Fédération internationale des Sociétés
de la Croix-Rouge et du Croissant-Rouge

Sécurité de l'information : Politique d'utilisation

Numéro de référence : 062

Autorisation				
Attribution	**Nom**	**Fonction**	**Signature**	**Date d'approbation**
Auteur	Ed Happ	Chef, Département des systèmes d'information (ISD)		20 décembre 2013
Propriété	Michael Veltman	Chef, Département des ressources humaines		19 février 2014
Approbation	Malika Aït-Mohamed Parent	Sous-secrétaire généralee, Soutien aux organes statutaires et à la direction		20 décembre 2013
Approbation	Matthias Schmale	Sous-secrétaire général, Développement des Sociétés nationales et des connaissances		20 décembre 2013
Consultation	Sayed Hashem	Chef, Département gestion des risques et audit		20 décembre 2013
Consultation	Élise Baudot	Chef, Département juridique		20 décembre 2013

Version : 2.5
Approuvé le 19 février 2014
Classification du document : interne

Historique des modifications

Le présent document est soumis à des mesures de contrôle des modifications ; toute modification aux versions principales est mentionnée ci-dessous

Historique des modifications

Version	Date	Commentaires
1.0	Octobre 2007	Première version de la politique
2.1	7 juin 2013	Politique révisée
2.2	17 juin 2013	Projet révisé comprenant les commentaires formulés par les parties prenantes consultées et reçus au 14 juin 2013
2.3	2 juillet 2013	Projet révisé comprenant les commentaires formulés par les parties prenantes consultéss et reçus au 1er juillet 2013
2.4	15 juillet 2013	Projet révisé comprenant les commentaires reçus au 12 juillet 2013
2.5	29 juillet 2012	Projet révisé comprenant les commentaires reçus au 26 juillet 2013

Avertissement

La version papier du présent document peut ne pas être la dernière version disponible. La dernière version, qui prévaut sur toutes les versions antérieures, peut être consultée sur FedNet.

Glossaire

Classification des informations : définit, sur la base de critère spécifiques, comment l'information doit être classée.

Confidentialité : fait de s'assurer que l'information n'est pas accessible ou ne peut être divulguée aux personnes, sociétés ou processus non autorisés.

Disponibilité : aptitude d'un utilisateur à accéder dans un lieu donné et dans le bon format aux informations quand il en a besoin.

Employé : se réfère à une catégorie de personnel de la Fédération. Ce terme désigne le personnel basé à Genève et les délégués (voir le Règlement du personnel et le Règlement interne de la Fédération).

Informations essentielles : collection identifiable d'informations sauvegardées sur un support (électronique, imprimé) et jugées importantes pour permettre à l'organisation de réaliser ses activités.

Intégrité de l'information : garantie de la précision et de l'exhaustivité de l'information tout au long de son cycle de vie.

Période de conservation : les dossiers de la Fédération doivent être détruits conformément aux règles relatives à la conservation et à la destruction des documents approuvées dans chaque département (voir les règles de la Fédération en matière de catégorie de classement et de conservation et de destruction des documents sur FedNet pour plus de détails).

Personnel : désigne les employés de la Fédération (personnel basé à Genève et délégués), le personnel local, les consultants, les volontaires et les stagiaires, ainsi que le personnel détaché et tous les individus travaillant au nom de la Fédération et sous son statut juridique (voir le Code de conduite de la Fédération).

Politique du bureau propre : politique qui exige des membres du personnel qu'ils débarrassent leur bureau de tout document avant de le quitter à la fin de la journée.

Principe du besoin d'en connaître : l'accès doit être réservé aux personnes qui en ont besoin dans l'exercice de leurs fonctions officielles.

Propriétaire des informations essentielles : personne ou groupe de personnes chargés de garantir la confidentialité des informations essentielles. Par défaut et sauf mention contraire, le responsable chargé des informations en est le propriétaire.

Renseignements nominatifs : les renseignements nominatifs se réfèrent à des informations qui, par elles-mêmes ou associées à d'autres informations, peuvent être utilisées pour identifier, contacter ou localiser une personne (par exemple, nom, adresse électronique, date de naissance, numéro de passeport, numéro d'assurance sociale, casier judiciaire, etc.).

