NOTE D'ORIENTATION SUR LES SYSTÈMES D'INFORMATION ET LE PARTAGE DE DONNÉES

19 août 2020

Objectif

L'utilisation de systèmes d'information, notamment de la communication par courrier électronique et du partage électronique de données, est cruciale pour la réalisation efficace des objectifs institutionnels et est essentielle pour que les données financières soient disponibles de manière efficace, fiable et opportune aux fins des prises de décisions à différents niveaux de mise en œuvre des subventions.

L'utilisation de ces systèmes expose toutefois les organisations à des risques liés à la cybersécurité, notamment aux courriels de hameçonnage, une pratique frauduleuse qui consiste à collecter des informations importantes auprès d'utilisateurs ou à leur fournir des renseignements incorrects en vue d'obtenir des avantages illégitimes.

C'est pourquoi il est demandé aux récipiendaires principaux de mettre à jour, selon que de besoin, leur manuel de procédures et leurs directives internes afin de garantir que des mesures efficaces de contrôle de la gestion soient en place pour préserver les données liées aux activités mises en œuvre dans le cadre des subventions du Fonds mondial. Il convient en particulier de sécuriser les données critiques, notamment les données relatives aux comptes bancaires, aux fournisseurs, aux prestataires de services, aux consultants et au personnel. Cela peut requérir d'introduire ou de modifier les procédures afin de pouvoir appliquer les contrôles exposés dans les recommandations ci-après.

La présente note d'orientation ne modifie aucunement les droits ou obligations au titre des accords de subvention du Fonds mondial ni ne constitue une renonciation à ceux-ci. Les récipiendaires principaux doivent continuer de s'assurer qu'eux-mêmes, et tous leurs partenaires de mise en œuvre (y compris les sous-récipiendaires, les fournisseurs et les sous-traitants), respectent les lois et réglementations applicables, notamment en matière de collecte et de traitement de données à caractère personnel et de communication de ces données au Fonds mondial à la demande de celui-ci[1].

Principes clés

Les principes clés suivants doivent être appliqués dans tous les cas, quelle que soit la nature des données critiques :

- **Répartition des responsabilités** – Le personnel chargé du traitement des paiements ne doit pas avoir accès à la base de données principale associée administrée par le récipiendaire principal ou le maître d'œuvre de la subvention, ni pouvoir la modifier. Les modifications des données critiques doivent être approuvées par un membre du personnel de haut niveau, dûment

[1] Pour de plus amples informations, veuillez vous reporter à la politique de confidentialité du Fonds mondial, disponible (en anglais) à l'adresse suivante : https://www.theglobalfund.org/en/legal/privacy-statement/

habilité et dont la fonction est séparée des personnes chargées des procédures de paiement et de modification ;

- **Redevabilité** – La base de données doit être administrée par du personnel dûment habilité au regard de chaque module respectif, et les différents modules doivent être mutuellement intégrés. Ce principe s'applique à la gestion des fichiers Excel s'il s'agit d'un système à saisie manuelle.
- **Confirmation** – Pour tous les paiements de plus de 50 000 dollars US[2], il est fortement recommandé que le récipiendaire principal obtienne confirmation auprès de la personne de contact désignée chez le fournisseur avant de procéder au paiement.

Contrôles spécifiques

Comptes bancaires

- Les données relatives aux comptes bancaires doivent être conservées dans le module de gestion de la trésorerie de la base de données, ou dans des fichiers en cas de système manuel, par une personne ou un service fonctionnellement séparé(e) de la personne ou du service chargé(e) du traitement des paiements.
- Les récipiendaires principaux sont vivement encouragés à mettre en œuvre des critères de signataires multiples pour les transactions importantes ou complexes. Ils sont également encouragés à changer régulièrement les signataires autorisés pour les décaissements.
- Les exigences (visées à l'annexe 1) relatives à l'ajout ou à la suppression de coordonnées bancaires doivent être appliquées avant de mettre à jour le module de gestion de la trésorerie de la base de données ou les systèmes manuels, selon le cas. Veuillez vous reporter à la section 5.6.1 – *Gestion des comptes bancaires* du manuel de gestion financière à l'intention des maîtres d'œuvre des subventions pour de plus amples détails.

