

Propositions du Conseil-exécutif et de la commission
ACE n° 1099
Loi sur la sécurité de l'information et la cybersécurité_LSIC

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

Nouveau : ???.

Modifié(s) : 551.1

Abrogé(s) : –

Droit en vigueur	Proposition du Conseil-exécutif I	Proposition de la commission I		Proposition du Conseil-exécutif II
		Majorité	Minorité	
	Loi sur la sécurité de l'information et la cybersécurité (LSIC)			
	<i>Le Grand Conseil du canton de Berne,</i> vu l'article 18, alinéa 3 et l'article 37 de la Constitution cantonale ¹⁾ , sur proposition du Conseil-exécutif, <i>arrête:</i>			
	I.			
	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:			

¹⁾ RSB [101.1](#)

Droit en vigueur	Proposition du Conseil-exécutif I	Proposition de la commission I		Proposition du Conseil-exécutif II
		Majorité	Minorité	
	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.			
	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)¹⁾ priment la présente loi.			

¹⁾ RSB [107.1](#)

Droit en vigueur	Proposition du Conseil-exécutif I	Proposition de la commission I		Proposition du Conseil-exécutif II
		Majorité	Minorité	
	² La présente loi s'applique à titre supplétif a aux informations dont la protection est aussi réglée dans d'autres lois cantonales ou fédérales; 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)¹⁾.			

¹⁾ RSB [152.04](#)

	Art. 4 Définitions ¹ Dans la présente loi, il est entendu par a sécurité de l'information: confidentialité, disponibilité, intégrité et traçabilité des informations (art. 5, al. 1, lit. b); 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.	a sécurité de l'information: confidentialité, disponibilité, intégrité et traçabilité des informations (art. 5, al. 1, lit. b); 1. <u>confidentialité : les informations ne sont accessibles qu'aux personnes autorisées;</u> 2. <u>disponibilité: les informations sont disponibles lorsqu'elles sont nécessaires;</u> 3. <u>intégrité: les informations ne peuvent pas être modifiées sans autorisation ni par mégarde;</u> 4. <u>traçabilité: la source et l'auteur du traitement des informations sont identifiables;</u>		<i>Proposition de la majorité de la commission I</i>
--	---	---	--	---

	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 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); 3. ne puissent pas être modifiées sans droit ni par mégarde (intégrité); 4. soient identifiables quant à leur source et leur auteur (traçabilité); c leurs outils TIC soient protégés contre les utilisations abusives et les perturbations.	b les informations au sens de la lettre a, en fonction de leurs besoins de protection, 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; 1. ne soient accessibles qu'aux personnes autorisées (confidentialité); 2. soient disponibles lorsque quelqu'un en a besoin (disponibilité); 3. ne puissent pas être modifiées sans droit ni par mégarde (intégrité); 4. soient identifiables quant à leur source et leur auteur (traçabilité);		<i>Proposition de la majorité de la commission I</i>

	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 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. Ce faisant, il définit aussi les conditions dans lesquelles les informations créées avant l'entrée en vigueur de la présente loi sont classifiées.			
	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 celle-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 considérablement nuire 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)¹⁾.			
	6 Mesures concernant les personnes			
	6.1 Sélection, formation et habilitation			
	Art. 19			

¹⁾ RS [784.10](#)

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

	Art. 21 Personnes soumises à un contrôle de sécurité et autorités de contrôle ¹ Sous réserve de leur consentement, les personnes suivantes peuvent être soumises à un contrôle de sécurité: a par l'autorité d'engagement, les personnes devant être engagées, avant la conclusion des rapports de travail, ou les personnes déjà employées par une autorité, pendant leurs rapports de travail; b par l'autorité d'élection ou l'autorité qui soumet la candidature, les personnes devant être élues membre d'une autorité;	<u>Renvoi à la commission en la chargeant :</u> d'étudier et de proposer une réglementation qui définit les fonctions à contrôler et les autorités chargées des contrôles, ainsi que la périodicité des contrôles de sécurité des personnes. Elle doit en outre examiner la validité des dispositions en ce qui concerne les juges. <i>Proposition subsidiaire si la proposition de renvoi est rejetée :</i> b par l'autorité d'élection ou l'autorité qui soumet la candidature, les personnes devant être élues membre d'une autorité, <u>en particulier les juges;</u>		<i>Proposition de la majorité de la commission I</i>
--	--	---	--	---