Restrictions applicables selon la classification des informations : définit la manière dont les informations essentielles, sur la base de leur classification, doivent être gérées.

Sécurité de l'information : désigne le processus visant à protéger les données stockées, en transit ou en traitement de tout accès ou de toute utilisation, divulgation, destruction ou modification non autorisée ou de toute interruption accidentelle ou intentionnelle. Le processus de sécurité de l'information garantit la confidentialité, l'intégrité et la disponibilité de l'information.

Utilisateurs : dans le présent document, le terme utilisateurs désigne l'ensemble du personnel de la Fédération, les sous-traitants et les fournisseurs tiers autorisés à accéder aux informations ou données de la Fédération, à les manipuler ou à les utiliser.

Sommaire

1. Introduction

La Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge (la Fédération) utilise de différentes manières l'information qu'elle reçoit et qu'elle traite. Sa réputation et l'efficacité de son action peuvent être considérablement mises en péril si les utilisateurs, c'est-à-dire le personnel[1], les sous-traitants et les fournisseurs tiers autorisés à accéder aux informations de la Fédération, à les manipuler ou à les utiliser ne se conforment pas aux normes et mesures de contrôle en matière de sécurité de l'information.

Il incombe au Département des systèmes d'information de garantir la sécurité et l'intégrité des systèmes d'information et de communication de la Fédération. Avec le Département des ressources humaines, il veille à faire connaître le cadre de la Fédération pour la sécurité de l'information[2] et les normes de conduite qui doivent être respectées par les utilisateurs concernant l'utilisation des ressources en technologies de l'information et de la communication[3]. Le Département des systèmes d'information est également chargé de prendre toutes les mesures nécessaires en cas de non-respect de ces normes.

2. Objectif

Conformément aux règles applicables en matière de sécurité de l'information, la présente politique définit ce que les utilisateurs doivent faire et ne pas faire pour :

- mettre en place des mesures de contrôle adéquates en matière de sécurité de l'information, et
- garantir que l'utilisation que les membres du personnel font des ressources de la Fédération en technologies de l'information et de la communication est efficace et conforme aux Principes fondamentaux du Mouvement international de la Croix-Rouge et du Croissant-Rouge (le Mouvement).

3. Champ d'application et portée

Le cadre pour la sécurité de l'information, y compris la présente politique, s'applique à l'ensemble des utilisateurs. La présente politique s'applique également aux Sociétés nationales participantes et aux Sociétés nationales hôtes qui ont signé un accord avec la Fédération et relèvent de sa responsabilité en matière de sécurité, et qui doivent se conformer au Code de conduite. La présente politique n'est pas applicable aux Sociétés nationales qui ne sont pas intégrées aux délégations de la Fédération sur le terrain et qui ne peuvent bénéficier que d'un accès « invité », sauf signature de la présente politique.

La politique s'applique aux informations et aux données quel que soit leur format, notamment les copies papier de documents, les données électroniques, images, déclarations verbales, équipements informatiques, réseaux ou équipements de communication de données, programmes informatiques, procédures et logiciels, dispositifs et supports de sauvegarde de données.

[1] Voir le glossaire pour une définition du terme « personnel ».
[2] Voir la Charte relative à la sécurité de l'information pour plus de détails.
[3] Aux fins de la présente politique, les ressources en technologies de l'information et de la communication comprennent le matériel, tels que les ordinateurs de bureau, les ordinateurs portables, les notebooks, les téléphones mobiles et satellites et toute autre application liée, toutes données et tout logiciel sous licence ou détenus par la Fédération.

4. Normes en matière de sécurité de l'information

Il incombe à l'ensemble des utilisateurs de mettre en œuvre les contrôles adéquats pour limiter les risques en matière de sécurité de l'information ou des données auxquelles ils ont accès, qu'ils manipulent ou utilisent et de signaler tout abus aux responsables concernés[4].

Conformément aux Principes de classification de l'information[5], les contrôles appropriés sont définis selon la catégorie de l'information/des données utilisées, qui est spécifiée par le propriétaire des informations[6] dans l'information/les données elles-mêmes, quel que soit le support (document, électronique)[7].

