CF Morale & Welfare SERVICES

SERVICES Bien-être et moral FC

7331-0 (COO)

20 March 2018

Distribution List

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS

Reference: A-FN-105 Chapter 40

1. As part of the Payment Card Industry (PCI) Data Security Standards (DSS), CFMWS is required to provide a corporate policy and awareness training to all individuals who handle customer credit cards.

2. The current policy on credit card retention and storage (A-FN-105 Chapter 40 – Credit Card Information, Storage, and Retention) has been rescinded and replaced by a standalone corporate policy (attached).

3. Training on the importance of credit card handling shall be completed on an annual basis by all individuals who handle customer credit card information. Training has been developed and is now available on the Defence Learning Network (DLN) under the course title "NPP Credit Card Management" and must be completed annually by June of each year starting this year. Monitoring of course completion will be exercised by CFMWS divisional OPIs. A list of those

7331-0 (CO)

Le 20 mars 2018

Liste de distribution

NORME DE SÉCURITÉ DE L'INDUSTRIE DES CARTES DE PAIEMENT

Référence : A-FN-105, chapitre 40

1. Conformément à la Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS), les SBMFC sont tenus de fournir une politique organisationnelle et de donner une formation de sensibilisation sur la gestion des cartes de crédit à toutes les personnes qui manipulent des cartes de crédit de clients.

2. Le chapitre 40 du manuel A-FN-105 (Stockage et conservation de l'information relative aux cartes de crédit), qui tenait lieu de politique jusqu'à maintenant, a été annulé et remplacé par une politique organisationnelle indépendante (ci-jointe).

3. Toute personne qui traite de l'information relative aux cartes de crédit de clients doit suivre une formation annuelle portant sur les précautions nécessaires quant aux cartes de crédit. Cette formation est maintenant accessible sur le Réseau d'apprentissage de la Défense (RAD), sous la description « Cours des BNP sur la gestion des cartes de crédit ». Elle doit être réussie avant juin tous les ans, et ce, dès cette année. Les BPR des divisions des SBMFC veilleront à ce que

4210, rue Labelle Street, Ottawa, Ontario K1A 0K2
www.cfmws.com • www.sbmfc.com

Canada

that have successfully completed the DLN course will be provided to the Learning and Development committee members on a quarterly basis.

4. Should you require clarification, contact Sarah Myrer, Senior Advisor Policy and Programs, (613) 995-7186 or myrer.sarah@cfmws.com.

cette exigence soit respectée. Chaque trimestre, les membres du Comité de l'apprentissage et du perfectionnement recevront la liste des personnes ayant réussi le cours sur le RAD.

4. Si vous désirez obtenir de plus amples renseignements, veuillez communiquer avec Sarah Myrer, conseillère supérieure en matière de politiques et de programmes, au 613-995-7186 ou à myrer.sarah@sbmfc.com.

Le chef des opérations,

M.J. Ward
Chief Operating Officer

Enclosure: 1

Distribution List

Action

Base/Wing Commanders
Canadian Army Comptroller
Sr VP Commercial Services
Sr VP PSP
CFO
VP IS/CIO
VP HR
DMFS
VP Corporate Services

Information

Internal

Managing Director NPP

Pièce jointe : 1

Liste de distribution

Exécution

Commandants des bases/escadres
Contrôleur de l'Armée canadienne
VP Sup Services commerciaux
VP Sup PSP
CSF
VP SI/CSI
VP RH
DSFM
VP Services généraux

Information

Interne

Directeur général des BNP

NPP POLICY ON CREDIT CARD MANAGEMENT

POLITIQUE DES BNP SUR LA GESTION DES CARTES DE CRÉDIT

DATE OF ISSUE: 15 MARCH 2018

DATE DE PUBLICATION : 15 MARS 2018

APPLICATION

1. This policy applies to members of the CAF, employees of DND, and Staff of the Non-Public Funds, Canadian Forces who handle customer credit cards for payment on NPP purchases.

APPLICATION

1. La présente politique s'applique aux membres des Forces armées canadiennes (FAC), aux employés du ministère de la Défense nationale (MDN) et aux employés du Personnel des fonds non publics, Forces canadiennes (Personnel des FNP, FC) qui manipulent des cartes de crédit de clients utilisées pour le paiement d'achats dans le cadre d'activités des Biens non publics (BNP).

2. This policy applies to all payment channels, including in person and e-commerce. It is the responsibility of all individuals having access to credit card information to be responsible for safeguarding the information at all times. Cardholder information is to be disclosed only when there is a required business purpose.

2. La présente politique est valable pour tous les paiements, y compris ceux effectués en personne et en ligne. Il est de la responsabilité de toutes les personnes ayant accès à des renseignements de carte de crédit d'en assurer la protection en tout temps. L'information du titulaire la carte peut être divulguée seulement aux fins d'activités professionnelles.

APPROVAL AUTHORITY

3. This policy is issued under the authority the CFMWS/Chief Financial Officer.

AUTORITÉ APPROBATRICE

3. La présente politique est publiée avec l'autorisation du chef des services financiers des Services de bien-être et moral des Forces canadiennes (SBMFC).

ENQUIRIES

4. Enquiries should be directed to the Finance Division, Senior Advisor, Policy and Programs.

DEMANDES DE RENSEIGNEMENTS

4. Les demandes de renseignements doivent être adressées au conseiller supérieur en matière de politiques et de programmes de la Division des finances.

