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 du canton de Berne (ConstC) du 6 juin 1993,

arrête:

I.

1 Dispositions générales

Art. 1 *But*

[1] La présente loi garantit 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 des autorités à décider et à agir;
b l'ordre et la sécurité publics;
c le respect des obligations légales et contractuelles des autorités en matière de protection des informations.

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 communes et aux autres organisations chargées de tâches publiques que les dispositions

a sur les informations classifiées, lorsqu'elles traitent des informations classifiées du canton ou de la Confédération, et
b sur 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 dispositions de la loi du 2 novembre 1993 sur l'information et l'aide aux médias (LIAM)[1)] régissant les demandes d'accès à des informations (art. 27 à 31a) ont la priorité sur la présente loi.

[2] La présente loi s'applique de manière complémentaire pour des informations dont la protection est en même temps réglée dans d'autres lois cantonales ou fédérales et 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)[2)].

Art. 4 *Définitions*

[1] Dans la présente loi, on entend par:

a informations: des indications portant sur des faits qui concernent les intérêts publics au sens de l'article 1, alinéa 2;
b sécurité de l'information: confidentialité, disponibilité, intégrité et traçabilité des informations;
c cybersécurité: sécurité de l'information lors de la transmission de données via des réseaux;
d outils TIC: biens et services des technologies de l'information et de la communication (TIC), incluant les logiciels et le matériel.

2 Principes

Art. 5 *Obligations des autorités en matière de sécurité de l'information et de cybersécurité*

[1] Chaque autorité veille à ce que

a les besoins de protection des informations relevant de son domaine de responsabilité soient évalués;
b les informations au sens de la lettre a, en fonction de leurs besoins de protection,
1. ne soient accessibles qu'aux personnes autorisées (confidentialité);
2. soient disponibles lorsque quelqu'un en a besoin (disponibilité);

---

1) RSB 107.1
2) RSB 152.04

3. ne puissent pas être modifiées sans autorisation ni par accident (intégrité);
4. soient identifiables quant à leur source et leur auteur (traçabilité);

c leurs outils TIC soient protégés contre toute utilisation abusive, défaut et dérangement.

[2] Elle assure la gestion des risques en

a évaluant continuellement les risques pour la sécurité de l'information;
b prenant les mesures nécessaires pour les éliminer ou les réduire à un niveau tolérable;
c 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 le non-respect des exigences et des mesures découlant de la présente loi soit sanctionné, et
c la mise en œuvre des exigences et des mesures découlant de la présente loi fasse l'objet d'un contrôle approprié.

Art. 7 *Réactivité et planification préventive*

[1] Les autorités veillent à détecter rapidement toute atteinte à la sécurité de l'information, à en éliminer les causes et à en réduire les répercussions au minimum.

[2] Elles veillent à

a la conception de plans d'action pour les cas d'atteinte grave à la sécurité de l'information risquant de menacer l'accomplissement de tâches cantonales très importantes pour la population;
b la mise en œuvre et l'actualisation régulière de ces plans d'action.

3 Mesures concernant l'organisation

Art. 8 *Classification*

[1] Les autorités classifient les informations dont la prise de connaissance par des personnes non autorisées porte préjudice aux intérêts publics selon l'article 1, alinéa 2, lettres a et b.

[2] La classification comporte les échelons suivants:

a "INTERNE", en présence de risque de préjudice aux intérêts publics,
b "CONFIDENTIEL", en présence de risque de préjudice important aux intérêts publics,
c "SECRET", en présence de risque de préjudice grave aux intérêts publics.

[3] La classification est l'exception. Elle est restreinte à l'échelon minimum nécessaire et si possible limitée dans le temps.

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

Art. 9 *Accès aux informations classifiées*

[1] Seules ont accès à des informations classifiées les personnes offrant la garantie qu'elles ne portent pas atteinte aux intérêts publics au sens de l'article 1, alinéa 2 et qu'elles ont besoin de ces informations pour accomplir une tâche légale ou contractuelle.

[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'organe parlementaire, le tribunal ou le Ministère public compétent en la matière procède à l'audition du service qui a classifié ladite information.

4 Mesures techniques

Art. 11 *Procédure de sécurité*

[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 (procédure de sécurité).

[2] 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 l'échelon 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 celle-ci,
d la compétence pour l'attestation de sécurité des outils TIC et pour l'acceptation des risques restants,
e la marche à suivre en cas de changement concernant les risques.

[3] L'échelon de sécurité des outils TIC est

a «protection très élevée» lorsque les intérêts mentionnés à l'article 1, alinéa 2 sont exposés à un préjudice grave;
b «protection élevée» lorsque les intérêts mentionnés à l'article 1, alinéa 2 sont exposés à un préjudice important;
c «protection de base» dans les autres cas.

[4] 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.

[5] Le Conseil-exécutif peut régler par ordonnance les mesures de protection à prendre pour les outils TIC, pour les informations et pour les données personnelles, en fonction

a de l'échelon de sécurité des outils TIC,
b de la classification des informations,
c du besoin de protection des données personnelles conformément à la législation sur la protection des données.

Art. 12 *Sécurité de l'exploitation*

[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. 13 *Principe*

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

Art. 14 *Zones de sécurité*

[1] Les autorités peuvent 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 du plus haut échelon de sécurité sont utilisés.

[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 contrôles des sacs et des personnes,
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 1ter de la loi fédérale du 30 avril 1997 sur les télécommunications (LTC)[1)].