5. Bonnes pratiques

Il est recommandé aux utilisateurs de se conformer aux règles générales ci-dessous afin de limiter au minimum les risques en matière de sécurité de l'information.

- Aucune information ne doit être sauvegardée sur le disque local (C:\) ou le bureau de l'ordinateur. Les sauvegardes effectuées sur le bureau sont un frein à la flexibilité et ralentissent le processus de connexion. De plus, des données peuvent être perdues, le Département des systèmes d'information ne faisant aucune sauvegarde du disque local ou du bureau.
- Lorsqu'ils recrutent des collaborateurs temporaires ou occasionnels, les responsables doivent déterminer les systèmes et dossiers auxquels ces utilisateurs ont accès pour exercer leurs fonctions avant de demander aux Services d'assistance de leur donner accès au réseau.
- Il est recommandé aux utilisateurs de verrouiller leur ordinateur lorsqu'ils laissent leur poste de travail sans surveillance un court moment ou de se déconnecter lorsqu'ils sont susceptibles de s'absenter plus longtemps.

6. Utilisation admise des ressources en technologies de l'information et de la communication

Les principes suivants s'appliquent concernant l'utilisation des ressources de la Fédération en technologies de l'information et de la communication :

1. Les ressources en technologies de l'information et de la communication ne peuvent être utilisées que pour des motifs légitimes liés aux activités de la Fédération. Lorsqu'ils utilisent ces ressources, les membres du personnel sont tenus de respecter et d'appliquer les normes éthiques et de conduite professionnelle les plus rigoureuses. Tout abus peut donner lieu à des mesures disciplinaires pouvant aller jusqu'au licenciement.

2. Les ressources en technologies de l'information et de la communication doivent être utilisées dans le strict respect des Principes fondamentaux du Mouvement, de la présente Politique et du Code de conduite du personnel.

3. Il incombe aux utilisateurs de garder en sûreté tous les équipements informatiques qui leur sont fournis (tels que des ordinateurs portables ou des téléphones mobiles). Toute perte doit être signalée

[4] Voir la Charte relative à la sécurité de l'information pour plus d'informations sur le rôle et les responsabilités.
[5] Voir les Principes en matière de classification de l'information sur FedNet. Les contrôles de classification de l'information sont également disponibles dans l'annexe du présent document.
[6] Voir le glossaire pour une définition de « détenteur de l'information ».
[7] Voir les Principes en matière de classification de l'information pour plus de détails.

aux Services d'assistance dans les meilleurs délais avec les détails des données sauvegardées sur l'équipement.

4. L'utilisation que les membres du personnel font des ressources en technologies de l'information et de la communication doit être conforme aux lois nationales et internationales relatives à la fraude informatique, à la pornographie, à l'utilisation abusive des équipements et ressources informatiques, à la confidentialité des informations etaux infractions pénales qui y sont liées et à toute autre norme légale telles que les normes relatives aux droits d'auteur et aux obligations découlant de la licence.

5. L'utilisation des ressources en technologies de l'information et de la communication peut être contrôlée pour des raisons de sécurité, de gestion du réseau ou d'autres raisons, et soumise à restriction.

7. Utilisation non admise des ressources en technologies de l'information et de la communication

Toute utilisation des ressources en technologies de l'information et de la communication à des fins répréhensibles, illégales ou contraires au Code de conduite, à la présente Politique, au Règlement interne ou aux politiques relatives aux ressources humaines est interdite. Sont notamment inacceptables et interdits les actes suivants :

1. Utiliser les ressources de la Fédération en technologies de l'information et de la communication en violation du Code de conduite ou de la présente Politique.

2. Visiter sur Internet, télécharger, envoyer par courrier électronique ou consulter volontairement des contenus indécents, pornographiques, haineux ou désobligeants (sauf instruction spécifique dans le cadre du travail). L'accès à ces contenus constitue une faute grave qui peut être sanctionnée par un licenciement sans préavis.

3. Tenter de contourner le système de sécurité, d'accéder à des données non autorisées ou de modifier des données sans autorisation.

