# Recommandation de la CNIL sur les mots de passe et autres secrets partagés

## Tableau de correspondance avec les recommandations de l'ANSSI

| Recommandation CNIL – Recommandation générale | | Recommandation de l'ANSSI |
|---|---|---|
| 1 | Si le traitement comporte des risques spécifiques, est ce que des mesures complémentaires adaptées sont prévues ? | |
| 2 | Est-ce que des mesures complémentaires sont prévues pour les catégories d'utilisateurs à risques (tels que les administrateurs informatiques) ? | |
| **Gouvernance** | | |
| 3 | Une politique de gestion des mots de passe a-t-elle été formalisée et validée ? | R16, R20 |
| 4 | Les accès des personnels sont-ils revus au moins une fois par an ? | |
| 5 | L'application effective de la politique de gestion des mots de passe est-elle vérifiée au moins une fois par an ? | |
| 6 | La politique de gestion des mots de passe, en particulier ses mesures techniques, est-elle revue au moins une fois par an afin d'évaluer la nécessité d'une mise à jour ? | |
| 7 | Les personnes concernées sont-elles destinataires des parties de la politique de gestion des mots de passe qui les concerne ? | |
| 8 | L'ensemble des personnels ont-ils été formés ou sensibilisés à la gestion de leurs mots de passes ? | R17 |
| 9 | Un gestionnaire de mots de passe est-il proposé aux personnels ? | R31 |
| 10 | Est-ce que l'ensemble des mécanismes cryptographiques mis en œuvre respectent les règles et recommandations décrites dans les annexes B1 et B2 du RGS ou le guide mécanismes cryptographiques de l'ANSSI ? | |
| 11 | Est-ce que les logiciels et composants logiciels utilisés mettent en œuvre des versions à jour en ce qui concerne la sécurité ? | |

| | | | |
|---|---|---|---|
| 12 | | Est-ce qu'une veille sur les mises-à-jour et les vulnérabilités publiés est mise en œuvre pour l'ensemble des logiciels et composants logiciels utilisés ? | |
| 13 | A | Est-ce que la page d'authentification est sécurisée par le protocole TLS de manière conforme aux recommandations de l'ANSSI dans son document SDE-NT-35/ANSSI/SDE/NP1 intitulé « Recommandations de sécurité relatives à TLS » ? | R11 |
| | B1 | L'identité du serveur d'authentification est-elle contrôlée de manière sûre, par exemple par un certificat de sécurité ? | R11 |
| | B2 | La communication entre le client et le serveur d'authentification est-elle chiffrée ? | R11 |
| 14 | | S'il est fait usage de clés privées, ces dernières sont-elles conservées de manière sécurisée ? | |
| 15 | | Est-ce qu'aucun mot de passe n'apparait ni en clair ni haché dans les URL ? | |
| 16 | | Si l'authentification s'effectue sur une page web, est-ce que cette page ne contient ni publicité ni appel à des sites tiers ? | |
| **Choix de la PMP (Password management platform)** | | | |
| **Recommandations de la CNIL** | | | **Recommandations de l'ANSSI** |
| 17 | | Dans le cas où les utilisateurs ont la liberté de choisir des mots de passe non aléatoire, est-ce que les risques sur les personnes d'une usurpation d'identité ont été identifiés ? | |
| 18 | | Si les risques sur les personnes établis en 17 ne sont pas négligeables, est-ce que la politique mis en œuvre demande des mots de passe (très) longs plutôt que complexes ? | |
| 19 | | Si les risques sur les personnes établis en 17 sont, au moins, importants, est-ce que des mesures supplémentaires sont mises en œuvre (ex : augmentation de l'entropie, 2FA, etc.) ? | |
| 20 | | Si le mot de passe est destiné à être utilisé pour un traitement sensible à la soumission abusive de mots de passe (notamment les traitements accessibles via Internet), existe-t-il une taille maximale possible pour le mot de passe ? | R22 |
| 21 | | S'il ne s'agit pas de codes de déverrouillage, la taille maximale définie est-elle supérieure à 50 caractères ? | R22 |
| 22 | | Les mots de passe les plus courants sont-ils interdits ? | |
| 23 | | La comparaison avec les mots de passe les plus courants est-elle non-sensible à la casse ? | |