	c par l'autorité qui leur confie le mandat, 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.			
	Art. 22 Conditions ¹ Une personne peut faire l'objet d'un contrôle de sécurité dès lors que les risques de sécurité liés à son activité le justifient, notamment 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» ou «secret», 2. des données personnelles particulièrement dignes de protection, dont la publication pourrait porter gravement atteinte aux droits de la personnalité des personnes concernées; b elle dispose d'un large accès à d'importantes affaires politiques ou sensibles, sur lesquelles elle peut exercer une influence; c elle a accès à des installations ou locaux sensibles ou à des zones de sécurité au sens de l'article 18 soit régulièrement, soit sans accompagnement.			
	Art. 23 Obligation de coopérer			

	¹ La personne soumise au contrôle est tenue de collaborer à l'établissement des faits.			
	Art. 24 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. 25 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 20. 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. 26 Résultat ¹ Si un contrôle de sécurité établit l'existence d'un risque au sens de l'article 20, l'autorité de contrôle en communique les résultats à la personne contrôlée. ² La personne contrôlée peut consulter le dossier correspondant dans les dix jours et demander la rectification de données inexactes.	¹ Si un contrôle établit l'existence d'un risque au sens de l'article 20, l'autorité de contrôle <u>L'autorité de l'article 20, l'autorité en contrôle</u> communique les résultats <u>du contrôle de sécurité</u> à la personne contrôlée. ² La personne <u>contrôlée</u> peut consulter le dossier correspondant dans les dix jours et demander la rectification de données <u>inexactes. Ce délai peut être prolongé dans des cas motivés.</u>		<i>Proposition de la majorité de la commission I</i> <i>Proposition de la majorité de la commission I</i>
	Art. 27 Conséquences ¹ Si la personne devant être contrôlée ne consent pas à subir ce contrôle (art. 21) 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			

	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.			
	7 Organisation de la sécurité			
	Art. 28 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)¹⁾. ³ Les communes municipales et les communes mixtes sont représentées de manière appropriée dans ces organes pour autant qu'elles soient concernées.			
	Art. 29 Organisation de la sécurité des autres autorités			

¹⁾ RSB [109.1](#)

	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 informatique et b qui dispose des compétences et des ressources appropriées ainsi que d'une formation adéquate.			
	8 Dispositions d'exécution			
	Art. 30 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. 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.			

	Art. 31 Grand Conseil ¹ Les dispositions d'exécution de l'article 30 s'appliquent au Grand Conseil, à ses organes et aux Services parlementaires sauf dispositions contraires édictées par le Grand Conseil. ² Le Bureau du Grand Conseil exerce, pour le Grand Conseil, les compétences que la présente loi confère aux autorités.	¹ Les dispositions d'exécution de la <u>présente loi</u> s'appliquent <u>par analogie</u> au Grand Conseil, à ses organes et aux Services parlementaires <u>à moins que le Grand Conseil ou son Bureau n'arrête ses propres dispositions d'exécution.</u> ² Le Bureau du Grand Conseil exerce, pour le Grand Conseil, les compétences que la présente loi confère aux autorités. <u>Il peut les déléguer à d'autres organes du Grand Conseil ou aux Services parlementaires.</u>		¹ Les dispositions d'exécution de la présente loi s'appliquent par analogie au Grand Conseil, à ses organes et aux Services parlementaires <u>dans la mesure où à moins que le Grand Conseil ou son Bureau n'arrête pas ses propres dispositions d'exécution.</u> <i>Proposition de la majorité de la commission I</i>
	9 Dispositions finales			
	Art. 32 Modification d'un acte législatif ¹ La loi du 10 février 2019 sur la police (LPol)¹⁾ est modifiée.			
	Art. 33 Entrée en vigueur			

¹⁾ RSB [551.1](#)

	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:			
Art. 17 ¹ La Police cantonale peut déléguer à des personnes privées ou à des organisations externes à l'administration des tâches qui lui sont attribuées par la présente loi, pour autant que l'exécution correcte de ces dernières soit assurée, notamment dans les domaines suivants: a les services de circulation et le contrôle des véhicules en stationnement, y compris la perception d'amendes et l'établissement de dénonciations, b l'exploitation et la maintenance d'installations techniques et de systèmes de traitement de données, c les activités et services manuels et techniques tels que services de remorquage, de serrurerie et prestations analogues, d les interventions de sauvetage dans des zones impliquant des difficultés particulières, e la prévention.				

