CHANCELLERIE D'ÉTAT

ne.ch
REPUBLIQUE ET CANTON DE NEUCHÂTEL

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

Incident à Bâle-Ville : examen des processus et définition de mesures

Vote Électronique Neuchâtel

Auteur	**Direction du vote électronique (GR)** **Direction du vote électronique (NE)** **Direction du projet E-Voting (LU)** **Direction du vote électronique (SG)** **Spécialiste du vote électronique (TG)**
Date	09.06.2026
Version	1.0
Classification	Aucune

Contrôle des modifications

Version	Date	Description	Nom
0.9	27 mars 2026	Version initiale : projet de demande d'autorisation des cantons des Grisons, de Saint-Gall et de Thurgovie pour le scrutin du 14 juin 2026	Direction du vote électronique (GR) Direction du vote électronique (NE) Direction du projet E-Voting (LU) Direction du vote électronique (SG) Spécialiste du vote électronique (TG)
0.99	17.04.2026	Version mise à jour pour la demande provisoire d'octroi d'une autorisation générale pour NE	Direction du vote électronique (NE)
1.0	09.06.2026	Version mise à jour pour la demande définitive d'octroi de l'autorisation générale pour NE	Direction du vote électronique (NE)

Documents référencés

N°	Document	Version
[1]	Concept de vote électronique	Version actuelle
[2]	Glossaire	Version actuelle
[3]	Concept de vérifiabilité complète	Version actuelle
[4]	Directive sur la sécurité de l'information	Version actuelle
[5]	Matériel et infrastructure	Version actuelle
[6]	Concept Formations et information interne	Version actuelle

Table des matières

1 Introduction

Le 5 mars 2026, le canton de Bâle-Ville a signalé à l'organisation de crise du vote électronique qu'il n'avait peut-être plus accès au mot de passe administrateur nécessaire au déchiffrement de l'urne électronique pour le scrutin du 8 mars 2026. Les cantons, la Poste Suisse et la Chancellerie fédérale ont immédiatement activé leur dispositif commun de gestion de crise. Les efforts déployés pour accéder au mot de passe n'ont malheureusement pas abouti et le canton de Bâle-Ville a indiqué, dans un communiqué de presse du 7 mars 2026, que les 2048 votes exprimés par voie électronique dans le canton de Bâle-Ville n'avaient pas pu être décryptés et n'avaient donc pas pu être comptabilisés[1]..

Le 10 mars 2026, le canton de Bâle-Ville a annoncé qu'il ferait analyser par un externe les circonstances et les causes de l'incident. Parallèlement, il a pris acte du fait que le ministère public de Bâle-Ville a ouvert une procédure pénale. Le canton de Bâle-Ville a également précisé que l'incident survenu lors de la votation fédérale du 8 mars 2026 ne s'était produit que dans le canton de Bâle-Ville et qu'il était imputable à l'utilisation d'un composant externe (clé USB) et non au système de vote électronique mis à disposition par la Poste suisse.

Le 11 mars 2026, la Chancellerie fédérale a annoncé qu'elle prévoyait, à titre de mesure immédiate, que tous les cantons pratiquant le vote électronique réexaminent leurs processus de protection des clés de déchiffrement des urnes électroniques. Les mesures supplémentaires à prendre seront examinées dans le cadre des processus établis, en étroite collaboration avec tous les acteurs concernés.

Le 11 mars 2026 également, les cantons des Grisons, de Saint-Gall et de Thurgovie ont annoncé leur intention de maintenir le vote électronique. Les expériences sont positives. Le vote électronique se trouve toujours en phase d'expérimentation. Celle-ci vise délibérément à acquérir de l'expérience pratique et à améliorer et développer en permanence les procédures et les processus. Du point de vue des trois cantons, il est donc opportun de poursuivre cette phase d'expérimentation.

Dans le présent document, les cantons décrivent les processus mis en place jusqu'à présent en matière de déchiffrement de l'urne et exposent les vérifications effectuées à la suite de l'incident survenu à Bâle-Ville ainsi que les mesures prises.

