CHANCELLERIE D'ETAT

ne.ch
REPUBLIQUE ET CANTON DE NEUCHÂTEL

DÉPARTEMENT DE LA SÉCURITÉ,
DE LA DIGITALISATION ET DE LA CULTURE
SERVICE INFORMATIQUE DE L'ENTITÉ NEUCHÂTELOISE

Directive sur la sécurité de l'information

Vote Électronique Neuchâtel

Auteur	**Direction du vote électronique**
Date	09.06.2026
Version	1.0
Classification	Aucune

Contrôle des modifications

Version	Date	Description	Nom
0.9	16.12.2025	Version pour les auditeurs	Direction du vote électronique
0.99	17.04.2026	Modifications formelles	Direction du vote électronique
1.0	09.06.2026	Modifications formelles	Direction du vote électronique

Autorités de contrôle/de validation

Contrôle	Validation	Date
Direction de la Chancellerie	Direction de la Chancellerie	05.06.2026

Documents de référence

N°	Document	Version
[1]	Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE) des 8 et 9 mai 2012	État au 01.10.2022
[2]	Politique générale de sécurité des systèmes d'information (PGSSI) de l'administration cantonale de Neuchâtel	Version du 04.11.2019
[3]	Politique de sécurité des systèmes d'information (PSSI)	Version du 11.11.2021
[4]	Directive sur la classification et le traitement de l'information (DIR-2016-02-SEC)	Version du 02.10.2025
[5]	Concept de vote électronique	Version actuelle
[6]	Directive sur la gestion des risques	Version actuelle
[7]	Concept de formation et d'information interne	Version actuelle
[8]	Normes et architectures pour les applications de cyberadministration en Suisse (eCH-0014 / SAGA.ch)	Version 8.0 du 13.09.2017
[9]	Loi sur le statut de la fonction publique (LSt, RS 152.510) du 28 juin 1995	État au 01.10.2022
[10]	Règlement général d'application de la loi sur le statut de la fonction publique (RSt, RS 152.511) du 9 mars 2005	État au 27.05.2025
[11]	Matériel et infrastructure	Version actuelle
[12]	Ordonnance de la ChF du 25 mai 2022 sur le vote électronique (OVotE, RS 161.116)	Version du 1er juillet 2022
[13]	Glossaire	Version actuelle
[14]	Plan d'urgence	Version actuelle
[15]	Gestion de la documentation	Version actuelle

Table des matières

1 Introduction

La présente directive a pour but de définir la gestion, les principes et les mesures liées à la sécurité de l'information pour l'exploitation du vote électronique. Elle s'adresse à toutes les unités administratives du canton de Neuchâtel impliquées dans les activités en rapport avec le vote électronique, ainsi qu'aux tiers concernés.

2 Objectifs et exigences

2.1 Objectifs

Les principaux objectifs de la gestion de la sécurité de l'information pour le vote électronique sont les suivants :

- Sécuriser le canal de vote électronique pour les électrices et électeurs du canton de Neuchâtel. Il convient notamment de garantir le secret du vote ainsi que la conformité du scrutin grâce à la vérifiabilité.

- Garantir la conformité de la mise en œuvre et de l'exploitation du vote électronique au regard du droit cantonal et des exigences réglementaires de la Confédération.

2.2 Exigences applicables à la sécurité de l'information

La gestion de la sécurité de l'information doit être conforme aux exigences légales et réglementaires liées à la sécurité de l'information, à la protection des données et à la continuité des activités en rapport avec le vote électronique :

- Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE) (voir *le document de référence [1]*)

- Politique générale de sécurité des systèmes d'information (PGSSI) de l'administration cantonale de Neuchâtel (voir *le document de référence [2]*)

- Politique de sécurité des systèmes d'information (PSSI) (voir *le document de référence [3]*)

- Directive sur la classification et le traitement de l'information (DIR-2016-02-SEC) (voir *le document de référence [4]*)

- Exigences réglementaires de la Confédération, Directive sur la gestion des risques (voir *le document de référence [5] ; section 2 - Bases légales*)

Conformément à la directive sur la classification et le traitement de l'information (voir *le document de référence [4]*), le système de vote électronique correspond aux niveaux de classification Confidentiel (niveau 3). Du fait de cette classification, le canton doit garantir un niveau de protection élevé pour les applications et les systèmes informatiques correspondants.