4. Utiliser les ressources en technologies de l'information et de la communication sous une fausse identité ou en usurpant l'identité d'un tiers (sauf si cela est nécessaire, par exemple pour tester les systèmes d'information).

5. Utiliser ou installer des accessoires non standard ou des logiciels non autorisés[8]. Toute utilisation des ressources en technologies de l'information et de la communication doit être conforme aux obligations contractuelles de la Fédération, notamment aux restrictions contenues dans les logiciels et autres accords de licence.

6. Les utilisateurs ne sont pas autorisés à configurer Outlook de façon à transférer leurs messages électroniques vers leur adresse électronique personnelle ou toute autre adresse en dehors de la Fédération, et ce afin de limiter le risque que des données sensibles soient transférées vers des systèmes de messagerie non sécurisés.

7. Utiliser les ressources en technologies de l'information et de la communication en violation des lois civiles ou pénales, y compris les normes applicables aux droits d'auteur qui régissent la copie, l'affichage et l'utilisation des logiciels et autres supports numériques.

[8] Voir la liste des exceptions sur https://servicedesk.ifrc.org

8. Utilisation des ressources en technologies de l'information et de la communication à des fins personnelles

Les membres du personnel sont autorisés, dans la limite du raisonnable, à utiliser les ressources de la Fédération en technologies de l'information et de la communication pour des motifs personnels. Il appartient à la seule Fédération d'apprécier le caractère raisonnable de l'utilisation en fonction des circonstances. La Fédération peut, si elle l'estime nécessaire, restreindre ou interdire l'utilisation à des fins personnelles des ressources en technologies de l'information et de la communication, lesquelles sont destinées en priorité aux activités professionnelles.

L'utilisation à des fins personnelles des ressources en technologies de l'information et de la communication ne doit pas nuire au bon fonctionnement du réseau, ni entraver ou distraire les autres membres du personnel dans leur travail ni engendrer des coûts supplémentaires pour la Fédération ou engager sa responsabilité. De même, l'utilisation de ces ressources à des fins personnelles ne doit pas empêcher l'employé de remplir ses fonctions. Sont considérées comme des activités susceptibles d'avoir un impact sur le travail de la Fédération (que ce soit en termes de coût, de capacité du réseau ou autres) : les communications personnelles, le partage de données à débit élevé (telles que les vidéos ou la diffusion en flux continu), l'utilisation de la vidéconférence, les jeux interactifs, le téléchargement de fichiers importants et l'utilisation de messageries instantanées. Les membres du personnel sont tenus de prendre conseil auprès du Département des systèmes d'information en cas de doute sur l'impact potentiel de l'utilisation qu'ils font des ressources en technologies de l'information et de la communication de la Fédération.

Les membres du personnel sont autorisés à utiliser ponctuellement (et dans les limites du raisonnable) les systèmes informatiques de la Fédération pour stocker et transmettre, à leurs propres risques, des fichiers et des messages personnels. La Fédération ne peut garantir la confidentialité de ces fichiers ou messages et peut limiter ou mettre fin à cette tolérance si elle l'estime nécessaire.

9. Utilisation du courrier électronique

Les utilisateurs doivent être conscients du fait que chaque fois qu'ils envoient un courriel en utilisant l'adresse « ___.ifrc.org », ils représentent la Fédération. Selon leur contenu, les courriels peuvent entraîner des obligations juridiques pour la Fédération et porter atteinte à sa réputation. En conséquence, les utilisateurs doivent veiller à respecter les normes éthiques les plus strictes.

Sont considérées comme des pratiques répréhensibles : le fait de poster des messages hostiles et incendiaires (« flaming ») ; le fait d'envoyer des pourriels ou de participer à une chaîne de courriels ; le fait d'usurper l'identité d'un autre utilisateur et d'envoyer des courriels insultants et désobligeants.

Les utilisateurs devraient mettre en œuvre des contrôles appropriés de la sécurité de l'information et adopter de bonnes pratiques concernant l'utilisation du courrier électronique, notamment archiver les courriels reçus, limiter la taille des fichiers attachés et limiter au strict nécessaire l'utilisation de la fonction « répondre à tous ». Les courriels et fichiers personnels ne seront archivés dans le système que dans la limite qui sera strictement nécessaire. Les courriels reçus ou envoyés à titre de communication officielle doivent être archivés et conservés aussi longtemps que nécessaire pour satisfaire aux exigences administratives et juridiques de la Fédération.