Les cantons prennent très au sérieux l'incident survenu à Bâle-Ville en mars 2026. Il est important d'en tirer les leçons qui s'imposent. Les informations disponibles à ce jour concernant l'incident à Bâle-Ville ont été prises en compte. Les éventuelles conclusions supplémentaires issues de l'analyse externe commandée par Bâle-Ville seront prises en considération dès qu'elles seront disponibles.

2 Description du processus lié au déchiffrement

Pour un aperçu du processus de vote électronique, les cantons renvoient au document « Concept de vote électronique » (voir *le document référencé[1]*).

[1] Voir Communiqué de presse du 07.03.2026

2.1 Principe de base du chiffrement et du déchiffrement des votes électroniques

Lors de la préparation du scrutin, une paire de clés est générée le « jour 2 » (D2) à l'aide de deux mots de passe (mot de passe commission administrative[2] / mot de passe commission électorale[3]). Cette paire de clés[4] est combinée avec les clés des composants de contrôle. La clé publique combinée est utilisée par l'appareil de l'électeur pour crypter le vote.

Après la fermeture des urnes samedi avant le dimanche de votation à 12h00[5] , le déchiffrement des votes a lieu. Les votes ne peuvent être déchiffrés que si tous les composants de contrôle mixent les votes (et les déchiffrent partiellement) et si tant la commission administrative que la commission électorale saisissent leurs mots de passe respectifs afin de restaurer la clé privée. Le déchiffrement final a ensuite lieu à l'aide de la clé privée (récupérée à partir des deux mots de passe de la commission administrative et de la commission électorale). Cela garantit que les votes sont chiffrés de bout en bout et ne peuvent être déchiffrés que grâce à la collaboration de la commission administrative et de la commission électorale. Si l'un des deux mots de passe manque, aucun déchiffrement n'est possible.

---

2 Ce terme désigne les administrateurs cantonaux qui gèrent le processus de vote électronique selon le principe du 4-yeux (voir «Glossaire», *document de référence[2]*).

3 Ce terme désigne les personnes qui, en vertu du droit cantonal, sont chargées de veiller au bon déroulement du scrutin électronique et qui assument le rôle de vérificateurs prévu dans l'ordonnance de la Chancellerie Fédérale sur le vote électronique (voir «Glossaire» et «Concept de vérifiabilité complète», *documents référencés[2] et[3]*).

4 Pour plus d'informations sur la clé de sécurité, merci de se référer à la *section 4.2.2* de la spécification du système et à la note de bas de page numéro 6.

5 Le déchiffrement n'est possible « qu'après » 12 h 15. Le canton a défini un délai de 15 minutes. Ainsi, les électeurs qui se sont connectés peu avant 12 h 00 disposent de 15 minutes pour terminer leur vote électronique. Il n'est pas possible de se connecter après 12 h 00 (voir «Concept de vote électronique», *document référencé[1]*).