Fournisseurs et prestataires de services

- Les récipiendaires principaux doivent disposer d'une procédure claire d'exécution de vérification préalable et des antécédents avant de signer ou de modifier un contrat passé avec tout fournisseur ou prestataire de services, y compris de vérification des renseignements clés tels que l'enregistrement de l'entreprise (certificat) et les coordonnées bancaires.
- Toutes les informations clés, notamment le nom de l'organisation, le signataire autorisé, la personne de contact, l'adresse et les coordonnées bancaires, doivent figurer expressément dans le contrat.
- Toute demande de modification d'informations clés du fournisseur ou du prestataire de services doit être étayée par la documentation requise, vérifiée et approuvée par un membre autorisé du personnel avant que l'information puisse être modifiée dans la base de données et dans le contrat.
- Toute correspondance sensible, notamment concernant toute demande de modification des informations clés du fournisseur ou du prestataire de services, doit être effectuée exclusivement par l'intermédiaire de la personne de contact désignée dans le contrat.
- Le fournisseur ou prestataire de services ne peut être classé inactif dans le système que lorsque tous les passifs et obligations au titre d'un contrat auquel le fournisseur ou le prestataire de services est partie ont été entièrement acquittés.

[2] Ou d'un montant supérieur au seuil défini par le récipiendaire principal, si ce seuil est inférieur à 50 000 dollars US.

Personnel et consultants

- Les données à caractère personnel, notamment les noms, dates de naissance et coordonnées bancaires, doivent être conservées dans le module Ressources humaines de la base de données, ou dans des fichiers de personnel, par des membres habilités du personnel du récipiendaire principal.
- Les membres du personnel responsables de la préparation de la paie ou des paiements ne doivent pas avoir les droits ou accès nécessaires pour modifier les données à caractère personnel du personnel de l'organisation.
- Les données à caractère personnel figurant dans le module RH doivent être intégrées avec les données du module de gestion de la trésorerie afin de faciliter les paiements. En cas de système manuel, des mesures appropriées de contrôle de la gestion, notamment de vérification, d'examen et d'approbation, doivent être en place.
- Pour de plus amples détails sur la création, la modification ou la suppression de données sur le personnel, veuillez vous reporter à la section 4.5 - *Ressources humaines* du manuel de gestion financière à l'intention des maîtres d'œuvre des subventions.
- Des protections doivent être en place pour les données identifiant, ou susceptibles d'être utilisées pour identifier, des personnes telles que des membres du personnel et des consultants. Ces protections peuvent comprendre des mesures techniques et organisationnelles telles que des autorisations d'accès, l'anonymisation, le classement confidentiel de données à caractère personnel sensibles, des périodes de conservation garantissant que les données à caractère personnel ne sont pas conservées au-delà du délai nécessaire et des systèmes sécurisés pour le stockage et le transfert de ces données.
- Pour des orientations plus détaillées sur la protection des données à caractère personnel, veuillez vous reporter aux recommandations publiées par l'autorité compétente en matière de protection des données dans votre territoire.

Renforcement de vos systèmes de gestion de la sécurité des informations

Les maîtres d'œuvre doivent prendre des mesures en vue de renforcer en permanence la sécurité des informations de leur architecture informatique et numérique, conformément aux normes internationales en matière de pratiques exemplaires comme les normes ISO 27001[3] et ISO 27002[4] (codes de bonne pratique). Ces normes offrent aux maîtres d'œuvre des orientations sur la manière de gérer les risques liés à la sécurité des informations, de manière à préserver la confidentialité, l'intégrité et la disponibilité des informations en appliquant une procédure de gestion des risques et en garantissant aux parties intéressées que les risques sont gérés de manière adéquate.

Les références suivantes peuvent par ailleurs aider les maîtres d'œuvre dans le cadre du développement de leur architecture numérique et informatique, notamment en ce qui concerne la définition des politiques et normes de sécurité et de protection de la confidentialité :

1. Guide pratique OMS-UIT sur les stratégies nationales en matière de cybersanté[5] ;
2. *Digital Health Platform Handbook: Building a Digital Information Infrastructure for Health*, Genève, Union internationale des télécommunications[6] ; et
3. Principes de développement numérique[7].

