



REPUBLIQUE ET CANTON DE GENEVE
Chancellerie d'Etat
Direction du Support et des Opérations de Vote

CHANCELLERIE D'ÉTAT



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

Plan d'urgence

Vote électronique

Auteur	Direction du vote électronique (GE) Direction du vote électronique (NE)
Date	09.06.2026
Version	1.0
Classification	Aucune

Contrôle des modifications

Version	Date	Description	Nom
0.9	10.06.2025	Version pour les auditeurs	Direction du vote électronique (GE)
0.91	16.12.2025	Modifications NE / Modifications formelles	Direction du vote électronique (GE) Direction du vote électronique (NE)
0.99	17.04.2026	Modifications au chapitre 3.2.7 / Modifications formelles	Direction du vote électronique (NE)
1.0	09.06.2026	Modifications formelles	Direction du vote électronique (GE) Direction du vote électronique (NE)

Autorités de contrôle/de validation

Contrôle	Validation	Date
Vice-chancelière (NE)	Vice-chancelière (NE)	05.06.2026

Documents de référence

N°	Document	Version
[1]	Concept de vérifiabilité complète	Version actuelle
[2]	Concept de vote électronique	Version actuelle
[3]	Ordonnance de la ChF du 25 mai 2022 sur le vote électronique (OVotE, RS 161.116)	Version du 01.07.2022
[4]	Glossaire	Version actuelle

Codes de couleur

Les contenus spécifiques à chaque canton sont indiqués par différentes couleurs de police (**rouge** = Genève ; **vert** = Neuchâtel).

Table des matières

1	But du document	4
2	Généralités	4
2.1	Champ d'application	4
2.2	Services concernés	4
3	Scénarios et flux d'informations.....	5
3.1	Scénarios de vérifiabilité universelle	5
3.1.1	Erreurs ou anomalies pendant la configuration.....	5
3.1.2	Erreurs ou anomalies pendant le dépouillement.....	6
3.2	Autres scénarios	6
3.2.1	Panne d'ordinateur	6
3.2.2	Faible de sécurité logicielle avant le scrutin	7
3.2.3	Faible de sécurité logicielle pendant le scrutin.....	8
3.2.4	Erreur dans le logiciel de vote électronique	9
3.2.5	Détection d'un incident dans le monitoring de la Poste	10
3.2.6	Détection dans le monitoring des cantons	11
3.2.7	Panne du système de vote électronique	12
4	Liste des tableaux.....	12

1 But du document

Le présent document décrit le plan d'urgence que les cantons sont tenus d'appliquer en cas d'incidents se produisant dans le cadre de l'exploitation du vote électronique. Des scénarios spécifiques sont élaborés en plus des règles de base. La liste des scénarios sera complétée en fonction des expériences acquises au fil du temps.

2 Généralités

2.1 Champ d'application

Le plan d'urgence cantonal s'applique lorsque des incidents susceptibles de perturber le déroulement d'un scrutin et la publication en bonne et due forme des résultats surviennent dans le cadre de l'exploitation du vote électronique. En sa qualité de fournisseur du système, la Poste dispose, tout comme la Chancellerie fédérale, de son propre plan d'urgence. Une convention définissant à quel moment la cellule de crise doit être informée ou activée est conclue entre la Chancellerie fédérale, les cantons et la Poste afin d'assurer la coordination en cas de crise.

2.2 Services concernés

Le tableau ci-après énumère les services qui jouent un rôle dans le plan d'urgence.

Service	Description
Direction du vote électronique	Lors d'un incident, la direction du vote électronique décide si le plan d'urgence doit être appliqué. Elle est tenue d'informer les services suivants : - Direction de l'autorité supérieure VE - Commission électorale incluant les vérificatrices et vérificateurs - Communes
Direction du support et des opérations de vote / Chargé des droits politiques	Est informée des situations d'urgence et des anomalies par la direction du vote électronique.
Direction de l'autorité supérieure VE	La Direction de l'autorité supérieure VE est la plus haute instance décisionnelle du canton. Elle prend les décisions pour le canton en temps de crise.
Commission électorale / vérificatrices et vérificateurs	Ils sont informés de chaque situation d'urgence en raison de leurs tâches et de leurs responsabilités (voir <i>document de référence [1]</i>).
Communes	Elles sont informées en fonction de la situation et de leurs tâches (voir <i>document de référence [1]</i>).
Cellule de crise	La cellule de crise est définie dans la convention de crise. Elle est informée et activée conformément aux dispositions et aux scénarios de la convention de crise.
Fournisseur du système	En sa qualité de fournisseur du système, la Poste accompagne les cantons sur les questions techniques. Elle possède sa propre équipe de piquet et sa propre organisation de crise.