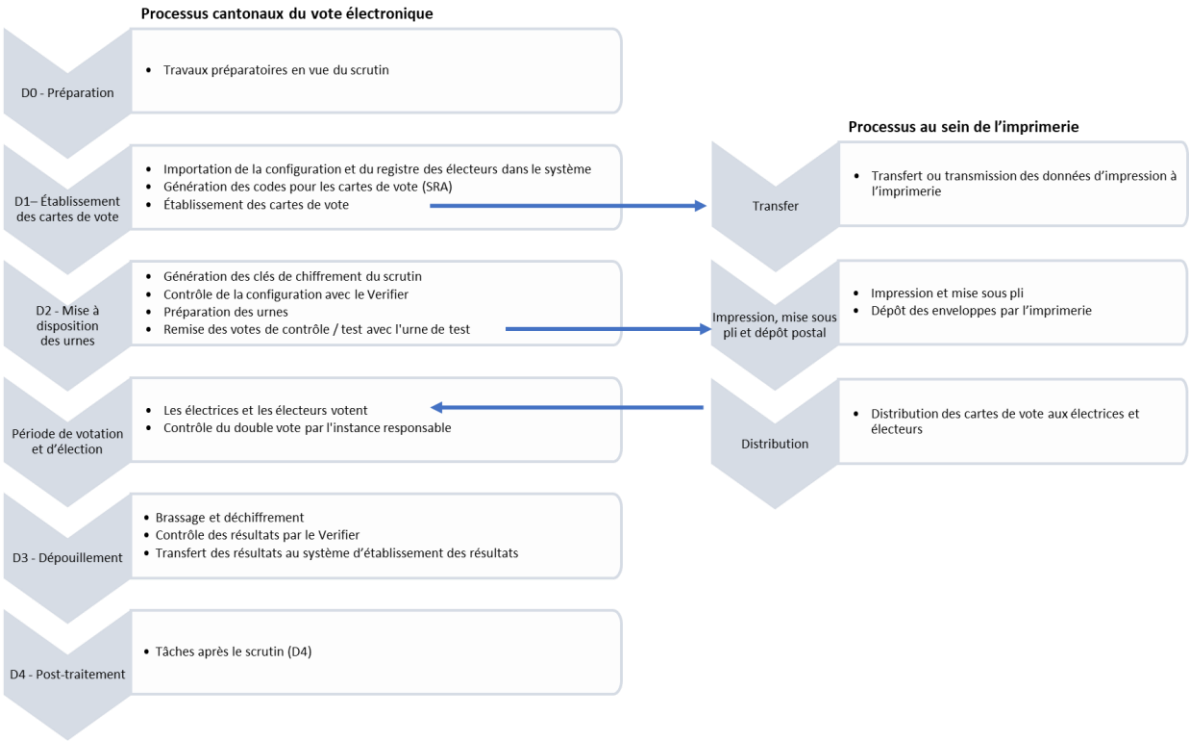

Illustration1 : schéma du processus de vote électronique tiré du « Concept de vote électronique » (voir *les documents référencés[1]*)

2.2 Processus de création et de conservation sécurisée des deux mots de passe

Les processus de création et de conservation des deux mots de passe ainsi que la manipulation des clés USB nécessaires à cet effet sont décrits ci-dessous :

- **Génération des deux mots de passe le jour 2 (D2) selon un processus clairement défini :** les deux mots de passe sont définis lors de la préparation du scrutin le jour 2, en présence de la commission électorale, selon un processus clairement défini : Les deux mots de passe sont générés de manière aléatoire avec une entropie suffisante sur un appareil hors ligne (ordinateur de configuration) à l'aide du logiciel KeePass et comptent chacun 50 caractères[6]. Le processus est exécuté par la commission administrative selon le principe du contrôle 4-yeux et est observé et surveillé par la commission électorale.

- **Stockage sur trois clés USB protégées par un code PIN chacune :** les deux mots de passe sont exclusivement stockés sur trois clés USB protégées par un code PIN chacune, qui ne sont utilisées qu'à cette fin. Il existe ainsi deux sauvegardes par mot de passe.

---

6 Voir à ce sujet la *section 4.3* de la «Directive sur la sécurité de l'information» (voir *le document référencé [4]*) ainsi que la *section 4.2.2* de la spécification du système. La longueur en bits des mots de passe doit correspondre au niveau de sécurité. Dans le système de vote électronique, le niveau de sécurité est de 128 bits. Avec 7 bits par caractère, un mot de passe de 19 caractères serait donc déjà suffisant. Les mots de passe sont générés selon le principe du 4-yeux, sous la supervision et l'observation de la Commission électorale. Une longueur de 50 caractères a été délibérément choisie afin de garantir que personne ne puisse mémoriser les deux mots de passe.

