *But*

¹ Le Conseil-exécutif ou l'organe de l'administration cantonale qu'il a désigné définit une procédure permettant de garantir la sécurité de l'information lors de l'utilisation d'outils TIC.

Art. 12 *Contenu*

¹ La procédure de sécurité comprend en particulier

- a* l'évaluation des besoins concernant la protection des informations avant l'utilisation d'outils TIC,
- b* la définition de la catégorie de sécurité correspondant aux besoins de protection ainsi que des mesures de sécurité appropriées,
- c* la mise en œuvre des mesures de sécurité et le contrôle de celles-ci,
- d* la désignation de l'organe habilité à attester la sécurité des outils TIC et à assumer les risques restants,
- e* la marche à suivre en cas de changement concernant les risques.

Art. 13 *Catégorie de sécurité*

¹ La catégorie de sécurité des outils TIC est

- a* «protection très élevée» lorsqu'une violation de la sécurité de l'information peut nuire gravement aux intérêts mentionnés à l'article 1, alinéa 2;
- b* «protection élevée» lorsqu'une violation de la sécurité de l'information peut nuire considérablement aux intérêts mentionnés à l'article 1, alinéa 2;
- c* «protection de base» dans les autres cas.

Art. 14 *Compétence*

¹ L'application de la procédure de sécurité relève de la compétence de l'autorité qui utilise les outils TIC pour accomplir ses tâches légales ou qui les met à la disposition d'autres autorités.

Art. 15 *Délégation*

¹ Le Conseil-exécutif peut régler par voie d'ordonnance les mesures de protection à prendre pour les informations, pour les outils TIC et pour les données personnelles, en fonction

- a* de la classification des informations,
- b* de la catégorie de sécurité des outils TIC et

- c du besoin de protection des données personnelles conformément à la législation sur la protection des données.

4.2 Sécurité de l'exploitation

Art. 16

¹ Chaque autorité garantit, dans son domaine de responsabilité, la sécurité des outils TIC qu'elle exploite pour elle-même ou sur mandat d'une autre autorité.

5 Mesures physiques

Art. 17 *Principe*

¹ Chaque autorité assure, dans son domaine de responsabilité, une protection physique appropriée des informations et des outils TIC.

Art. 18 *Zones de sécurité*

¹ Chaque autorité peut définir comme zones de sécurité des locaux ou des secteurs dans lesquels

- a des informations classifiées à l'échelon «secret» sont régulièrement traitées ou
- b des outils TIC de la catégorie de sécurité «protection très élevée» sont exploités.

² Dans les zones de sécurité, elles peuvent

- a interdire le port de certains objets, en particulier d'appareils d'enregistrement;
- b surveiller des secteurs sensibles au moyen d'appareils d'enregistrement;
- c procéder à des fouilles;
- d procéder de manière inopinée à des contrôles des locaux, y compris en l'absence des personnes employées;
- e exploiter des installations perturbatrices au sens de l'article 34, alinéa 1^{er} de la loi fédérale du 30 avril 1997 sur les télécommunications (LTC)⁴⁾.

6 Mesures concernant les personnes

6.1 Sélection, formation et habilitation

Art. 19

¹ Chaque autorité veille à ce que les personnes ayant accès à ses informations, ses outils TIC, ses locaux et ses autres infrastructures

⁴⁾ RS [784.10](#)

- a soient sélectionnées soigneusement et identifiées en fonction des risques, bénéficient d'une formation, initiale et continue, conforme à leur fonction, et soient le cas échéant tenues de garder le secret et de faire preuve d'une vigilance particulière;
- b ne soient habilitées à accéder qu'aux informations, outils TIC, locaux et autres infrastructures qui leur sont nécessaires pour accomplir leurs tâches légales ou contractuelles.

² Le canton met à la disposition des autres organisations chargées de tâches publiques et des communes, contre rémunération, les formations et perfectionnements nécessaires.

6.2 Contrôle de sécurité relatif aux personnes

Art. 20 But

¹ Le contrôle de sécurité des personnes sert à évaluer si l'accès d'une personne à des informations ou à des installations sensibles dans l'exercice de ses fonctions ou dans le cadre de l'exécution d'un mandat pourrait présenter un risque pour la sécurité de l'information ou des installations.

² Il consiste à recueillir les données relatives à la loyauté de la personne contrôlée, notamment à ses éventuelles activités pénalement répréhensibles et à sa situation financière, qui sont nécessaires à l'évaluation au sens de l'alinéa 1.