| | | |
|---|---|---|
| **24** | Le cas d'usage et le public ciblé a-t-il été pris en compte dans le choix des critères à imposer dans la politique de gestion des mots de passe ? | |
| **25** | Est-ce que la politique de mots de passe propose aux utilisateurs une politique de mot de passe correspondant à un des cas de la recommandation ou un niveau plus élevé ? | |
| **26** | Cas 1 : La politique correspond -elle à un niveau équivalent ou supérieur à 80 bits ? | |
| **27** | Cas 1 : Est-ce que mesures particulières ont été prises pour aider les utilisateurs à atteindre le niveau de sécurité (par exemple : outil de visualisation de la résistance du mot de passe) ? | |
| **28** | Cas 2 : La politique correspond -elle à un niveau équivalent ou supérieur à 50 bits ? | |
| **29** | Cas 2 : Est-ce qu'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives est mis en œuvre ? | |
| **30** | Cas 2 : L'impact de l'indisponibilité de leur compte sur les utilisateurs considérés a-t-il été évalué comme limité ou négligeable ? | |
| **31** | Cas 3 : La politique pour le mot de passe correspond -elle à un niveau équivalent ou supérieur à 13 bits ? | |
| **32** | Cas 3 : L'authentification concerne-t-il un matériel détenu en propre par une personne ? | |
| **33** | Cas 3 : Est-ce que le nombre d'essai d'authentification est limité à (au plus) 3 ? | |
| **Modalités pratiques générales** | | |
| **Recommandations de la CNIL** | | **Recommandations de l'ANSSI** |
| **34** | Les mots de passe sont-ils masqués par défaut lors de leur saisie ? | |
| **35** | Lors d'un échec d'authentification, le message d'erreur ne donne-t-il aucune information sur la cause de l'échec ? | R14 |
| **36** | S'il existe un mot de passe par défaut, est-il imposé à l'utilisateur de changer ce dernier lors de sa première connexion ? | R38 |
| **37** | Est-ce que l'utilisateur est en mesure de coller un mot de passe dans le champ prévu à cet effet depuis le presse-papier de son système d'exploitation ? | |
| **38** | Pour les mots de passes envoyés par voie postale, est-ce que des mesures pour détecter leur interception ou empêcher leur utilisation sont prévus ? | |

| | | |
|---|---|---|
| **39** | Pour tous les autres canaux, est-ce qu'aucun mot de passe n'est transmis en clair à l'utilisateur ? | |
| **40** | Est-ce que tous les mots de passes fournis à l'utilisateur sont soit temporaires soit à usage unique ? | |
| **Création, modification ou renouvellement d'un mot de passe** | | |
| **Recommandations de la CNIL** | | **Recommandation de l'ANSSI** |
| **41** | Des mesures techniques aident-elles à l'utilisateur de renseigner un mot de passe robuste ? | R27 |
| **42** | Les conditions d'acceptabilité du mot de passe sont-elles clairement affichées à l'utilisateur et cela de façon compréhensible par celui-ci ? | |
| **43** | Les utilisateurs sont-ils guidés dans le processus de sélection de leurs mots de passe afin de facilement déterminer un mot de passe robuste et conforme à la politique ? | |
| **44** | En cas de sélection d'un mot de passe non-conforme, est-il clairement affiché à l'utilisateur la règle ayant entraîné le rejet du mot de passe ? | |
| **45** | L'utilisateur est-il en mesure de modifier son mot de passe lui-même, en toute autonomie ? | |
| **46** | Est-ce qu'**il n'est pas** imposé aux utilisateurs de modifier leur mot de passe de manière périodique ? | R24 |
| **47** | Est-ce qu'**il est** imposé aux comptes à privilège de modifier leur mot de passe de manière périodique ? | R25 |
| **48** | Lorsqu'une réinitialisation est demandée par l'utilisateur, est-ce que seul un message du type « si un compte existe, alors une information est envoyée » est affiché ? | |
| **49** | Si le renouvellement du mot de passe se fait par l'envoi d'un lien ou d'un jeton par un autre canal, est-ce que cela se fait via un canal préalablement validé ? | |
| **50** | Est-ce que les canaux de communication récemment ajoutés ou modifiés sont exclus de ces envois ? | |
| **51** | Est-ce qu'un ajout, une modification ou une suppression des canaux de communication est systématiquement notifié à l'utilisateur ? | |
| **52** | S'il est envoyé un lien ou un jeton à l'utilisateur, ce lien ou jeton est-il à usage unique ? | |
| **53** | S'il est envoyé un lien ou un jeton à l'utilisateur, ce lien ou jeton a-t-il une durée de validité d'au maximum 24 heures ? | |