- **Clés utilisées et leur manipulation :** les clés USB protégées par un code PIN ne sont connectées à aucun autre appareil que les appareils de vote électronique hors ligne. Les clés USB utilisées par les cantons sont répertoriées dans le document « Matériel et infrastructure » (voir *le document référencé[5]*). Les clés USB sont cryptées au niveau matériel. L'accès aux données qui y sont stockées (= le mot de passe de la commission administrative ou de la commission électorale) n'est possible qu'après la saisie d'un code PIN. La saisie du code PIN permet de déverrouiller la clé. Les clés USB sont protégées contre les attaques par force brute. Dix saisies erronées du code PIN entraînent la destruction irréversible des données stockées sur la clé. Il est donc d'autant plus important de définir soigneusement le code PIN et de conserver les clés en lieu sûr.

    - Les **codes PIN des trois clés USB de la commission administrative** (généralement composés de 6 à 8 caractères) sont définis selon le principe du contrôle 4-yeux. Il faut donc s'assurer que les deux personnes connaissent le code PIN et peuvent ouvrir la clé à l'aide de ce code. Les membres de la commission administrative mémorisent le ou les codes PIN. Les codes PIN sont notés à titre de sauvegarde et conservés en lieu sûr sous la responsabilité de la commission administrative. L'ouverture de la clé est testée à plusieurs reprises, y compris l'ouverture à l'aide du code PIN noté.

    - **Les codes PIN des trois clés USB de la commission électorale** (généralement composés de 6 à 8 caractères) sont définis par les personnes concernées elles-mêmes. Les membres de la commission électorale mémorisent les codes PIN. Les codes PIN sont consignés par écrit à titre de sauvegarde et doivent être conservés en lieu sûr. L'ouverture de la clé par le membre concerné de la commission électorale est testée à plusieurs reprises, y compris l'ouverture à l'aide du code PIN noté.

- **Déchiffrement test lors de la préparation du scrutin (D2) :** le jour 2, une urne de test est déchiffrée afin de s'assurer que le processus peut être mené à bien. Pour ce faire, on suit exactement la même procédure que pour le déchiffrement des votes après la fermeture des urnes. Pour le déchiffrement, il faut saisir les mots de passe préalablement générés et enregistrés pour la commission administrative et la commission électorale. Afin de pouvoir saisir ces deux mots de passe, on ouvre respectivement une clé USB protégée par un code PIN de la commission administrative et de la commission électorale à l'aide du code PIN correspondant, puis on transfert le mot de passe sur l'ordinateur de déchiffrement.

- **Conservation des deux mots de passe et des trois clés USB protégées par un code PIN :** le mot de passe de la commission administrative et celui de la commission électorale sont conservés séparément. Cela garantit que personne n'a accès aux deux mots de passe et que les urnes ne peuvent être déchiffrées que lorsque la commission administrative et la commission électorale sont réunies pour le déchiffrement.

    - Les trois **clés USB de la commission administrative** sont conservées dans un coffre-fort. L'accès au coffre-fort n'est possible que selon le principe strict du contrôle 4-yeux. Cela signifie qu'aucune personne ne peut, de fait, y accéder sans la collaboration d'une autre.

    - La conservation des **clés USB de la commission électorale** varie d'un canton à l'autre : les clés sont conservées en lieu sûr et tous les cantons veillent à ce que la

commission administrative ne puisse pas accéder au mot de passe de la commission électorale et inversement.

2.3 Évaluation des risques

Conformément aux dispositions de l'ordonnance de la Chancellerie fédérale sur le vote électronique (OVotE), les cantons sont tenus de procéder à une évaluation systématique des risques et d'analyser les scénarios de menace définis dans l'OVotE. En conséquence, les cantons ont également analysé les risques liés à la disponibilité des deux mots de passe et défini des mesures qui ont servi de base au processus décrit à *la section 2.2* . L'analyse des risques a été réexaminée et complétée à la suite de l'incident survenu à Bâle-Ville.