Art. 21 Degrés de contrôle

¹ Le contrôle de sécurité relatif aux personnes prend la forme d'un contrôle de base ou d'un contrôle élargi.

² Lors du contrôle de sécurité de base, l'autorité de contrôle peut

- a recueillir des données du casier judiciaire ou des registres des offices des poursuites et des faillites;
- b tenir compte d'informations extraites de sources publiques ou de ses propres dossiers;
- c interroger la personne concernée;
- d interroger des tiers si la personne concernée y consent.

³ Lors du contrôle de sécurité élargi, l'autorité de contrôle peut en outre demander à la Police cantonale de recueillir des données

- a des systèmes de traitement de données de la Police cantonale au sens de l'article 143 de la loi du 10 février 2019 sur la police (LPol)⁵⁾,

⁵⁾ RSB [551.1](#)

b des systèmes de traitement de données de la Confédération ou d'autres cantons, dans la mesure où la Police cantonale s'est vu conférer un accès direct conformément à l'article 147 LPol.

⁴ La Police cantonale ne communique à l'autorité de contrôle les données visées à l'alinéa 3 que dans la mesure requise par le but du contrôle. Si les données s'y prêtent, elle les anonymise et les résume.

Art. 22 *Conditions*

¹ Le contrôle de sécurité de base peut être réalisé lorsque la personne à contrôler est dans l'une ou l'autre des situations suivantes:

- a* elle a accès soit fréquemment, soit en grand nombre à
 1. des informations classifiées «confidentiel»,
 2. des données personnelles sensibles, dont la publication pourrait porter gravement atteinte aux droits de la personnalité des personnes concernées;
- b* elle a accès à d'importantes affaires politiques ou sensibles;
- c* elle a accès à des installations sensibles ou à des zones de sécurité au sens de l'article 18;
- d* elle exerce une activité présentant des risques similaires.

² Le contrôle de sécurité élargi peut être réalisé lorsque la personne à contrôler est dans l'une ou l'autre des situations suivantes:

- a* elle a accès, soit fréquemment, soit en grand nombre à
 1. des informations classifiées «secret»,
 2. des données personnelles, dont la publication pourrait porter gravement atteinte à l'intégrité physique des personnes concernées;
- b* elle a accès à des installations sensibles ou à des zones de sécurité au sens de l'article 18 soit régulièrement, soit sans accompagnement;
- c* elle exerce une activité présentant des risques similaires.

Art. 23 *Personnes à contrôler*

¹ Les autorités suivantes règlent, chacune pour leur domaine, le degré de contrôle valant pour chaque fonction:

- a* le Grand Conseil pour les personnes qu'il a élues ainsi que pour les personnes employées ou mandatées par lui ou par les Services parlementaires: par voie d'instruction du Bureau;
- b* le Conseil-exécutif pour les personnes qu'il a nommées ainsi que pour les personnes employées ou mandatées par les Directions et la Chancellerie d'État: par voie d'ordonnance;

c la Direction administrative de la magistrature pour les personnes employées ou mandatées par les autorités judiciaires ou le Ministère public: par voie d'instruction.

² Le Conseil-exécutif peut décider, par ordonnance, que la réglementation prévue à l'alinéa 1, lettre b relative aux personnes employées ou mandatées soit fixée par voie d'instructions des Directions, de la Chancellerie d'État ou d'organes spécialisés de l'administration.

³ Pour les juges ainsi que pour la procureure générale ou le procureur général et sa suppléance, le contrôle se limite à recueillir des données du casier judiciaire ou des registres des offices des poursuites et des faillites avant leur élection et à demander d'éventuels renseignements complémentaires à ces personnes. Ce contrôle peut être renouvelé en cas de réélection.

Art. 24 *Autorité de contrôle*

¹ Les personnes employées par une autorité sont contrôlées par leur autorité d'engagement.

² Les personnes mandatées par une autorité sont contrôlées par l'autorité qui a établi le mandat.

³ Les personnes candidates à l'élection au sein d'une autorité sont contrôlées

a par l'autorité qui propose leur candidature;

b par l'autorité d'élection lorsque leur candidature n'est pas proposée par une autorité.