3 Gestion de la sécurité de l’information

3.1 Organisation et champ d’application

L’organisation de la gestion de la sécurité de l’information en rapport avec le vote électronique est identique à celle de l’exploitation du vote électronique définie dans le document « Concept de vote électronique » (voir *le document de référence [5]*). Ce cadre constitue également le champ d’application.

3.2 Rôles et responsabilités

Les rôles et les responsabilités sont définis dans le document « Concept de vote électronique » (voir *le document de référence [5]*). Les deux rôles concernés par le présent document sont la « direction du vote électronique » et la « direction de l'autorité supérieure VE ».

3.2.1 Responsabilités

Les responsabilités en matière de sécurité de l’information sont globalement définies comme suit :

- La direction de l'autorité supérieure VE s’assure que les exigences légales pour la mise en œuvre du vote électronique sont remplies et que la sécurité des informations est garantie de manière systématique et vérifiable. Il en résulte notamment les tâches suivantes :
    - Veiller à ce que la gestion de la sécurité de l’information soit mise en œuvre conformément à la présente directive.
    - Mettre à jour le présent document afin qu’il reflète les objectifs du canton en matière de sécurité de l’information lors du vote électronique.
    - S’assurer que les responsabilités en matière de sécurité de l’information sont établies à tout moment et qu’elles sont connues au sein de l'Etat et des prestataires.
    - Assurer le respect des directives du canton de Neuchâtel en matière de sécurité de l'information (voir *point 2.2*) et sensibiliser les intervenants aux questions de sécurité au sein des processus de vote électronique.
    - Garantir les ressources en personnel nécessaires au bon fonctionnement de la gestion de la sécurité de l’information, et soutenir les collaboratrices et collaborateurs concernés afin qu’ils puissent contribuer à une gestion efficace de la sécurité de l’information.
    - Garantir la fiabilité du personnel affecté au vote électronique.
    - Garantir la transmission des informations concernant l’importance d’une gestion efficace de la sécurité de l’information et du respect des exigences.
    - Promouvoir l’amélioration continue.

- La direction du vote électronique :
    - est responsable de la coordination opérationnelle de la gestion de la sécurité de l'information et des rapports concernant l'application de la directive ;
    - met en œuvre les formations et les programmes de sensibilisation à la sécurité de l'information auprès des personnes employées par le canton et les tiers concernés ;
    - maintient le contact avec les autorités chargées d'intervenir en cas de crise (voir *le document de référence [14]*).
- Les propriétaires des différents actifs informationnels sont responsables des mesures visant à protéger l'intégrité, la disponibilité et la confidentialité de ces derniers (voir *point 4.2*).

3.3 Gestion des risques

Le canton doit identifier, évaluer et, le cas échéant, atténuer les risques en lien avec la sécurité de l'information.

La gestion des risques est définie dans la « Directive sur la gestion des risques » (voir *le document de référence [6]*). Le canton applique un processus complet d'identification, d'appréciation et de traitement des risques issu de la méthodologie OCTAVE Allegro[1].

3.4 Formation, sensibilisation et communication

En collaboration avec les personnes concernées au sein de l'organisation, la direction de l'autorité supérieure VE doit s'assurer de la mise en œuvre des mesures de sensibilisation auprès de toutes les personnes du canton et des tiers impliqués dans le vote électronique.