3 Révision des processus

3.1 Procédure

Les cantons prennent très au sérieux l'incident survenu à Bâle-Ville. En collaboration avec la Poste Suisse, les cantons pratiquant le vote électronique, la Chancellerie Fédérale ainsi que l'Office fédéral de la cybersécurité (BACS), ont réexaminé les processus, et défini des mesures qui, pour certaines, ont déjà été mises en œuvre. L'analyse ne s'est pas limitée au processus de décryptage qui fait l'objet d'une attention particulière à Bâle-Ville. L'accent a été mis sur la robustesse des processus dans les cantons, mais aussi à la Poste Suisse ou dans les imprimeries, ainsi que sur les moyens d'accroître la résilience.

Au cours de deux ateliers consacrés à l'examen des processus et à la définition des mesures, les questions suivantes ont notamment été abordées :

- Existe-t-il des failles ou des angles morts quelque part ?
- Comment s'assurer que les processus définis sont efficaces, respectés et ne sont pas contournés (par négligence ou intentionnellement) ?
- Comment renforcer encore davantage le principe des 4-yeux ?

Les éventuelles conclusions supplémentaires issues de l'enquête externe commandée par Bâle-Ville seront prises en compte dès qu'elles seront disponibles.

3.2 Résumé des principales conclusions de l'examen des processus

Rien n'indique que de nouvelles expériences avec le vote électronique soient remises en cause. Les processus sont efficaces s'ils sont respectés. Le principe des yeux de 4 personnes est essentiel pour garantir leur respect. Les processus peuvent être améliorés ponctuellement et leur respect peut être encore mieux soutenu (voir *la section 4*). Aucun nouveau scénario de menace n'a été identifié.

4 Mesures

La mesure la plus importante et la plus efficace consiste à mieux soutenir le respect des processus. Les mots clés sont la sensibilisation / Awareness ainsi que l'amélioration des instructions et des listes de contrôle. Cela inclut notamment la sensibilisation à l'importance du principe 4-yeux et les mesures visant à le renforcer. Dans ce contexte, tous les cantons ont vérifié

l’accès au coffre-fort. Conformément aux exigences, l'accès au coffre-fort n'est autorisé que selon le principe strict du 4-yeux. Cela signifie qu'il faut s'assurer qu'aucune personne ne puisse accéder seule aux données critiques qui y sont conservées. Tout accès au coffre-fort par ces deux personnes doit en outre être consigné. L'analyse s'est concentrée sur les éventuelles clés de secours et mots de passe principaux utilisés pour la configuration des modules 4-yeux.

La section suivante documente les adaptations à court terme apportées au processus. *le chapitre 4.2* donne un aperçu des mesures élaborées par les cantons en collaboration et en concertation avec tous les acteurs.

Les cantons sont convaincus que l’analyse de l’incident survenu à Bâle-Ville, l’examen des processus qui s’en est suivi et les mesures définies ont permis de tirer de nombreux enseignements et que beaucoup a déjà été accompli. Ils sont convaincus que les leçons nécessaires ont été tirées de cet incident et qu’il n’y a aucune raison de remettre en cause la poursuite des essais de vote électronique.

Les cantons sont en échange permanent entre eux, avec la Poste Suisse et avec la Chancellerie fédérale, et veilleront au suivi des mesures dans le cadre des structures déjà en place.

4.1 Adaptations à court terme des processus

L'examen des processus a montré que ceux-ci sont fondamentalement bons. Cependant, les processus ne fonctionnent que s'ils sont respectés. Les modifications doivent être apportées avec soin et de manière ciblée afin qu'elles n'aient pas d'effets négatifs (c'est-à-dire une réduction de la sécurité due à une adaptation précipitée et non mûrement réfléchie). À court terme, les adaptations suivantes seront apportées au processus, en complément des mesures déjà en cours de mise en œuvre ou déjà mises en œuvre selon le chapitre 4.2 (notamment dans le domaine de la sensibilisation) :

- **Renouvellement (partiel) des clés USB :** les cantons des Grisons, de Saint-Gall et de Thurgovie n’ont jusqu’à présent rencontré aucun problème de fonctionnement avec les clés USB protégées par code PIN utilisées pour le stockage des deux mots de passe. Par mesure de précaution, il a néanmoins été décidé que chaque canton remplacerait chacune des trois clés USB par une nouvelle clé. Cette mesure ne concerne par les nouveaux cantons comme le Canton de Neuchâtel.