[3] https://www.iso.org/fr/isoiec-27001-information-security.html
[4] https://www.iso.org/fr/standard/54533.html
[5] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-E_HEALTH.05-2012-PDF-F.pdf
[6] https://ehna.acfee.org/c67802a7d4b3dc8914700842bf6776402b8d343c.pdf
[7] https://digitalprinciples.org/

Formation du personnel

Dans le cadre de la gestion élémentaire des risques financiers et de cybersécurité et des bonnes pratiques en la matière, les récipiendaires principaux doivent veiller à ce que leur personnel soit dûment formé et conscient des caractéristiques des cyberattaques et des méthodes utilisées, notamment de hameçonnage. Ils doivent affecter des membres du personnel à la tâche de répondre aux questions liées aux risques financiers et cyber.

Une formation sur le hameçonnage est disponible en ligne pour les partenaires externes (cliquez ici). Tous les membres du personnel des instances de coordination nationale, des récipiendaires principaux et des sous-récipiendaires réalisant des transactions financières sont tenus de suivre cette formation. Celle-ci dure 15 minutes.

Les membres du personnel exerçant les activités ci-après sont tenus de suivre cette formation :

1. Modification des données concernant des tiers (banques, fournisseurs, membres du personnel et consultants) ;
2. Règlement des transactions ;
3. Émission d'ordres de paiement.

Il incombe également aux récipiendaires principaux de veiller à ce que les sous-récipiendaires suivent cette formation. Les agents locaux du Fonds s'assureront de la mise en œuvre de la formation dans le cadre du prochain rapport sur les résultats actuels et la demande de décaissement.

Les participants qui ne sont pas encore inscrits sur la plateforme iLearn du Fonds mondial sont priés de le faire (cliquez ici). Une fois inscrits, ils pourront accéder à d'autres formations en ligne gratuites du Fonds mondial, telles que des formations sur l'établissement des subventions et sur la communication d'informations par les récipiendaires principaux.

L'annexe 2 à la présente note d'orientation met en lumière des options et ressources connexes à ces fins. Les récipiendaires principaux doivent les étudier, ainsi que les autres ressources disponibles, et s'assurer que les membres de leur personnel sont vivement encouragés à suivre des formations appropriées.

Annexe 1 : Recommandations concernant les procédures internes relatives à la création, modification ou suppression de données clés liées aux fournisseurs et prestataires de services

Informations clés	Création	Modification	Suppression
Compte bancaire	▪ Les coordonnées bancaires doivent être incluses dans la base de données uniquement si les conditions suivantes sont respectées : ✓ un formulaire de coordonnées bancaires est fourni (de préférence dans un format prédéfini fourni par le récipiendaire principal) ; ✓ le fournisseur ou prestataire de services fournit la liste des signataires bancaires autorisés (au moins deux signataires), assortie de spécimens certifiés des signatures ; ✓ les procédures de signature multiple pour les transactions complexes ou importantes (au-delà d'un seuil donné) sont fournies ; ✓ une (lettre de) confirmation est obtenue auprès de la banque gestionnaire du compte concerné, sur papier à en-tête de la banque ; ✓ la banque gestionnaire du compte figure sur la liste de la Banque mondiale des banques commerciales admissibles (ou sur une autre liste reconnue à l'international) ; ✓ la banque a été approuvée au terme d'un contrôle antiterroriste, par exemple au travers de ✓ https://bridgerinsight.lexisnexis.com/ ; ✓ l'IBAN du compte a été vérifié, par exemple sur https://www.tbg5-finance.org/?ibancheck.shtml ; et ✓ le code SWIFT de la banque a été vérifié sur https://www2.swift.com/bsl/index.faces. ➢ **Signaux d'alerte** : ○ Le compte bancaire est à un autre nom que celui du fournisseur ou prestataire de services ○ L'adresse du titulaire du compte est différente de l'adresse enregistrée du fournisseur ou prestataire de services	▪ Les coordonnées bancaires ne peuvent être modifiées que lorsque : ✓ toutes les étapes figurant dans la colonne Création ont été appliquées ; ✓ la demande est envoyée par la personne de contact désignée dans une communication officielle sur papier à en-tête officiel ; ✓ la demande est dûment signée par un signataire autorisé ; ✓ la modification est valablement justifiée dans la demande ; ✓ la modification doit être examinée par un membre du personnel de haut niveau avant d'être validée ; et ✓ la personne traitant le paiement est différente de la personne validant la modification (répartition des tâches).	▪ Les coordonnées bancaires doivent être classées inactives dans la base de données lorsque tous les passifs au titre d'un contrat concerné ont été pleinement acquittés. ▪ Du personnel de haut niveau et indépendant doit examiner annuellement l'ensemble de la base de données de fournisseurs/prestataires de services pour confirmer leur statut actif/inactif. ➢ **Signaux d'alerte** : Il n'y a aucun passif impayé au titre d'un contrat en cours mais le fournisseur ou prestataire de services apparaît encore comme étant actif dans la base de données.
Personne de contact pour les avis	Les coordonnées (y compris de courrier électronique) de la personne autorisée à recevoir et envoyer de la correspondance au nom du fournisseur ou prestataire de services doivent être indiquées dans tout contrat pertinent.	Toutes les étapes figurant dans la colonne Création doivent être appliquées. Toute demande de modification des coordonnées de la personne de contact doit être transmise exclusivement par un représentant autorisé de l'entité en question dans un courrier officiel, et confirmée par le maître d'œuvre (par du personnel de haut niveau du maître d'œuvre ou de l'entité concernée pour laquelle la personne travaille).	