Les mesures de sensibilisation sont mises en place afin que les personnes concernées puissent contribuer efficacement à la gestion de la sécurité de l'information à leur niveau et avoir connaissance des réglementations, directives et procédures en vigueur ainsi que des conséquences induites par le non-respect de ces règles.

Les mesures nécessaires à la formation et à la sensibilisation sont définies dans le document « Concept de formation et d'information interne » (voir *le document de référence [7]*). Les preuves de leur mise en œuvre sont conservées tel que précisé dans le concept.

[1] Voir https://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419

3.5 Évaluation et amélioration de l'efficacité

Si la direction du vote électronique constate que la directive n'est pas respectée ou que les mesures de sécurité sont insuffisantes, il convient de :

- documenter les écarts constatés,
- mettre en œuvre des mesures correctives immédiates afin d'en limiter les effets,
- procéder à une analyse permettant d'identifier les causes de la non-conformité ou des manquements,
- mettre en œuvre des mesures visant à remédier à ces causes,
- évaluer l'efficacité des mesures de correction.

La direction du vote électronique doit conserver la documentation relative à l'évaluation et à l'amélioration de l'efficacité conformément aux règlements organisationnels du canton.

4 Mesures relatives à la sécurité de l'information

Les chapitres suivants définissent les directives et les mesures spécifiques aux thèmes de la sécurité de l'information.

4.1 Personnel

La loi générale relative au personnel de l'administration cantonale (voir *le document de référence [9]*) a un caractère contraignant stipulé dans les contrats de travail. Cette loi définit les obligations des collaboratrices et collaborateurs cantonaux (Chapitre 2, Droits et devoirs). Il est stipulé qu'ils doivent accomplir leurs tâches avec engagement, fidélité, honnêteté et impartialité, dans le respect des instructions reçues (art. 15), qu'ils sont soumis à l'obligation de garder le secret (art. 20), et que les cadres sont responsables des actes accomplis conformément aux instructions qu'ils ont données (art. 16). L'exploitation du vote électronique ne fait l'objet d'aucune disposition particulière en matière de droit du personnel ; les bases juridiques et les règlements mentionnés s'appliquent. Les collaboratrices et collaborateurs externes doivent être tenus par contrat de respecter les directives en sécurité informatique et la présente directive.

La direction de l'autorité supérieure VE tient à jour une liste de règles de sécurité applicables au vote électronique. L'ensemble des collaboratrices et collaborateurs du canton impliqué dans le vote électronique est tenu de connaître et de respecter ces règles. Les principales règles sont rappelées par la direction de l'autorité supérieure VE à toutes les personnes concernées au moins une fois par an au début d'un scrutin (env. 7 semaines avant le vote).

La direction du vote électronique veille à ce que toutes les personnes du canton et les tiers impliqués dans le vote électronique soient formés conformément à leurs tâches (voir *point 3.4*).

4.2 Gestion des actifs informationnels

La direction du vote électronique tient un inventaire détaillé des actifs informationnels et des conteneurs ainsi que de leurs propriétaires.

Dans le cadre du vote électronique les actifs informationnels sont classés selon la liste ci-dessous. Entre parenthèse, la classification conformément à la directive sur la classification et le traitement de l'information (voir *le document de référence [4]*) est donnée :

- 1er niveau : public (dans la directive correspond à : public)
- 2e niveau : interne (dans la directive correspond à : interne)
- 3e niveau : confidentiel (dans la directive correspond à : confidentiel)
- 4e niveau : secret (dans la directive correspond à : confidentiel)

La direction du vote électronique doit s'assurer que les processus (initialisation, utilisation et destruction) prévus pour les appareils et les supports de données utilisés dans le cadre du vote électronique sont conformes aux processus définis dans le document « Matériel et infrastructure » (voir *le document de référence [11]*).

Toutes les données nécessaires à l'exploitation du vote électronique sont conservées exclusivement en Suisse. La transmission des données entre la Poste et le canton ou entre le canton et l'imprimerie passe par des plateformes techniques exploitées exclusivement en Suisse.