Tableau 1 : Services concernés par le plan d'urgence

3 Scénarios et flux d'informations

Les scénarios décrivent les mesures et les flux d'informations à appliquer en cas d'urgence dans le cadre de l'exploitation cantonale du vote électronique.

La direction du vote électronique informe immédiatement la Poste en cas d'urgence. La commission électorale ainsi que les vérificatrices et vérificateurs sont également informés de toutes les situations d'urgence. La Direction de l'autorité supérieure VE est informée si nécessaire, et dans tous les cas lorsqu'une situation d'urgence est susceptible de conduire à une situation de crise. Les flux d'informations au sein du canton et à destination de la Poste ne sont pas présentés séparément dans les tableaux ci-après.

Si l'incident déclenche une crise selon les scénarios de la convention de crise, les processus de la convention de crise s'appliquent.

La Direction de l'autorité supérieure VE, la commission électorale ou les vérificatrices et vérificateurs peuvent faire appel à des expertes et des experts indépendants de la Poste pour analyser les événements et confirmer l'analyse de la Poste (voir *document de référence [1]*). Ce point n'est pas présenté séparément dans les tableaux ci-après.

3.1 Scénarios de vérifiabilité universelle

Ces scénarios s'appliquent lorsque le Verifier détecte des erreurs ou des anomalies. La gestion des erreurs et des anomalies est décrite dans le concept de vérifiabilité complète (voir *document de référence [1]*).

3.1.1 Erreurs ou anomalies pendant la configuration

Description	Le Verifier détecte des erreurs ou des anomalies pendant l'exécution du processus D2.
Mesures à prendre lors de l'incident	Une analyse est immédiatement lancée par le canton et la Poste afin de déterminer la cause de l'incident. - Une fois la cause trouvée, le problème est corrigé et les processus D1 et D2 sont répétés. - Des mesures spéciales sont définies pour les étapes suivantes du scrutin ainsi que pour les futurs scrutins (si nécessaire). - Un rapport contenant la description du problème, l'analyse des causes, leurs justifications et les éventuelles mesures à prendre est rédigé. - Le rapport est mis à la disposition des vérificatrices et vérificateurs.
Flux d'informations	Autres cantons : immédiatement, et après la résolution du problème. Chancellerie fédérale : au moment de l'incident et à la remise du rapport. Communes : selon les besoins. Public : selon les besoins.
La cellule de crise doit-elle être activée ?	Oui, si les processus D1 et D2 ne peuvent pas être répétés.

3.1.2 Erreurs ou anomalies pendant le dépouillement

Description	Le Verifier détecte des erreurs ou des anomalies pendant le dépouillement (processus D3).
Mesures à prendre lors de l'incident	Une analyse est immédiatement lancée par le canton et la Poste afin de déterminer la cause de l'incident. Les questions suivantes doivent être traitées (pour plus de détails, voir le <i>document de référence [1]</i>) : - Quels sont les points de contrôle concernés (exhaustivité, authenticité, cohérence, intégrité, preuves, écart dans la configuration) ? - Quel est l'objectif de sécurité (exactitude ou secret du vote) ? - Les étapes peuvent-elles être corrigées ou répétées ? - Les étapes peuvent-elles être répétées avec succès après la correction ? - Le nombre de votes concernés a-t-il une influence sur le résultat ? Les étapes possibles sont répétées en fonction des résultats. Un rapport exposant le problème, l'analyse des causes, la justification et les éventuelles mesures à prendre est rédigé. Les processus sont adaptés, et il est procédé à une analyse des risques sur la base du rapport.
Flux d'informations	Autres cantons : immédiatement, et après la résolution du problème. Chancellerie fédérale : au moment de l'incident et à la remise du rapport. Cellule de crise : au moment de l'incident et à la remise du rapport. Communes : lorsque les résultats ne peuvent pas être fournis dans les délais impartis. Public : lorsque le rapport est publié.
La cellule de crise doit-elle être activée ?	Oui, si les résultats ne peuvent pas être publiés en temps voulu.