6 Mesures concernant les personnes

6.1 Sélection, formation et habilitation

Art. 15 *Conditions d'accès aux informations et aux outils TIC*

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

a soient soigneusement sélectionnées,
b soient identifiées en fonction des risques,
c bénéficient d'une formation, initiale et continue, conforme à leur fonction,
d soient le cas échéant tenues de garder le secret et de faire preuve d'une vigilance particulière.

Art. 16 *Habilitation restrictive*

[1] Les autorités veillent à ce que les personnes au sens de l'article 15 ne disposent que des informations, outils TIC, locaux et autres infrastructures qui leur sont nécessaires pour accomplir leurs tâches légales ou contractuelles.

6.2 Contrôle de sécurité relatif aux personnes

Art. 17 *Conditions et but*

[1] Le contrôle de sécurité relatif aux personnes sert à évaluer si l'accès d'une personne à des informations 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.

[2] Sous réserve de leur consentement, les personnes pouvant faire l'objet d'un contrôle de sécurité sont les suivantes:

---

1) RS 784.10

a les personnes devant être engagées ou déjà employées par une autorité, avant la conclusion de leur contrat de travail et pendant leurs rapports de travail: par l'autorité d'engagement;
b les personnes devant être élues membre d'une autorité: par l'autorité d'élection ou l'autorité qui soumet la candidature,
c les personnes privées habilitées, dans le cadre des tâches ou des prestations qui leur sont confiées par mandat, à accéder directement aux données traitées par des autorités, à les traiter en toute autonomie ou à les consulter: par l'autorité ayant délivré le mandat.

[3] Elles peuvent être contrôlées lorsque les risques de sécurité liés à leur activité le justifient, notamment dans l'une ou l'autre des situations suivantes:

a elles ont accès à des informations classifiées ou à des données personnelles particulièrement dignes de protection, soit fréquemment, soit à un grand nombre ;
b elles disposent de vastes droits d'accès à d'importants dossiers politiques ou affaires de sécurité, sur lesquels elles peuvent exercer une influence;
c elles ont accès à des installations ou locaux sensibles ou à des zones de sécurité au sens de l'article 14 soit régulièrement, soit sans accompagnement.

[4] La personne faisant l'objet d'un contrôle a l'obligation de coopérer à son contrôle.

[5] Les dispositions de la législation fédérale sont réservées pour les personnes qui traitent des informations classifiées de la Confédération ou qui ont accès à des outils TIC de la Confédération.

Art. 18 *Objet*

[1] Le contrôle de sécurité relatif aux personnes consiste à recueillir les données touchant au mode de vie de la personne concernée, notamment à ses éventuelles activités pénalement répréhensibles et à sa situation financière, qui sont nécessaires à l'évaluation prévue à l'article 17, alinéa 1.

[2] Les données peuvent être recueillies

a dans le casier judiciaire;
b dans les registres des autorités des poursuites et faillites;
c dans les systèmes de traitement de données de la Police cantonale selon l'article 143 de la loi du 10 février 2019 sur la police (LPol)[1)];

[1)] RSB 551.1

d dans les systèmes de traitement de données de la Confédération ou des cantons, dans la mesure où la Police cantonale s'est vu conférer un accès direct conformément à l'article 147 LPol;
e en interrogeant la personne concernée;
f en interrogeant des tiers, si la personne concernée y consent.

Art. 19 *Protection juridique et conséquences*

[1] L'autorité contrôleuse communique les résultats du contrôle de sécurité relatif aux personnes à la personne concernée si le contrôle établit l'existence d'un risque au sens de l'article 17, alinéa 1.

[2] La personne qui a fait l'objet du contrôle peut consulter le dossier correspondant dans les dix jours et demander la rectification de données inexactes.

[3] Si la personne qui fait l'objet du contrôle ne consent pas à subir ce contrôle ou si le contrôle aboutit à des conclusions qui s'opposent à un rapport de travail ou à l'attribution d'un mandat, il est possible

a de renoncer à la conclusion d'un contrat de travail 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.

7 Organisation de la sécurité

Art. 20 *Organisation de la sécurité des autorités cantonales au sens de l'article 2, alinéa 1*

[1] Le Conseil-exécutif définit par 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 b de la loi du 7 mars 2022 sur l'administration numérique (LAN)[1)].

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

[1)] RSB 109.1

Art. 21 *Organisation de la sécurité des communes et des autres organisations chargées de tâches publiques au sens de l'article 2, alinéa 2*

[1] Les autorités qui n'appartiennent pas à l'administration cantonale 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 responsable de la sécurité informatique disposant des compétences et des ressources appropriées ainsi que d'une formation adéquate.

8 Dispositions d'exécution

Art. 22

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

[2] Il peut déléguer à la Direction des finances, à un office ou à un organe spécialisé de l'administration cantonale le soin d'édicter des dispositions d'exécution techniques ou organisationnelles comme des standards, des exigences en matière de sécurité et des processus. Il peut habiliter la Direction des finances à édicter des ordonnances de Direction.

[3] Il 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 Dispositions finales

Art. 23 *Modification d'autres actes*

[1] La loi du 10 février 2019 sur la police (LPol)[2)] est modifiée comme suit:.

Art. 24 *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 01.01.2023) est modifié comme suit:

[2)] RSB 551.1

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.

IV.

[Clause finale]

Berne, le

[Autorité]

[Fonction 1]
[NOM 1]

[Fonction 2]
[NOM 2]