- **Sauvegarde supplémentaire du mot de passe de la commission administrative :** dans le canton de Bâle-Ville, l’accès au mot de passe de la commission administrative n’était plus possible. À titre de mesure à court terme, ce mot de passe est, dans tous les cantons, enregistré sur l’ordinateur de configuration (ainsi que sur les trois clés USB) à titre de mesure de sécurité supplémentaire et de support de stockage alternatif. L'ordinateur de configuration est un appareil hors ligne, avec un disque dur chiffré, utilisé lors de la configuration de l'urne et qui n'est plus utilisé lors du déchiffrement de l'urne. Tous les appareils sont conservés dans un coffre-fort sous la responsabilité de la commission administrative. L'accès au coffre-fort n'est possible que selon le principe strict du contrôle 4-yeux.

- **Adaptation du guide d'utilisation (instructions étape par étape, qui sert également de liste de contrôle) :** la création des différentes copies de sauvegarde est déjà documentée étape par étape dans le guide opérationnel. En collaboration avec la Poste Suisse, le guide a été optimisé de manière à rendre la création des trois sauvegardes ou clés USB plus robuste, garantissant ainsi, à la fin du jour 2 (D2), que les sauvegardes ont été correctement

créées, qu'elles fonctionnent et que l'ouverture des clés par la saisie du code PIN est assurée.

4.2 Aperçu des mesures

Une caractéristique essentielle du vote électronique est le processus d'amélioration continue, qui ne sera jamais terminé. De même, plusieurs des mesures ci-dessous (telles que la sensibilisation) ne sont jamais vraiment terminées et doivent plutôt être considérées comme une tâche récurrente. Par « terminés », on entend que les mesures sont menées à bien en vue de la demande provisoire.

N°	Mesure	Description	Date de mise en œuvre	Statut
0 A	**Vérification des processus et, si nécessaire, définition de mesures : cantons**	Même si l'incident survenu à Bâle-Ville n'avait aucun lien avec le système de la Poste Suisse ou avec les imprimeries, la question s'est néanmoins posée pour tous les acteurs de savoir dans quelle mesure les processus pouvaient être renforcés et comment la résilience pouvait être améliorée. L'accent a toutefois été mis sur les cantons. Pour la Poste Suisse et les imprimeries, une mesure complémentaire au contrôle consiste à sensibiliser à nouveau de manière ciblée toutes les parties prenantes au respect des processus et, en particulier, à l'importance du principe 4-yeux.	À court terme	Terminé
0 B	**Vérification des processus et, si nécessaire, définition de mesures : La Poste Suisse**		À court terme	Terminé
0 C	**Vérification des processus et, si nécessaire, définition de mesures : imprimeries**		À court terme	Terminé
1	**Vérifier l'analyse des risques**	Les cantons réexaminent leur analyse des risques en lien avec l'incident survenu à Bâle-Ville. L'examen continu des risques fait partie des processus établis et constitue donc une tâche permanente qui n'est jamais achevée.	À court terme	Terminé
2 A	**Vérifier le principe strict du contrôle 4-yeux et le renforcer si nécessaire (notamment l'accès au coffre-fort)**	Les cantons (et les imprimeries) réexaminent l'accès à leurs coffres-forts en tenant compte d'éventuelles clés de secours / mots de passe principaux. À moyen et long terme : les cantons vérifient la détectabilité (« tamper-evident ») si les mesures définies ne sont plus efficaces. De plus, le moment de la suppression des données critiques est réexaminé.	À court terme À moyen et long terme	Terminé En analyse
3 A	**Améliorer le respect des processus (en particulier le principe du contrôle 4-yeux): listes de contrôle / instructions**	Les cantons examinent comment améliorer la documentation / les instructions / les listes de contrôle afin de garantir le respect des processus et de s'assurer que rien n'est oublié (même en cas de pression temporelle).	À court terme	Terminé