10. Sécurité

Toutes les données électroniques (personnelles ou officielles) transférées ou sauvegardées dans le système informatique de la Fédération sont la propriété de cette dernière. La Fédération se réserve le

droit d'accéder à ces données, notamment à tous les courriels et messages SMS reçus ou envoyés via son système informatique, de les consulter ou de les modifier.

Il incombe aux utilisateurs de garantir la sécurité des données concernant leur compte personnel et leurs mots de passe.

- Les utilisateurs doivent s'abstenir d'utiliser comme mot(s) de passe des mots qui peuvent être associés avec eux (par exemple, leur nom, leur date de naissance, etc.).
- Ils doivent veiller à mémoriser leur(s) mot(s) de passe et à ne pas l'écrire/les écrire ou le(s) communiquer à d'autres.

Les utilisateurs doivent être conscients des dangers liés aux virus et autres programmes malveillants et s'engagent à prendre les mesures nécessaires pour protéger les ressources de la Fédération en technologies de l'information et de la communication, notamment à :

- procéder à la mise à jour régulière des programmes antivirus afin que les ressources en technologies de l'information et de la communication placées sous leur contrôle soient protégées contre les programmes malveillants, et
- effectuer une analyse antivirus avant toute utilisation d'un support amovible sur le système de la Fédération.

11. Droits d'auteur, licence et logiciel

La Fédération a pour politique d'acheter un nombre de licences suffisant pour permettre aux membres du personnel d'accomplir leurs tâches. Le Département des systèmes d'information contrôle l'achat et le renouvellement des licences des logiciels installés sur les équipements fournis par la Fédération. Un logiciel non standard ne peut être installé sur les ordinateurs de la Fédération que s'il est sous licence et a fait l'objet d'une autorisation. Il appartient aux utilisateurs de se procurer la documentation concernant la licence.

L'installation de tout logiciel sur un ordinateur de la Fédération doit être conforme aux politiques et procédures établies qui sont disponibles auprès du Département des systèmes d'information.

12. Mise en œuvre et procédure

La Fédération attache une grande valeur au principe de confidentialité et de respect de la vie privée et reconnaît le droit de chaque individu de protéger contre tout accès non autorisé les données stockées dans le système informatique de l'Organisation. Elle se réserve néanmoins le droit, lorsque les circonstances l'exigent, d'accéder à ces données sans que la personne concernée n'en ait été informée et/ou sans qu'elle y ait consenti.

Il s'agit notamment des cas où :

- l'accès aux données est nécessaire pour permettre d'identifier d'éventuels problèmes et vulnérabilités en matière de sécurité, de procéder à un diagnostic du système ou de préserver l'intégrité des ressources en technologies de l'information et de la communication ;
- il existe des raisons de penser qu'une infraction aux règlements, règles ou politiques de la Fédération a été commise et que l'accès aux systèmes peut permettre de collecter des informations utiles dans le cadre des investigations menées sur de possibles manquements ;
- l'accès aux systèmes d'information est nécessaire pour permettre l'accomplissement des activités essentielles de la Fédération.

L'accès aux données informatiques d'un employé sans son consentement ou sans que celui-ci en ait été informé n'est possible, à moins qu'il ne soit nécessaire pour préserver l'intégrité du système, qu'avec l'accord du responsable du Département des systèmes d'information et et/ou du responsable du Département des ressources humaines (ou leurs représentants). La Fédération se réserve également le droit de désactiver le compte d'un utilisateur ou de limiter ses droits d'accès aux ressources en technologies de l'information et de la communication.

Sanctions

Toute infraction à la présente Politique par un membre du personnel est passible de sanctions. Toute violation de la présente Politique et de toute autre politique afférente, des normes, des procédures et des règles sera sanctionnée par des mesures disciplinaires, conformément aux procédures définies dans le chapitre IX du Règlement interne ou les règles applicables au personne local le cas échéant. La violation par un sous-traitant des politiques, normes, procédures et/ou règlements peut entraîner la résiliation de son contrat avec la Fédération. En outre, la Fédération se réserve le droit de recouvrer auprès des utilisateurs toutes les dépenses engagées par elle au titre de la violation de la Politique (notamment la réparation du préjudice, les frais de rapatriement, etc.)

