canton de vaud
LIBERTÉ ET PATRIE

POLICE CANTONALE

SERVICES GENERAUX

Lausanne, le 30.11.2023

Genre de document	**NOTE**		No : 1126
Emanant de	**DIRECTEUR SUPPORT**		
Sujet / Code	**UTILISATION DES OUTILS DE COMMUNICATION ELECTRONIQUE**		
Annule	---		
En vigueur dès le	15.12.2023	Echéance	INDETERMINEE
Destinataires	- secrétariat cdt PCV et EM - secrétariat EM gendarmerie - secrétariat police de sûreté - TARS (par émetteur)		

Va à : - officiers pour information au personnel

Pour information :
- commandante de la Police cantonale
- remplaçant de la commandante de la Police cantonale et chef EM
- commandant de la gendarmerie et son remplaçant
- chef de la police de sûreté et son remplaçant
- chef opérationnel de la gendarmerie
- chef opérationnel de la police de sûreté
- SOPV

Annexes : - guide démarrage Threema Work

1. ORIENTATION

L'essor des moyens électroniques de communication impose de mettre en place un cadre quant à leur utilisation, qui permette une cohabitation intelligente de ces différents moyens. Le durcissement des règles de Protection des données, les récentes affaires de hacking ou de fuite de données sensibles ainsi que l'introduction de l'application Threema Work rendent indispensable que les règles et procédures soient améliorées, précisées ou rappelées.

La Direction générale du numérique et des systèmes d'information (DGNSI) est responsable d'assurer que le réseau informatique réponde aux plus hautes exigences sécuritaire pour éviter toute intrusion, corruption ou vol de données. De son côté, les collaborateurs de la PCV (y compris les polices communales qui utilisent le réseau cantonal) ont la responsabilité d'utiliser les outils informatiques de manière à empêcher toute fuite de données sensibles ou personnelles.

2. INTENTION

Je veux :
- définir le périmètre des différents outils de communication existants
- préciser le cadre de leur utilisation en fonction de la sensibilité des données
- mettre en place des règles de modération et de contrôle
- préciser le déploiement de l'application Threema Work à la PCV

3. BASES

- Loi du 11.09.2007 sur la protection des données personnelles (PLrD)
- Loi sur les dossiers de police judiciaire du 01.12.1980 (LDPJu)
- Règlement relatif à l'informatique cantonale du 21.01.2009 (RIC)
- NPJ 25 sur la durée de conservation des données et des dossiers de police judiciaire
- OS 1000 sur la publication et la classification des documents
- Directive de la DGNSI « usage acceptable des outils informatiques étatiques »
- Bonnes pratiques Webex émises par la DGNSI

4. NIVEAUX DE CLASSIFICATION

Dans ce contexte, la PCV est responsable que les traitements des données auxquels elle procède (collecte, conservation, communication, etc.) respectent la LPrD. C'est elle qui définit ses besoins spécifiques en matière de sécurité des données.
L'ordre de service susmentionné précise 4 niveaux de classification des informations :

Public : information en libre accès, qui peuvent être rendues publiques.

Interne : information limitée à un usage exclusif du service. Il ne peut être diffusé au-delà qu'avec l'autorisation de l'émetteur, après analyse des enjeux et conséquences étant précisé au destinataire externe qu'aucune rediffusion du document ne doit être faite.

Confidentiel : contenant des données personnelles. Ce genre de document ne doit être accessible qu'aux personnes autorisées qui peuvent être définies nominativement par leur fonction ou leur appartenance à un groupe. Il ne peut être diffusé au-delà qu'avec l'autorisation de l'émetteur, après analyse des enjeux et conséquences.

Secret : information avec un haut niveau de confidentialité, accessible uniquement à des personnes déjà identifiées et autorisées.

5. UTILISATION DES OUTILS DE COMMUNICATION

Le tableau ci-dessous, illustre en fonction du besoin de communication, quels outils sont les plus appropriés en fonction du niveau de classification de l'information, respectivement de la donnée transmise.