		À court terme : le guide opérationnel sera amélioré. À moyen et long terme : les cantons et la Poste Suisse améliorent en permanence le soutien apporté au respect des processus (dans le cadre du processus d'amélioration continue qui a fait ses preuves).	À court terme À moyen et long terme	Terminé En cours (processus d'amélioration continue)
3 B	**Améliorer le respect des processus (en particulier le principe 4-yeux) : soutien / exigence au niveau de la mise en œuvre**	Les cantons examinent à nouveau, conjointement avec La Poste Suisse, si et comment le principe 4-yeux peut être encore mieux pris en charge / exigé au niveau de l'application. À moyen terme : pour la version 1.6 (publication à l'été 2026, mise en service à partir de 2027), une amélioration ciblée de l'interface utilisateur lors de la définition des deux mots de passe est à l'étude.	À moyen terme	En analyse (premières idées disponibles)
4	**Vérifier l'application du principe 3-2-1**	Les cantons examinent si et comment le principe 3-2-1 peut être renforcé. Le principe 3-2-1 est une règle de base éprouvée pour la protection contre la perte de données. Il stipule que les données importantes doivent être conservées en au moins trois copies, sur deux supports de stockage différents, dont une copie est conservée dans un lieu externe. L'objectif est non seulement de pallier les défaillances ponctuelles, mais aussi de réduire les risques systémiques. L'idée centrale qui sous-tend ce principe est la diversification des risques. Désormais, trois copies sont déjà créées pour chaque mot de passe, les clés USB contenant les mots de passe sont conservées en lieu sûr et il est garanti que les mots de passe ne sont réunis que lorsque la commission administrative et la commission électorale sont réunies lors du déchiffrement des urnes. Les cantons vont se pencher de manière plus approfondie sur ce principe. Comme cela doit se faire avec soin et de manière mûrement réfléchie, aucune adaptation n'est envisagée à court terme. À court terme, une amélioration est déjà mise en œuvre pour le mot de passe de la commission administrative. Il est enregistré en plus sur l'ordinateur de configuration de la commission administrative, à titre de deuxième support de stockage.	À court terme : enregistrement du mot de passe de la commission administrative sur l'ordinateur de configuration en tant que support de stockage supplémentaire À moyen et long terme	Terminé En analyse
5	**Sensibilisation / Awareness en général et surtout le jour**	Toutes les personnes concernées doivent connaître les principes et les mesures de sécurité les plus importants (en particu-	À court terme	Terminé

	2 (création et enregistrement des mots de passe pour le déchiffrement) : renouveler / renforcer	lier le principe 4-yeux) et comprendre pourquoi ils sont importants. La sensibilisation sera renouvelée de manière ciblée pour le prochain scrutin. À moyen et long terme : la sensibilisation et la prise de conscience constituent une tâche récurrente importante, déjà documentée en conséquence dans le « Concept de formation et d'information interne » (voir *le document référencé[6]).* Les cantons examinent si et comment la durabilité et l'efficacité des mesures peuvent être encore améliorées.	À moyen et long terme	En analyse
6	**Vérifier le cycle de vie (clés USB / autre matériel)**	Les cantons des Grisons, de Saint-Gall et de Thurgovie n'ont jusqu'à présent constaté aucun problème de fonctionnement avec le matériel (en particulier les clés USB). Une partie des clés USB doit néanmoins être renouvelée à court terme. À moyen et long terme, les cantons examinent la mise en place d'une politique commune concernant le cycle de vie du matériel informatique central.	À court terme (ne concerne par Neuchâtel qui a un matériel récent) À moyen et long terme	Terminé En analyse
8	**Vérification de la nécessité de l'utilisation de clés USB protégées par un code PIN**	Les cantons ont vérifié l'utilisation des clés USB protégées par code PIN. Conformément aux exigences de l'ordonnance sur le vote électronique (OVotE), les données critiques ne peuvent être stockées sur des supports de données que sous forme chiffrée. Techniquement, il existerait théoriquement d'autres solutions. Celles-ci présentent toutefois des inconvénients et le défi fondamental demeure (conservation sécurisée de la clé de déchiffrement, afin que seule la commission administrative et la commission électorale puissent procéder ensemble au déchiffrement). Il n'est donc pas possible de se passer des clés USB avec chiffrement matériel. À court terme, les cantons ne modifieront donc pas l'utilisation des clés USB. Les mesures 5, 3A (et 3B) constituent l'approche la plus pertinente. À moyen terme, il convient d'examiner attentivement si la solution actuelle peut être améliorée de manière ciblée.	À court terme À moyen et long terme	Examen terminé, aucune mesure En analyse
9	**Tenir compte des conclusions de l'analyse forensique informatique**	Les cantons examinent si l'analyse forensique informatique de la Poste Suisse et du canton de Bâle-Ville fait apparaître des besoins d'amélioration, par exemple en matière de renforcement de la sécurité et d'enquête sur les incidents. Une première	À moyen et long terme	En analyse