Politique relative à la sécurité de l'information, Fédération, décembre 2013

DÉCLARATION D'ADHÉSION

Je déclare avoir reçu, lu et compris la Politique relative à la sécurité de l'information de la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge et m'engage à en respecter les dispositions, qui font partie intégrante de mon contrat d'engagement avec la Fédération et de mes conditions de service.

Signature _____

Nom _____

Lieu _____

Date _____

Annexe : restrictions applicables selon la classification des informations[9]

La présente section contient un résumé des restrictions applicables selon le niveau de sécurité de l'information. Les procédures, normes et prescriptions en matière de technologies de l'information restent applicables à tout moment s'agissant des données électroniques[10].

Accès strictement limité

CYCLE DE VIE DE L'INFORMATION		RESTRICTIONS
Utilisation et modification	Changement de support	L'information ne peut pas être reproduite dans un autre format sauf s'il est protégé comme il se doit (par exemple, l'intégrité de la présentation de l'information doit être conservée par l'utilisation d'un format PDF non modifiable).
Diffusion	Transmission manuelle des documents	✓ Une enveloppe opaque doit être utilisée. ✓ La diffusion ne peut se faire que par le biais d'un service de livraison de courrier agréé par le propriétaire du document/des données. ✓ La remise d'un accusé de réception signé est requise.
	Transmission électronique des données	✓ La transmission des données doit être effectuée via un système de messagerie hautement sécurisé. Elle ne peut être effectuée au moyen d'un courriel standard, qu'il soit professionnel ou personnel. ✓ Les données ne peuvent être transmises qu'à des destinataires individuels (aucune liste de distribution n'est autorisée) et ne peuvent être transférées à d'autres destinataires. ✓ La remise d'un accusé de réception électronique est requise. ✓ Les informations dont l'accès est strictement limité ne peuvent pas être transmises par fax. ✓ Les imprimantes ne doivent pas être laissées sans surveillance lors de l'impression de documents dont l'accès est strictement limité. ✓ L'option d'impression sécurisée doit être utilisée pour l'impression d'informations essentielles.
	Déclarations verbales	✓ Elles doivent se dérouler à huis clos dans des lieux entièrement fermés. Sauf impossibilité, il est fortement recommandé de ne pas transmettre d'informations par téléphone. ✓ Les informations dont l'accès est strictement limité ne doivent pas être transmises par radio. ✓ Les informations doivent être effacées des équipements et/ou tableaux blancs avant de quitter une pièce.

[9] Voir les Principes de classification de l'information disponibles sur FedNet pour plus de détails
[10] Voir les procédures, normes et prescriptions en matière de technologies de l'information sur FedNet pour plus de détails.