4.3 Cryptographie

Les règles applicables aux mesures cryptographiques pour le vote électronique (processus de génération, d'utilisation et de sécurisation des clés cryptographiques) sont définies par la Poste. L'entropie est assurée par le logiciel de la Poste pour le choix des valeurs aléatoires, notamment pour le composant de configuration et les composants de contrôle. Le canton définit la graine destinée aux valeurs publiques conformément aux directives de la Poste[2].

Les cartes de vote prêtes à imprimer sont transmises à l'imprimerie sous forme chiffrée et signée. Le canton utilise des algorithmes cryptographiques conformes à la norme eCH-0014 (voir *le document de référence [8]*).

Tous les certificats électroniques utilisés par le canton sont gérés selon les meilleures pratiques.

Le certificat permettant de signer les cartes de vote est établi par le canton.

Pour l'échange de certificats, la règle générale de vérifier l'authenticité des certificats au moyen d'une empreinte digitale s'applique. Pour ce faire, le certificat et l'empreinte digitale doivent être transmis par des voies séparées. Pour les certificats de composants fiables au sens du ch. 2 de l'ordonnance de la ChF sur le vote électronique (OVotE), un processus manuel doit être prévu conformément au ch. 3.8 de l'OVotE. Cette exigence est garantie par la remise physique de

[2] Cryptographic Primitives of the Swiss Post Voting System, Pseudo-code Specification, V1.4.1, point 8.2

l'empreinte digitale. Si une remise physique n'est pas possible, l'empreinte digitale doit être fournie par un canal électronique sécurisé (p. ex. Threema) et vérifiée lors d'une réunion en ligne. Les clés privées des certificats ne sont stockées que sur des ordinateurs hors ligne ou des supports de données chiffrés appartenant au canton. Le principe des 4-yeux est assuré lors de l'accès et de l'utilisation.

Tous les mots de passe nécessaires à l'exploitation du vote électronique doivent être générés de manière aléatoire et avoir une longueur suffisante. Les mots de passe des ordinateurs doivent comporter au moins 13 caractères. Pour le scrutin, des mots de passe de 50 caractères[3] sont générés tout en garantissant une entropie suffisante (au moyen du mouvement de la souris et de la saisie au clavier).

4.4 Sécurité physique

Le contrôle des accès et les mesures visant à protéger les locaux sont définis dans le document « Matériel et infrastructure » (voir *le document de référence [11]*).

La sécurisation physique et le stockage spécifique des appareils et des supports de données utilisés lors du vote électronique sont décrits dans le document « Matériel et infrastructure » (voir *le document de référence [11]*). En principe, tous les éléments physiques sont conservés dans le coffre-fort aussi bien pendant qu'en dehors d'un scrutin. Il est garanti que le coffre-fort ne peut pas être ouvert par une seule personne (principe des 4-yeux) et que tous les accès sont consignés.

La maintenance des ordinateurs est également décrite dans le document « Matériel et infrastructure » (voir *le document de référence [11]*).

4.5 Sécurité de l'exploitation

Les procédures documentées liées au vote électronique doivent être mises à la disposition des personnes compétentes.

Une suppléance doit être définie pour chaque rôle impliqué dans le vote électronique. La présence des personnes concernées pour la période en question est définie dans une liste du personnel avant le scrutin.

Une sauvegarde des appareils hors ligne est effectuée régulièrement pendant le scrutin, afin qu'il puisse avoir lieu même en cas de panne (voir *le document de référence [11]*). La procédure de sauvegarde est testée à chaque nouvelle version, mais au moins une fois par an.

Après chaque scrutin, toutes les informations stockées sur les appareils utilisés dans le cadre du vote électronique doivent être détruites à l'aide de moyens de suppression sécurisés. Cette étape de processus est décrite dans le document « Matériel et infrastructure » (voir *le document de référence [11]*).