| | | |
|---|---|---|
| **54** | S'il est envoyé un lien ou un jeton à l'utilisateur, les liens ou jetons précédemment envoyés sont-ils automatiquement révoqués ? | |
| **55** | Si le renouvellement nécessite la réponse à des questions secrètes, est-ce que les informations habituellement publiques (nom des parents, lieu d'étude, nom des animaux de compagnie, etc.) sont exclues ? | |
| **56** | Les réponses à ces questions secrètes sont-elles conservées dans un endroit différent du mot de passe ou bien chiffrées ? | |
| **57** | Est-ce qu'un ajout, une modification ou une suppression de ces questions secrètes est systématiquement notifié à l'utilisateur ? | |
| **Stockage des mots de passe** | | |
| **Recommandations de la CNIL** | | **Recommandations de l'ANSSI** |
| **58** | Les mots de passe ne sont-ils jamais stockés en clair ? | R29 |
| **59** | Si un PAKE est mis en œuvre, s'agit-il d'un schéma public et prouvé sûr ? | |
| **60** | Dans le cadre du mécanisme d'authentification, les mots de passe stockés sont-ils conservés sous forme hachée avec une fonction spécialisée pour le stockage des mots de passe ? | R29 |
| **61** | La fonction de stockage de mots de passe choisie utilise-t-elle au moins un paramètre de configuration du coût en temps, au moins un paramètre de configuration du coût en mémoire et un sel ? | R29 |
| **62** | Le sel est-il généré aléatoirement et fait-il au moins 128 bits ? | R28 |
| **63** | Les paramètres sont-ils revus au moins une fois par an ? | R29 |
| **64** | Le choix de la fonction de hachage est-il réévalué au moins une fois par an ? | |
| **65** | Pour les gestionnaires de mots de passe, les mots de passe sont-ils stockés chiffrés avec un algorithme public réputé sûr (ie. conforme aux annexes B1 et B2 du RGS) ? | |
| **Gestion des compromissions** | | |
| **Recommandations de la CNIL** | | **Recommandations de l'ANSSI** |
| **66** | Les utilisateurs sont-ils systématiquement notifiés en cas de compromission avérée ou suspectée de ses moyens d'authentification ? | |

| | | |
|---|---|---|
| **67** | En cas de compromission avérée ou suspectée, est-ce qu'une évaluation du risque d'usurpation de compte et de ses impacts est prévue afin de décider de la nécessité de bloquer temporairement les comptes ou de renforcer l'identification des utilisateurs ? | |
| **68** | En cas de compromission avérée ou suspectée, l'utilisateur est-il obligé de renouveler son mot de passe ? | R26 |
| **69** | S'il est fait usage d'une information complémentaire (cas nº 3), cette dernière est-elle obligatoirement renouvelée en cas de compromission avérée ou suspectée ? | |
| **70** | S'il est fait usage de questions secrètes, ces dernières et leurs réponses sont-elles obligatoirement renouvelées en cas de compromission avérée ou suspectée ? | |
| **Journalisation** | | |
| **Recommandations CNIL** | | **Recommandations ANSSI** |
| **71** | Les authentifications réussies sont-elles journalisées ? | |
| **72** | Les échecs d'authentification sont-ils journalisés ? | |
| **73** | Est-ce que les mots de passe utilisés sont exclus de toute journalisation ? | |
| **74** | Est-ce que les identifiants inconnus du système sont exclus de la journalisation ? | |
| **Sous-traitants et éditeurs de logiciels** | | |
| **Recommandations CNIL** | | **Recommandations ANSSI** |
| **75** | Le contrat stipule-t-il clairement le périmètre des responsabilités ? | |
| **76** | Le contrat stipule-t-il clairement le niveau de sécurité du système ? | |
| **77** | Une documentation reprenant l'ensemble des points des présentes recommandations techniques indiquant est-elle mise à disposition des responsables de traitements ? | |
| **78** | Pour les logiciels, une documentation précise-t-elle les modalités de génération, stockage et transmission des mots de passe ? | |
| **79** | La solution est-elle configurable de manière à respecter l'ensemble des présentes recommandations techniques ? | |

| | | |
|---|---|---|
| **80** | La solution est-elle configurée par défaut de manière à respecter l'ensemble des présentes recommandations techniques ? | |
| **81** | En cas d'hébergement pour le compte d'un responsable de traitement, les journaux sont-ils régulièrement audités de manière à détecter des comportements suspects ? | |
| **82** | En cas d'hébergement pour le compte d'un responsable de traitement, les compromissions avérées ou suspectées sont-elles systématiquement notifiées au responsable de traitement ? | |