Art. 25 *Contrôle par le service spécialisé de la Confédération chargé des contrôles de sécurité relatifs aux personnes*

¹ À la demande des autorités de contrôle au sens de l'article 24, les responsables de la sécurité du Grand Conseil, des Directions, de la Chancellerie d'État ainsi que des autorités judiciaires et du Ministère public peuvent exceptionnellement, dans l'un ou l'autre des cas suivants, confier le contrôle de sécurité élargi relatif aux personnes au service spécialisé compétent de la Confédération:

a l'activité exercée présente un risque particulièrement élevé;

b la personne contrôlée a un lien avec l'étranger qui pourrait présenter des risques;

c il semble opportun que la personne contrôlée soit interrogée par des spécialistes.

² Dans ce cas, la portée et la procédure du contrôle de sécurité élargi sont régis par les articles 34 à 40 de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information (loi sur la sécurité de l'information, LSI)⁶⁾ ainsi que par les dispositions d'exécution correspondantes du droit fédéral.

³ L'autorité de contrôle peut renoncer à soumettre une personne au contrôle de sécurité lorsque celle-ci produit une déclaration de sécurité établie par le service spécialisé de la Confédération (art. 39 LSI) et que le délai de renouvellement (art. 30) n'est pas encore échu.

Art. 26 *Consentement et collaboration*

¹ Aucun contrôle de sécurité ne peut être réalisé sans le consentement de la personne à contrôler.

² La personne soumise au contrôle est tenue de collaborer à l'établissement des faits.

Art. 27 *Réserve de la législation fédérale*

¹ Les dispositions de la législation fédérale sur la sécurité de l'information sont réservées pour les personnes qui traitent des informations fédérales classifiées ou ont accès à des outils TIC de la Confédération.

Art. 28 *Résultat*

¹ L'autorité de contrôle communique les résultats du contrôle de sécurité à la personne contrôlée.

² La personne contrôlée peut consulter le dossier correspondant dans les dix jours et demander la rectification de données inexactes. Ce délai peut être prolongé dans des cas motivés.

³ L'autorité de contrôle détruit le dossier du contrôle

- a dans les trois mois après que la personne contrôlée
 - 1. a refusé l'engagement ou le mandat;
 - 2. n'a pas été retenue pour le poste ou le mandat;
 - 3. a cessé d'exercer la fonction pour laquelle elle a été contrôlée;
- b mais au plus tard au bout de dix ans.

Art. 29 *Conséquences*

¹ Si la personne devant être contrôlée ne consent pas à subir ce contrôle (art. 26, al. 1) ou si le contrôle aboutit à des conclusions qui s'opposent à un rapport de travail, à une élection ou à l'attribution d'un mandat, il est possible

⁶⁾ RS [128](#)

- a de renoncer à la conclusion d'un contrat de travail, à l'élection ou à l'attribution d'un mandat;
- b de se départir d'une promesse d'engagement orale ou écrite;
- c de prendre des mesures relevant du droit du personnel, si les rapports de travail sont déjà établis.

Art. 30 *Renouvellement*

¹ Le contrôle de sécurité relatif aux personnes employées ou mandatées est renouvelé comme suit:

- a contrôle de base: au plus tôt après cinq ans, mais au plus tard après dix ans,
- b contrôle élargi: au plus tôt après trois ans, mais au plus tard après cinq ans.

² L'autorité de contrôle peut renouveler le contrôle plus tôt si elle a des raisons de supposer que de nouveaux risques sont apparus depuis le dernier contrôle.

³ Le contrôle de sécurité relatif aux personnes membres d'une autorité peut être renouvelé à l'occasion de leur réélection.

7 Organisation de la sécurité

Art. 31 *Organisation de la sécurité du canton et de l'administration cantonale*

¹ Le Conseil-exécutif définit par voie d'ordonnance l'organisation et les tâches

- a des organes compétents pour les questions de sécurité au plan cantonal,
- b des organes de sécurité de l'administration cantonale.

² Il peut déléguer ces tâches à des organes au sens de l'article 21, alinéa 2, lettre a de la loi du 7 mars 2022 sur l'administration numérique (LAN)⁷⁾.

³ Les communes municipales et les communes mixtes sont représentées de manière appropriée dans ces organes pour autant qu'elles soient concernées.

Art. 32 *Organisation de la sécurité des autres autorités*

¹ Les autorités n'appartenant pas à l'administration cantonale auxquelles s'applique la présente loi se dotent d'une organisation de la sécurité appropriée en fonction de leurs tâches et des risques qui en découlent pour la sécurité.