3.2 Autres scénarios

3.2.1 Panne d'ordinateur

Description	Un ordinateur ne fonctionne plus pendant l'exécution d'une étape du processus (défaut matériel).
Mesures à prendre lors de l'incident	L'appareil de remplacement est installé. La sauvegarde est téléchargée sur l'appareil de remplacement. L'incident est documenté dans le journal des incidents du scrutin.
Flux d'informations	Aucun.
La cellule de crise doit-elle être activée ?	Non, tant que le scrutin peut se poursuivre.

3.2.2 Faille de sécurité logicielle avant le scrutin

Description	Une faille de sécurité affectant un logiciel utilisé par les cantons (p. ex. OpenSSL, logiciel de vote électronique) est détectée peu avant le scrutin.
Mesures à prendre lors de l'incident	L'impact de cette faille est analysé par le canton et la Poste. A la suite de cette analyse, les mesures suivantes sont prises en fonction de la situation : - Aucune action, car les conséquences sont acceptables. - Le logiciel est mis à jour. L'installation est effectuée selon le principe du double contrôle. - Des mesures spéciales sont prises pour réduire les éventuelles conséquences (p. ex. mesures de surveillance ciblées). L'incident et les mesures prises sont documentés dans le journal des incidents du scrutin.
Flux d'informations	Autres cantons : les mesures sont coordonnées avec les autres cantons. Chancellerie fédérale : les mesures sont évaluées avec le canton. Public : est informé si la faille de sécurité ne peut pas être corrigée.
La cellule de crise doit-elle être activée ?	Non, tant que le scrutin peut être réalisé (information et activation selon la convention de crise).

3.2.3 Faille de sécurité logicielle pendant le scrutin

Description	Une faille de sécurité affectant un logiciel utilisé par les cantons (p. ex. logiciel de vote électronique, VMGJ) est détectée pendant le scrutin.
Mesures à prendre lors de l'incident	L'impact de cette faille est analysé par le canton et la Poste. A la suite de cette analyse, les mesures suivantes sont prises en fonction de la situation : - Aucune action, car les conséquences sont acceptables. - Le logiciel est mis à jour. L'installation est effectuée selon le principe du double contrôle. - Des mesures spéciales sont prises pour réduire les éventuelles conséquences (p. ex. mesures de surveillance ciblées). L'incident et les mesures prises sont documentés dans le journal des incidents du scrutin.
Flux d'informations	Autres cantons : les mesures sont coordonnées avec les autres cantons. Chancellerie fédérale : les mesures sont évaluées avec le canton. Public : est informé si la faille de sécurité ne peut pas être corrigée.
La cellule de crise doit-elle être activée ?	Oui, si les conséquences de la faille de sécurité sont graves ou très graves (information et activation selon la convention de crise).

3.2.4 Erreur dans le logiciel de vote électronique

Description	Une erreur survient pendant l'exécution du scrutin conformément au guide d'utilisation de la Poste (p. ex. message d'erreur dans le Secure Data Manager, un script ne fonctionne pas, etc.).
Mesures à prendre lors de l'incident	L'erreur est corrigée conformément au guide d'utilisation de la Poste. Si l'erreur ne peut pas être corrigée, le service d'assistance de la Poste est sollicité. L'erreur et les mesures prises sont documentées dans le journal des incidents du scrutin ou dans les procès-verbaux des processus D1, D2 et D3. Chaque erreur est analysée par les cantons et la Poste, même si elle a pu être corrigée, et des mesures sont définies si nécessaire par la Poste et/ou les cantons.
Flux d'informations	Autres cantons : immédiat, coordination d'éventuelles mesures si besoin. Chancellerie fédérale : les mesures sont évaluées avec le canton.
La cellule de crise doit-elle être activée ?	Oui, si les conséquences de la faille sont graves ou très graves (information et activation selon la convention de crise).