Informations clés	Création	Modification	Suppression
Signataire de contrats autorisé	Des données de signataire autorisé ne doivent être créées que lorsque : ✓ des preuves de son autorité pour signer le contrat concerné au nom de l'entité sont fournies (par ex. par un certificat de la direction, les statuts) et vérifiées ; et ✓ le signataire fournit un spécimen certifié de sa signature (de préférence dans un format prédéfini fourni par le récipiendaire principal ou le maître d'œuvre de la subvention).	Toutes les étapes figurant dans la colonne Création doivent être appliquées. Toute demande de modification des signataires autorisés (par ex. pour des modifications du contrat) doit être envoyée par la personne de contact désignée dans une communication officielle sur papier à en-tête officiel et dûment vérifiée par le maître d'œuvre (confirmation de la direction) avant de procéder à toute modification.	
Adresse et coordonnées de contact de contrepartie	L'adresse enregistrée, l'adresse de correspondance, de courrier électronique et les numéros de téléphone et de télécopie de l'entité doivent être indiqués dans chaque contrat concerné. L'adresse enregistrée doit être vérifiée dans les registres publics, le cas échéant.	Toute demande de modification de l'adresse enregistrée ou de correspondance de l'entité doit être communiquée par la personne de contact de l'entité et dûment vérifiée par le maître d'œuvre par confirmation par la direction avant qu'il soit procédé à toute modification. Toutes les étapes figurant dans la colonne Création doivent être appliquées.	

Annexe 2 : **Ressources supplémentaires relatives à la sécurité des informations pour faire face aux risques cyber**

Outre la formation en ligne sur le hameçonnage proposée par le Fonds mondial, les récipiendaires principaux peuvent solliciter un éventail de services auprès de prestataires de services de sécurité des informations :

1. Formation en matière de sécurité des informations
2. Renforcement des systèmes de gestion des informations

Le Fonds mondial est en train de dresser une liste de fournisseurs préapprouvés d'assistance technique susceptibles d'aider les récipiendaires principaux et autres maîtres d'œuvre de subventions à améliorer les systèmes de gestion des informations et la cybersécurité.

Les récipiendaires principaux et autres maîtres d'œuvre de subventions pourraient par ailleurs envisager l'authentification multifacteur. Veuillez vous reporter aux conditions générales et aux orientations du fournisseur de services de messagerie électronique concerné concernant l'activation de l'authentification multifacteur. Voir les liens ci-après pour de plus amples détails concernant Gmail et Yahoo :

- Gmail : https://www.google.com/landing/2step/
- Yahoo : https://help.yahoo.com/kb/add-two-step-verification-extra-security-sln5013.html

Les récipiendaires principaux et autres maîtres d'œuvre de subventions peuvent également consulter le code de bonne pratique ISO 27002 pour le management de la sécurité de l'information[8]. Un système robuste de gestion de la sécurité de l'information peut bénéficier aux récipiendaires principaux et autres maîtres d'œuvre de subventions en donnant à leurs bénéficiaires et parties prenantes l'assurance qu'ils peuvent protéger leurs informations, gérer leurs finances et améliorer la sécurité de la chaîne d'approvisionnement.

[8] https://www.iso.org/fr/standard/54533.html