		évaluation n'a pas mis en évidence de besoins d'amélioration, mais cette analyse est toujours en cours.		
10	**Examen des clés USB à utiliser**	Les cantons utilisent différents types de clés USB : celles sur lesquelles la saisie du code PIN s'effectue directement sur la clé elle-même, et celles sur lesquelles la saisie du code PIN s'effectue après insertion dans l'ordinateur portable. Le choix des clés utilisées est consigné dans le document « Matériel et infrastructure » (voir *le document référencé[5]*). Outre la facilité d'utilisation des clés, il est important de garder à l'esprit les éventuelles failles de sécurité. À court terme, il a été vérifié que les clés USB utilisées ne présentaient aucune faille de sécurité connue. En conséquence, les modèles utilisés jusqu'à présent seront conservés à court terme. À moyen et long terme : l'utilisation des clés USB sera réexaminée dans le cadre de diverses autres mesures (par exemple n° 4) (y compris le suivi des éventuelles lacunes en matière de sécurité).	À court terme À moyen et long terme	Vérification terminée, aucune modification En analyse
11	**Révision et adaptation de la documentation**	Les cantons réexaminent leur documentation actuelle dans le but d'y intégrer les enseignements tirés de l'incident survenu à Bâle-Ville ainsi que les mesures prises. L'adaptation se fera en plusieurs étapes : à court terme (pour l'autorisation du scrutin du 14 juin 2026), l'accent est mis sur des adaptations ponctuelles. D'autres adaptations seront effectuées en tenant compte du calendrier des différentes procédures d'autorisation. L'objectif est de remplacer le présent document à moyen terme ou d'intégrer les contenus encore pertinents dans la documentation existante.	À court terme À moyen et long terme	Terminé En analyse
12	**Vérifier la formation / l'intégration des nouveaux collaborateurs et l'améliorer si nécessaire**	Les cantons réexaminent le concept de formation actuel (voir *le document référencé[6]*). L'objectif est d'élargir la base des formations et de mieux tirer parti des expériences et des synergies des différents acteurs. De premières idées ont déjà été formulées (comme par exemple prévoir des visites régulières dans d'autres cantons). Il a déjà été décidé que la Chancellerie Fédérale proposera à l'avenir des formations axées sur les exigences requises pour les nouveaux collaborateurs.	À moyen et long terme	En analyse

13	**Évaluer et améliorer la gestion de crise suite à l'incident survenu à Bâle-Ville**	Des processus bien établis existent pour la gestion de crise. Cela implique notamment que les cantons, en collaboration avec tous les autres acteurs, évaluent la gestion de crise liée à l'incident survenu à Bâle-Ville et l'améliorent si nécessaire.	À court et moyen terme	En analyse