[3] La longueur en bits des mots de passe doit correspondre au niveau de sécurité requis. Le niveau de sécurité utilisé pour le système de vote électronique est de 128 bits. Avec 7 bits par caractère, un mot de passe d'une longueur de 19 caractères serait donc déjà suffisant.

4.6 Séparation des tâches

En ce qui concerne la séparation des tâches selon l'annexe à l'ordonnance de la Chancellerie fédérale sur le vote électronique, le principe du double contrôle s'applique à toutes les opérations effectuées dans les domaines présentant des risques élevés, ainsi qu'à toutes les opérations manuelles en rapport avec l'urne électronique.

4.7 Contrôle des accès

L'accès et l'utilisation de composants fiables selon l'OVotE ou de supports de données contenant des données critiques sont consignés et font l'objet du principe des 4-yeux (voir *les points 4.4 et 4.6*). Les opérations manuelles en rapport avec l'urne électronique (p. ex. début du dépouillement) sont authentifiées explicitement.

4.8 Gestion des incidents affectant la sécurité de l'information

La direction du vote électronique répertorie et documente tous les incidents liés à la sécurité de l'information survenant pendant ou en dehors de la période du scrutin. Cette liste est également mise à la disposition de la commission électorale.

En sa qualité de fournisseur du système, la Poste surveille la situation dans le domaine de la sécurité de l'information en étroite collaboration avec l'Office fédéral de la cybersécurité (OFCS). Elle transmet les recommandations et les informations pertinents à la direction du vote électronique. Le SIEN surveille également la situation dans le domaine de la sécurité de l'information.

4.9 Gestion des fournisseurs

Le canton a conclu des contrats écrits avec tous les fournisseurs impliqués dans l'exploitation du vote électronique (notamment la Poste Suisse et l'imprimerie PERFECT. SA).

Les contrats permettent de s'assurer que les fournisseurs tiennent compte des bases légales et respectent les directives relatives à la sécurité de l'information. Les fournisseurs intègrent les risques identifiés lors de l'évaluation cantonale dans leur portefeuille de risques s'ils sont concernés par les risques en question. Ils sont par ailleurs responsables de la mise en œuvre d'éventuelles mesures. Le canton a la possibilité d'obtenir à tout moment des informations sur la mise en œuvre des exigences ou de contrôler la mise en œuvre sur site.

Les contrats sont contrôlés régulièrement (en particulier prise en compte des nouvelles connaissances issues de la vérification de l'évaluation des risques).

4.10 Gestion des changements

L'infrastructure informatique du canton, les droits d'accès, l'infrastructure de la Poste et l'infrastructure de PERFECT. SA ne peuvent être adaptés qu'en dehors des scrutins. Aucune modification n'est autorisée pendant un scrutin.

Une dérogation peut être accordée par la direction du vote électronique en cas d'urgence (p.ex. découverte d'une faille) selon le principe suivant : les avantages escomptés doivent toujours l'emporter sur les risques potentiels. L'exception est documentée et la commission électorale en est informée (voir également le *point 4.8*).

4.11 Sécurité de la communication

Les composants du réseau sont exploités et sécurisés par le Service informatique de l’Entité neuchâteloise conformément aux normes cantonales. L’ordinateur en ligne ne doit pas être visible sur le réseau du canton. Il ne peut se connecter qu’aux adresses IP dédiées définies par la direction du vote électronique. Les ordinateurs hors ligne ne doivent jamais être connectés au réseau ou à Internet.

5 Communication de la réglementation

La direction de l'autorité supérieure VE est chargée de veiller à ce que le personnel de du canton et les tiers concernés par le vote électronique soient informés des règles exposées dans la présente directive.

6 Validité et gestion des documents

Le présent document est valable à partir du 9 juin 2026.

Il est sous la responsabilité de la direction de l'autorité supérieure VE qui le vérifie au moins tous les trois ans et le met à jour si nécessaire.