CYCLE DE VIE DE L'INFORMATION		RESTRICTIONS
	Copie	✓ Les copies doivent se limiter à ce qui est strictement nécessaire pour les besoins opérationnels.
Sauvegarde	Sauvegarde physique	✓ Les documents doivent être conservés dans des placards ou des tiroirs verrouillés afin d'éviter tout accès non autorisé. ✓ En déplacement, les informations dont l'accès est strictement limité doivent en tout temps être conservées par le voyageur (elles ne doivent pas être placées dans les bagages).
	Sauvegarde électronique	✓ L'accès doit être réservé aux seules personnes qui le nécessitent dans l'exercice de leurs fonctions (sur la base du principe du besoin d'en connaître) ✓ Les données doivent être systématiquement sécurisées (autrement dit cryptées). ✓ Les données doivent être stockées sur un dispositif ou dans un lieu sécurisé (une clé USB cryptée) dûment protégé au moyen de restrictions d'accès. Ces données doivent être sauvegardées dans un lieu sécurisé prévoyant un niveau de sécurité identique ou supérieur et des restrictions d'accès. ✓ Les données dont l'accès est strictement limité ne peuvent pas être sauvegardées dans des lieux où la Fédération n'a aucun contrôle et qui sont susceptibles d'interception par un gouvernement (par exemple, Dropbox, Google Drive).
Sauvegarde	Supports électroniques	✓ L'accès aux sauvegardes est limité au strict nécessaire. ✓ La restauration des sauvegardes n'est autorisée que sur demande formelle et approbation du propriétaire de l'information. ✓ L'accès à la restauration des sauvegardes est réservé au propriétaire de l'information.
Destruction	Documents papier	✓ Les documents et documents de travail y relatifs qui doivent être détruits au terme de la période de conservation[11] seront déchiquetés dans les meilleurs délais et de manière sécurisée. ✓ Les documents et documents de travail y relatifs qui doivent être transmis aux archives de la Fédération au terme de la période de conservation le seront dans les meilleurs délais et de manière sécurisée.
	Supports électroniques	✓ Tous les supports électroniques doivent être détruits physiquement ou nettoyés au terme de la période de conservation. Les documents électroniques qui doivent être transmis aux archives de la Fédération au terme de la période de conservation seront imprimés puis transmis dans les meilleurs délais et de manière sécurisée. Ils doivent ensuite être détruits physiquement ou nettoyés.

[11] Voir le glossaire pour une définition de « période de conservation ».

Accès restreint

CYCLE DE VIE DE L'INFORMATION		RESTRICTIONS
Utilisation et modification	Changement de support	✓ L'information ne peut pas être reproduite sur un autre support sauf s'il est protégé comme il se doit (par exemple, l'intégrité de la présentation de l'information doit être conservée au moyen de l'utilisation d'un format PDF non modifiable).
Diffusion	Transmission manuelle des documents	✓ La transmission de documents (tels que des dossiers personnels) entre les bureaux de la Fédération (par exemple, bureau de terrain et Genève) doit être effectuée au moyen d'une enveloppe opaque par la poste ou un service de courrier.
	Transmission électronique des données	✓ La transmission électronique de données peut être effectuée par la messagerie professionnelle mais doit être protégée pour éviter des utilisateurs non autorisés puissent y avoir accès. ✓ Les données peuvent être transmises à des listes de distribution. ✓ Les messages électroniques peuvent être transférés aux destinataires qui doivent avoir connaissance de l'information. Les imprimantes ne doivent pas être laissées sans surveillance lors de l'impression de documents dont l'accès est restreint. ✓ La remise d'un accusé de réception électronique est requise.
	Déclarations verbales	✓ Elles doivent se dérouler à huis clos dans des lieux entièrement fermés. Sauf impossibilité, il est fortement recommandé de ne pas transmettre d'informations par téléphone. ✓ Les informations dont l'accès est restreint ne devraient pas être transmises par radio. ✓ Les informations doivent être effacées des équipements et/ou tableaux blancs avant de quitter une pièce.
	Copie	✓ Les copies doivent se limiter à ce qui est strictement nécessaire pour les besoins opérationnels.
Sauvegarde	Sauvegarde physique	✓ Les documents doivent être conservés dans des placards ou des tiroirs verrouillés afin d'éviter tout accès non autorisé. ✓ En déplacement, les informations dont l'accès est restreint doivent en tout temps être conservées par le voyageur (elles ne doivent pas être placées dans les bagages).
	Sauvegarde électronique	✓ L'accès doit être réservé aux seules personnes qui le nécessitent dans l'exercice de leurs fonctions (sur la base du principe du besoin d'en connaître). ✓ Les données doivent être stockées sur un dispositif ou