	Smartphone Tél fixe	App commerciales (WhatsApp, FaceTime,Zoom)	Cisco Webex / Jabber	Outlook	[Secemail]	Cryptage PKI	Threema Work
Appel vocal	P, I, C, S	P	P, I, C				P, I, C, S
Appel vidéo	P, I	P	P, I, C 1				P, I, C, S
Messagerie instantanée + SMS (y compris fichiers attachés)	P, I, C 4	P	P, I, C 1				P, I, C, S
Email				P, I, C 1,2	P, I, C	P, I, C, S	
Vidéoconférence (y compris partage ou envoi de fichiers)		P	P, I, C 3				P, I, C, S 5

Remarques

[1] Les fichiers (docs, images, etc.) concernant des affaires ou des personnes suivent les règles de conservation/diffusion principalement de la LDPJu (NPJ n° 25 sur la durée de conservation des données et des dossiers de police judiciaire).
C'est à l'utilisateur ou modérateur de groupe, de veiller à les respecter et les effacer de sa boîte, respectivement du groupe. **Pour les groupes Webex contenant de la donnée classée confidentielle, le délai pour effacer les données personnelles sensibles et les fichiers est fixé à 30 jours maximum.**

[2] L'envoi sur des adresse externes ACV doit être fait avec les précautions qui s'imposent, en s'assurant que leur éventuelle diffusion ne soit pas contraire aux niveaux de classification.

[3] Lors de vidéoconférence de groupe avec échange (y compris partage d'écran) de données confidentielles, un modérateur doit être nommé. Il est en charge de veiller aux éléments de la remarque 1. Si des collaborateurs externes sont invités, ils ne peuvent pas l'être via des compte génériques.

[4] Les appels vocaux et les SMS standard via le réseau GSM sont protégés par la Loi sur lés communications et ne peuvent être interceptés que par des mesures de surveillance ou des systèmes d'espionnage type IMSI Catchers. Leur sécurité est donc très bonne.

[5] Cette fonction n'est pas encore disponible (pour plus de 2 personnes) sur iPhone.
Les séances organisées de manière pérenne avec des partenaires externes doivent faire l'objet d'une attention particulière. Ainsi, il est de la responsabilité de l'organisateur (cas échéant à l'Officier en charge) de veiller qu'un modérateur s'assure du respect des règles ci-dessus et vérifier que seules des personnes autorisées et identifiées soient présentes.

6. DEPLOIEMENT THREEMA WORK

Pour pouvoir échanger des informations et données sensibles entre corps de police, nécessitant une protection élevée, la solution Threema Work a été choisie par la TIP (Technique et informatique policière suisse) et remplace désormais la solution IMP.

Par défaut, tous les collaborateurs.trices de la PCV (policiers ou employé.e.s civil.e.s) disposant d'un smartphone professionnel disposent d'une licence Threema Work.

L'accès à l'annuaire des polices suisses participantes permet de retrouver facilement un contact parmi celles-ci, mais elle garantit aussi que les contacts font bien partie d'une organisation policière.
L'accès automatisé (synchronisation) n'est pas possible avec le carnet de contacts personnels de l'utilisateur, ni avec les contacts Threema (licence privée). Il est cependant possible de rajouter manuellement des contacts externes à Threema Work, par l'échange des Threema ID.

Plus de détails sur le déploiement de Threema Work se trouvent dans le guide de démarrage annexé.

6.1. Création de groupes dans Threema Work

Des groupes peuvent être créés via Threema Work de manière individuelle ou par une entité :

- De manière individuelle : une personne crée son groupe (il devient le seul administrateur possible) et y ajoute les utilisateurs de son choix. Si cet administrateur quitte le groupe, il ne peut pas remettre son rôle et il faudra créer un nouveau groupe (en clônant « l'ancien »).

- Par entité : une entité peut demander à bénéficier de Threema Broadcast. Une des fonctionnalité est qu'un ou des administrateurs locaux sont créés par la DAAP et gèrent ensuite le groupe depuis une console Web. Le groupe reste ainsi pérenne. La possibilité existe que les administrateurs locaux ou du système (DAAP) ne puissent pas voir ni participer aux discussions

7. DISPOSITIONS PARTICULIERES ET EXCEPTIONS

L'utilisation des outils de messagerie instantanée hors Theema Work et Webex, pour l'utilisation expliquée (cf. tableau), est interdite pour les échanges professionnels contenant des informations classées internes, confidentielles ou secrètes.

Des exceptions peuvent être admises notamment en matière de coopération intercantonale ou internationale, lorsqu'il faut s'adapter à d'autres outils de messagerie instantanée utilisés par le service leader qui conduit la coopération (état ou autorité de coordination).
Les exceptions doivent être communiquées au remplaçant de la commandante pour validation.

Pour les outils de visioconférence imposés par d'autres cantons ou la confédération lorsqu'ils organisent la séance, aucune demande d'exception n'est nécessaire.

Le directeur DDS

Nicola ALBERTINI, com princ

Le remplaçant de la commandante et
chef d'état-major

Patrick SUHNER

Validé le 29.11.202