Norme relative au chiffrement acceptable

1.1 Aperçu

Afin d'éviter que des renseignements de nature délicate ne soient visibles en cas de vol de supports informatiques ou d'ordinateurs, tous les renseignements, quelle qu'en soit la forme, devront être chiffrés pour en garantir la confidentialité et la sécurité et pour prévenir toute divulgation non autorisée, qu'elle soit délibérée ou accidentelle.

Ce document définit des moyens de chiffrement efficaces visant à garantir le maintien d'un niveau de sécurité approprié des ressources informationnelles du Partenariat. Le Partenariat pourrait, à sa seule discrétion, imposer des directives plus strictes en la matière.

1.2 But

Ce document a pour but de fournir un ensemble de normes minimales de chiffrement (ci-après dénommé « la norme ») devant être mis en œuvre dans le contexte des ressources informationnelles du Partenariat.

Seuls les algorithmes de chiffrement ayant fait l'objet d'un examen public approfondi et ayant prouvé leur efficacité opérationnelle figureront dans la norme.

1.3 Portée

Cette norme est obligatoire et s'applique à l'ensemble du personnel, des consultants et des sous-traitants du Partenariat qui fournissent, installent ou acquièrent les technologies de chiffrement ou rendent possible leur utilisation.

1.4 Normes

i. Les technologies de chiffrement ne pourront s'appuyer que sur des algorithmes standard éprouvés tels qu'AES, Blowfish, RSA, RC5 et IDEA, que l'on pourra utiliser, indifféremment, dans des versions commerciales ou contributives (*shareware*). Le logiciel Pretty Good

Privacy (PGP) de Network Associate utilise, par exemple, une combinaison des algorithmes IDEA et RSA-Hellman, tandis que Secure Socket Layer (SSL) s'appuie sur le chiffrement RSA.

ii. La longueur de clé des systèmes de cryptographie symétrique devra être d'au moins 128 bits, celle des systèmes de cryptographie asymétrique devant garantir une puissance équivalente. Les exigences du Partenariat en matière de longueur de clé seront revues chaque année et améliorées en fonction des évolutions technologiques.

iii. À moins qu'ils n'aient été spécifiquement examinés par des experts indépendants qualifiés et approuvés par le directeur des technologies de l'information du Partenariat, on n'aura pas recours à des algorithmes de chiffrement propriétaires. Veuillez noter que les technologies de chiffrement sont réglementées par le droit canadien et international.

1.5 Contrôle de l'application de la norme

En cas de non-respect de la norme, le Partenariat pourra, sans que cela soit limitatif, prendre les mesures suivantes :

i. Refuser l'accès à ses ressources informationnelles et de technologies de l'information.

ii. Mettre en œuvre, pour les fournisseurs indépendants, les consultants ou les sous-traitants, les recours contractuels appropriés, par exemple les dispositions relatives aux manquements au contrat ou à sa résiliation.

iii. Mettre en œuvre, pour le personnel, des mesures disciplinaires pouvant inclure, sans que cela soit limitatif, un avertissement écrit, une suspension avec ou sans traitement, la cessation immédiate de l'emploi ou des poursuites en vertu de la loi.

1.6 Définitions

Terme	Définition
Ressources informationnelles et TI	Matériel informatique (y compris les ordinateurs portatifs et de bureau), logiciels, systèmes d'exploitation, supports de stockage, comptes réseau, courrier électronique, accès Internet, portails, passerelles, appareils réseau, appareils mobiles, serveurs, téléphones et systèmes téléphoniques, imprimantes multifonctions, ordinateurs personnels et domestiques connectés au réseau du Partenariat,

	directement ou par l'entremise d'une connexion VPN, ressources informationnelles (quel que soit le support ou le format), par exemple les renseignements commerciaux ou personnels, ainsi que tout autre élément que le Partenariat pourrait considérer comme une ressource informationnelle ou TI.
AES	Advanced Encryption Standard (AES) est une norme de chiffrement à clé symétrique largement utilisée dans tout le Canada par le gouvernement fédéral et les gouvernements provinciaux, ainsi que par des fournisseurs de soins de santé. Elle comprend trois chiffrements par blocs – AES-128, AES-192 et AES-256 – adoptés à partir d'un ensemble plus important publié à l'origine sous le nom de Rijndael.
Blowfish	Blowfish est un algorithme de chiffrement à clé symétrique par blocs offrant un bon taux de chiffrement et n'ayant pu faire l'objet d'aucune cryptanalyse efficace à ce jour. Advanced Encryption Standard, qui a rencontré un succès immédiat, tend aujourd'hui à le remplacer.
RSA	Rivest, Shamir et Adleman (RSA) est un algorithme de cryptographie à clé publique. C'est le premier algorithme connu pour être adapté aussi bien à l'authentification de signatures qu'au chiffrement.
RC5	RC5 est un algorithme de chiffrement par blocs qui se distingue par sa simplicité. Conçu par Ronald Rivest, il est à l'origine de l'élaboration de l'algorithme Advanced Encryption Standard (AES), également appelé RC6.
IDEA	IDEA (International Data Encryption Algorithm) est un algorithme de chiffrement par blocs symétrique. Bien que conçu pour remplacer l'algorithme Data Encryption Standard (DES), DES a été supplanté par AES, qui a été largement adopté.

1.7 Documents connexes

- Politique de gestion de l'information
- Politique de protection des renseignements personnels

- Politique de sécurité de l'information et des technologies de l'information
- Norme relative à la sécurité de l'infrastructure TI

Fin du document