² Les communes peuvent déléguer les tâches visées à l'alinéa 1, lettres a, b et e aux mêmes conditions. ³ La mise en œuvre de mesures de police et l'usage de la contrainte sont réservés dans tous les cas à la Police cantonale. ⁴ La Police cantonale peut soumettre des personnes privées et organisations extérieures à l'administration à un contrôle de sécurité relatif aux personnes si, dans le cadre des tâches qui leur sont confiées et des prestations à fournir, ces dernières ont accès à des installations et locaux de la police ou acquièrent des connaissances approfondies du travail policier. La procédure prévue par les articles 160 et suivants est applicable par analogie.	⁴ <i>Abrogé(e).</i>			
Art. 149 Sécurité des données ¹ La Police cantonale veille à la protection électronique des données qu'elle traite contre les manipulations, l'utilisation abusive et le vol, par la mise en œuvre de mesures organisationnelles et techniques appropriées et adaptées à l'état actuel de la technique. ² Elle garantit la sécurité physique de ses installations techniques et systèmes de traitement des données.				

³ Les autorités visées à l'article 2, alinéa 1, lettre b veillent à la sécurité des données traitées par elles conformément aux alinéas 1 et 2. ⁴ La Police cantonale peut soumettre à un contrôle de sécurité relatif aux personnes les personnes privées qui, dans le cadre des tâches ou prestations qui leur sont déléguées, sont autorisées à accéder directement ou à traiter ou consulter de manière autonome les données traitées par la Police cantonale. La procédure prévue aux articles 160 et suivants est applicable par analogie.	⁴ <i>Abrogé(e).</i>			
10.2.3 Contrôle de sécurité relatif aux personnes	10.2.3 <i>Abrogé(e).</i>			
Art. 160 Conditions ¹ La Police cantonale peut soumettre en tout temps ses collaborateurs et collaboratrices et les personnes avec lesquelles elle envisage d'instaurer des rapports de travail à un contrôle de sécurité relatif aux personnes pour s'assurer qu'ils ont une bonne réputation et sont dignes de confiance lorsque, dans le cadre de leurs activités, a ils ont accès à des données personnelles particulièrement dignes de protection, dont la révélation pourrait porter un grave préjudice aux droits individuels des personnes concernées ou	Art. 160 <i>Abrogé(e).</i>			

b qu'ils ont une connaissance approfondie d'importants dossiers de la politique de sécurité sur lesquels ils peuvent exercer une influence. ² La personne faisant l'objet du contrôle doit donner son consentement et apporter son concours à l'établissement des faits.				
Art. 161 Objet ¹ Le contrôle de sécurité relatif aux personnes consiste à recueillir des données pertinentes pour la sécurité touchant au mode de vie de la personne concernée, notamment à d'éventuelles activités pénalement répréhensibles et à sa situation financière. ² Les données peuvent être recueillies a dans les systèmes de traitement de données prévus à l'article 143, exploités par la Police cantonale; b 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; c dans les registres des autorités des poursuites et faillites des cantons et des bureaux du contrôle des habitants ou	Art. 161 <i>Abrogé(e).</i>			

d en interrogeant des tiers et la personne concernée, si cette dernière y consent.				
Art. 162 Protection juridique et conséquences ¹ La Police cantonale communique les résultats du contrôle de sécurité relatif aux personnes à la personne concernée. 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 des informations s'opposent à l'engagement d'une personne au sein de la Police cantonale, il est possible a de renoncer à la conclusion d'un contrat de travail; b de se départir d'une promesse d'engagement orale ou écrite ou c de prendre des mesures relevant du droit du personnel, si les rapports de travail sont déjà établis.	Art. 162 <i>Abrogé(e).</i>			
	III.			
	<i>Aucune abrogation d'autres actes.</i>			
	IV.			
	Le Conseil-exécutif fixe la date d'entrée en vigueur de la présente loi.			

	Berne, le 16 août 2023 Au nom du Conseil-exécutif, le président: Müller le chancelier: Auer	Berne, le 21 octobre 2024 Au nom de la commission, le président: Grupp	Berne, le 6 novembre 2024 Au nom du Conseil-exécutif, la présidente: Allemann le chancelier: Auer
--	---	--	---