CYCLE DE VIE DE L'INFORMATION		RESTRICTIONS
		dans un lieu sécurisé (une clé USB cryptée) dûment protégé au moyen de restrictions d'accès. Ces données doivent être sauvegardées dans un lieu sécurisé prévoyant un niveau de sécurité identique ou supérieur et des restrictions d'accès. ✓ Les informations dont l'accès est restreint peuvent être sauvegardées en dehors des locaux de la Fédération si elle sont correctement protégées.
Sauvegarde	Électronique	✓ L'accès aux sauvegardes est limité au strict nécessaire. ✓ La restauration des sauvegardes n'est autorisée que sur demande formelle et approbation du responsable.
Destruction	Documents papier	✓ Les documents et documents de travail y relatifs qui doivent être détruits au terme de la période de conservation seront déchiquetés dans les meilleurs délais et de manière sécurisée. ✓ Les documents et documents de travail y relatifs qui doivent être transmis aux archives de la Fédération au terme de la période de conservation seront transmis dans les meilleurs délais et de manière sécurisée.
	Supports électronique	✓ Tous les supports électroniques doivent être détruits physiquement ou nettoyés au terme de la période de conservation. Les documents électroniques qui doivent être transmis aux archives de la Fédération au terme de la période de conservation seront imprimés puis transmis dans les meilleurs délais et de manière sécurisée. Ils peuvent ensuite être détruits physiquement ou nettoyés.

Accès interne

CYCLE DE VIE DE L'INFORMATION		RESTRICTIONS
Utilisation et modification	Changement de support	✓ Aucune restriction
Diffusion	Transmission manuelle des documents	✓ Aucune restriction
	Transmission électronique des données	✓ Les adresses de courrier électronique professionnel doivent être utilisées pour toute première distribution des informations internes (par exemple, @ifrc.org)[12]. ✓ L'impression ou l'envoi par fax d'informations internes ne sont soumis à aucune restriction.
	Déclarations verbales	✓ Aucune restriction
	Copie	✓ Aucune restriction
Sauvegarde	Sauvegarde physique	✓ La politique du « bureau vide » doit être appliquée en toutes circonstances, autrement dit les documents internes ne doivent pas rester sans surveillance sur les bureaux après le départ du personnel.
	Sauvegarde électronique	✓ L'accès est limité aux utilisateurs internes.
Sauvegarde	Électronique	✓ L'accès aux sauvegardes est limité au strict nécessaire.
Destruction	Documents papier	✓ Les documents et documents de travail y relatifs qui doivent être détruits au terme de la période de conservation seront déchiquetés dans les meilleurs délais et de manière sécurisée. ✓ Les documents et documents de travail y relatifs qui doivent être transmis aux archives de la Fédération au terme de la période de conservation doivent être transmis dans les meilleurs délais et de manière sécurisée.
	Supports électroniques	✓ Tous les supports électroniques doivent être détruits physiquement ou nettoyés au terme de la période de conservation. Les documents électroniques qui doivent être transmis aux archives de la Fédération au terme de la période de conservation seront imprimés puis transmis dans les meilleurs délais et de manière sécurisée. Ils peuvent ensuite être détruits physiquement ou nettoyés.

[12] Les Sociétés nationales participantes ou les Sociétés nationales hôtes intégrées à une délégation de la Fédération sont responsables de la diffusion ultérieure des informations internes.

Accès public

CYCLE DE VIE DE L'INFORMATION		RESTRICTIONS
Utilisation et modification	Changement de support	✓ Aucune restriction
Diffusion	Transmission manuelle des documents	✓ Aucune restriction
	Transmission électronique des données	✓ La transmission des informations publiques, y compris l'impression et l'envoi par fax, n'est soumise à aucune restriction.
	Déclarations verbales	✓ Aucune restriction
	Copie	✓ Aucune restriction
Sauvegarde	Sauvegarde physique	✓ Aucune restriction
	Sauvegarde électronique	✓ Aucune restriction
Sauvegarde	Électronique	✓ Aucune restriction
Destruction	Documents papier	✓ Les documents et documents de travail y relatifs qui doivent être détruits au terme de la période de conservation seront déchiquetés dans les meilleurs délais et de manière sécurisée. ✓ Les documents et documents de travail y relatifs qui doivent être transmis aux archives de la Fédération au terme de la période de conservation seront transmis dans les meilleurs délais et de manière sécurisée.
	Supports électroniques	✓ Tous les supports électroniques doivent être détruits physiquement ou nettoyés au terme de la période de conservation. Les documents électroniques qui doivent être transmis aux archives de la Fédération au terme de la période de conservation seront imprimés puis transmis dans les meilleurs délais et de manière sécurisée. Ils peuvent ensuite être détruits physiquement ou nettoyés.