3.2.5 Détection d'un incident dans le monitoring de la Poste

Description	L'infrastructure du fournisseur du système est surveillée par un système de monitoring (voir <i>document de référence [3]</i>, point 14.1 de l'ordonnance de la ChF sur le vote électronique, OVotE), et des journaux système sont établis en continu (cf. point 14.2 OVotE). Les incidents détectés sont signalés à la direction du vote électronique, et les journaux système pertinents sont mis à disposition.
Mesures à prendre lors de l'incident	L'incident est analysé par la Poste en concertation et en échange avec la direction du vote électronique. A la suite de cette analyse, les mesures suivantes sont prises en fonction de la situation : - L'analyse est clôturée et le résultat est documenté. - L'analyse est poursuivie et une analyse forensique est lancée si nécessaire. - Les résultats de l'analyse et les expériences sont intégrés dans le processus d'amélioration continue (cf. point 14.3 OVotE). - Des mesures spéciales sont prises pendant le scrutin afin de résoudre l'incident. L'incident et les mesures prises sont documentés dans le journal des incidents du scrutin.
Flux d'informations	Autres cantons : l'analyse et les mesures sont coordonnées avec les autres cantons. Chancellerie fédérale : l'analyse et les mesures sont coordonnées avec la Chancellerie fédérale. Public : est informé selon les besoins. Communes : selon les besoins (si cela concerne les processus des communes). Autres acteurs (p. ex. police) : selon les besoins.
La cellule de crise doit-elle être activée ?	Oui, si les conséquences sont graves ou très graves (information et activation selon la convention de crise).

3.2.6 Détection dans le monitoring des cantons

Description	Les cantons documentent dans un journal tous les incidents survenus au cours du scrutin. Le canton prend des mesures en cas d'anomalies (p. ex. plusieurs appels d'électrices ou d'électeurs signalant des codes de vérification incorrects).
Mesures à prendre lors de l'incident	L'anomalie est analysée avec la Poste et les autres cantons. A la suite de cette analyse, les mesures suivantes sont prises en fonction de la situation : - L'analyse est clôturée et le résultat est documenté. - L'analyse est poursuivie et une analyse forensique est lancée si nécessaire. - Les résultats de l'analyse et les expériences sont intégrés dans le processus d'amélioration continue (cf. point 14.3 OVotE). - Des mesures spéciales sont prises pendant le scrutin afin de résoudre l'incident. L'incident et les mesures prises sont documentés dans le journal des incidents du scrutin.
Flux d'informations	Autres cantons : l'analyse et les mesures sont coordonnées avec les autres cantons. Chancellerie fédérale : l'analyse et les mesures sont coordonnées avec la Chancellerie fédérale. Public : est informé selon les besoins. Communes : selon les besoins (si cela concerne les processus des communes). Autres acteurs (p. ex. police) : selon les besoins.
La cellule de crise doit-elle être activée ?	Oui, si les conséquences sont graves ou très graves (information et activation selon la convention de crise).

3.2.7 Panne du système de vote électronique

Description	Une panne système se produit pendant la phase de vote. Le système de vote électronique n'est pas disponible.
Mesures à prendre lors de l'incident	Une analyse est immédiatement lancée par le canton et la Poste afin de trouver la cause du problème et de procéder à sa résolution. Si la disponibilité ne peut être rétablie dans un délai raisonnable, le canton de Neuchâtel, en collaboration avec les communes, veille à ce que le matériel de vote pour les canaux de vote conventionnels soit activement envoyé aux électrices et électeurs concernés par la panne.
Flux d'informations	Autres cantons : les mesures sont coordonnées avec les autres cantons. Chancellerie fédérale : les mesures sont évaluées avec le canton. Communes : information continue. Si la disponibilité ne peut pas être rétablie dans un délai raisonnable, les électrices et électeurs concernés inscrits pour le vote électronique sont informés par le canton par courrier électronique de la panne et de l'envoi actif du matériel de vote pour les canaux de vote conventionnels. Si le temps nécessaire à cet envoi n'est pas suffisant, les électrices et électeurs sont informés de la seule option restante (vote aux urnes avec une carte de vote électronique). Public : les cantons documentent les perturbations sur le portail d'information. Le public est informé activement si la disponibilité du système ne peut pas être rétablie dans un délai raisonnable. Selon les composants systèmes concernés, la Poste diffuse une information concernant la panne directement sur la page d'accueil ou sur le portail de vote.
La cellule de crise doit-elle être activée ?	Oui, si les conséquences de la panne sont graves ou très graves (p. ex. si le bon déroulement du scrutin est menacé ; information et activation selon la convention de crise).

4 Liste des tableaux

Tableau 1 : Services concernés par le plan d'urgence 4