² Elles désignent une personne

- a qui est responsable de la sécurité de l'information et

⁷⁾ RSB [109.1](#)

- b* qui dispose des compétences et des ressources appropriées ainsi que d'une formation adéquate.

8 Dispositions d'exécution

Art. 33 *Conseil-exécutif*

¹ Le Conseil-exécutif édicte les dispositions d'exécution par voie d'ordonnance.

² Il peut

- a* déléguer à la Direction des finances, à un office ou à un organe spécialisé de l'administration cantonale l'édiction des prescriptions techniques ou organisationnelles, telles que des normes, des exigences en matière de sécurité et des processus à cet effet;
- b* habiliter la Direction des finances à édicter des ordonnances de Direction.

Art. 34 *Grand Conseil*

¹ Les dispositions d'exécution de la présente loi s'appliquent par analogie au Grand Conseil, à ses organes et aux Services parlementaires pour autant que le Grand Conseil ou son Bureau n'ait pas arrêté ses propres dispositions d'exécution.

² Le Bureau du Grand Conseil exerce, pour le Grand Conseil, les compétences que la présente loi confère aux autorités. Il peut les déléguer à d'autres organes du Grand Conseil ou aux Services parlementaires.

9 Dispositions transitoires et dispositions finales

9.1 Dispositions transitoires

Art. 35 *Classification des informations selon l'article 8*

¹ Le Conseil-exécutif définit par voie d'ordonnance les conditions dans lesquelles les informations créées avant l'entrée en vigueur de la présente loi sont classifiées.

Art. 36 *Premier contrôle de sécurité relatif aux personnes selon l'article 30*

¹ Le premier contrôle de sécurité relatif aux personnes déjà employées ou mandatées à l'entrée en vigueur de la présente loi est réalisé dans les délais prévus à l'article 30, alinéa 1.

² Le premier contrôle de sécurité relatif aux personnes membres d'autorité en fonction à l'entrée en vigueur de la présente loi est réalisé à l'occasion de leur réélection.

Art. 37 *Fixation de délais par le Conseil-exécutif*

¹ Le Conseil-exécutif définit les délais dans lesquels les mesures prévues par la présente loi et ses dispositions d'exécution doivent être appliquées pour la première fois.

9.2 Dispositions finales**Art. 38** *Modification d'un acte législatif*

¹ La loi du 10 février 2019 sur la police (LPol)⁸⁾ est modifiée.

Art. 39 *Entrée en vigueur*

¹ Le Conseil-exécutif fixe la date d'entrée en vigueur de la présente loi.

II.

L'acte législatif [551.1](#) intitulé Loi sur la police du 10.02.2019 (LPol) (état au 01.08.2024) est modifié comme suit:

Art. 17 al. 4 (abrog.)

⁴ Abrogé(e).

Art. 149 al. 4 (abrog.)

⁴ Abrogé(e).

Titre après Art. 159**10.2.3 (abrog.)****Art. 160**

Abrogé(e).

Art. 161

Abrogé(e).

Art. 162

Abrogé(e).

III.

Aucune abrogation d'autres actes.

⁸⁾ RSB [551.1](#)

IV.

Le Conseil-exécutif fixe la date d'entrée en vigueur de la présente loi.

Berne, le 12 juin 2025

Au nom du Grand Conseil,
la présidente: Siegenthaler
le secrétaire général: Trees

Référendum législatif facultatif

Le vote populaire (référendum) peut être demandé au sujet de la présente loi adoptée par le Grand Conseil le 12 juin 2025 (article 62, alinéa 1, lettre a de la Constitution cantonale).

Les citoyennes et citoyens peuvent proposer un projet populaire (article 63, alinéa 3 de la Constitution cantonale, articles 133 ss de la loi du 5 juin 2012 sur les droits politiques).

Les articles 123 à 132 de la loi du 5 juin 2012 sur les droits politiques sont applicables à la collecte et au dépôt des signatures (au moins 10'000 personnes ayant le droit de vote en matière cantonale).

Début du délai référendaire: 2 juillet 2025

Expiration du délai référendaire (dépôt des signatures pour attestation): 2 octobre 2025

Dépôt des signatures attestées à la Chancellerie d'État: 3 novembre 2025

Le texte de la loi est publié sur la [page Internet du Grand Conseil](#). Vous pouvez également vous le procurer à la Chancellerie d'État.