DEFINITIONS

5. Card Verification Value Code (CVV, CVV2,CVC2, or CID) - The three or four-digit value printed on the back of the card or signature strip but not encoded on the magnetic strip.

DÉFINITIONS

5. Code de vérification de la carte (CVV, CVV2, CVC2 ou CID) – Les trois ou quatre chiffres imprimés au dos de la carte ou sur la bande de signature, mais qui ne

sont pas encodés dans la bande magnétique.

6. Masked – To cover up in order to conceal.

6. Masquer – Cacher des renseignements d'un document en les couvrant.

7. Payment Card Industry Data Security Standard (PCI DSS) - PCI DSS is a comprehensive security standard that establishes common practices and precautions for handling, processing, storing, and transmitting credit card data. Visa Inc. and MasterCard Worldwide originally developed these standards; however, American Express, Discover Financial Services, and JCB International have now formally joined the PCI Security Standards Council. This global forum was launched in 2006 and is responsible for the development, management, education, and awareness of the PCI Security Standard including the development of the PCI DSS.

7. Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) – Cette norme se veut une norme de sécurité complète établissant les pratiques courantes et les précautions qui s'imposent lors de la manipulation, du traitement, du stockage et de la transmission des données relatives aux cartes de crédit. Ces normes ont d'abord été rédigées par Visa Inc. et MasterCard Worldwide. Par la suite, American Express, Discover Financial Services et JCB International se sont officiellement joints au Conseil des normes de sécurité de l'IPC. Mis sur pied en 2006, ce forum international est chargé d'établir, de gérer et de faire connaître les normes de sécurité de l'industrie des cartes de paiement, ce qui comprend le développement de la norme PCI DSS.

8. Payment Deduction Authorization (PDA) - NPP entities may allow customers or members to pay for non-CANEX NPP activities such as Golf Memberships, Support Our Troops donations, Mess Dues, invoices etc., on a monthly recurring basis. Customers have the option of choosing Military Regular Force pay deduction, Non-Public Funds (NPF) pay deduction, bank deduction, or credit card payment using the Payment Deduction Authorization form.

8. Autorisation de prélèvement – Les entités des BNP peuvent autoriser les clients ou les militaires à effectuer des paiements mensuels ou récurrents pour des activités des BNP non liées au CANEX, entre autres les frais d'adhésion à un club de golf, les dons de bienfaisance, les cotisations de mess, etc. Les clients peuvent choisir de payer par délégation de solde s'ils sont membres de la Force régulière, par retenue salariale s'ils sont employés du Personnel des FNP, FC, par prélèvements bancaires ou encore par carte de crédit, au moyen du formulaire Autorisation de prélèvement par les BNP.

9. Packet-sniffing – Act of capturing packets of data flowing across a computer network.

10. Tokenization - Tokenization is the process of replacing sensitive credit card information with unique identification symbols that retain all essential information about the data without compromising its' security.

POLICY OBJECTIVE

11. The payment card industry data security standards provide a standard approach to safeguarding sensitive data for all credit card brands. The validation system within the data security standards identifies and corrects vulnerabilities by ensuring appropriate levels of cardholder data security are maintained. It is the responsibility of all individuals who handle credit cards to ensure that this information is safeguarded at all times.

RISK OF NON-COMPLIANCE

12. Failure to comply with this policy creates the risk of theft of private credit card information, damage to CFMWS reputation, and loss in consumer confidence.

GENERAL

13. The Canadian Forces Morale and Welfare Services (CFMWS) is committed to protecting the privacy of credit card information that is held and stored within Non-Public Property (NPP) activities

9. Reniflage de paquets – Action qui consiste à intercepter des paquets de données circulant sur un réseau informatique.

10. Segmentation en unités – La segmentation en unités est une méthode qui consiste à remplacer l'information de nature délicate relative aux cartes de crédit par des symboles d'identification uniques qui préservent tous les renseignements essentiels sans compromettre leur sécurité.

OBJECTIF DE LA POLITIQUE

11. La norme PCI DSS établit une méthode normalisée permettant à l'ensemble des sociétés émettrices de cartes de crédit de protéger les données de nature délicate. Elle comprend d'ailleurs un système de validation intégré qui permet de cibler les vulnérabilités et d'y remédier tout en veillant à ce que les données du titulaire de la carte soient protégées de la manière appropriée. Il incombe à toute personne qui manipule des cartes de crédit de veiller à ce que ces renseignements soient protégés en tout temps.

RISQUES LIÉS AU NON-RESPECT DE LA POLITIQUE

12. Le non-respect de la présente politique pourrait occasionner le vol des renseignements personnels liés à une carte de crédit, une atteinte à la réputation des SBMFC et une perte de confiance de la part des clients.

GÉNÉRALITÉS

13. Les SBMFC s'engagent à protéger l'information relative aux cartes de crédit conservée en format papier ou électronique dans le cadre des activités des BNP. Selon les Ordonnances et directives de sécurité

whether it be in physical or electronic format. A secure location as defined in the National Defence Security Orders and Directives is a cabinet with a built-in hasp or security bar and secured with a Grade 3 padlock (i.e. Abloy), or a cabinet equipped with a built in Sargent & Greenleaf® dial lock. Personal Credit Card Information is considered "particularly sensitive personal information" and as such, classified as "Protected B" which means that Personal Credit Card Information must be guarded against unauthorized disclosure. As detailed at Annex A, "General Office Information Security Procedures" and Protected B "Access Criteria" are to be strictly adhered to. National Defence security policies' information/guidance sources are provided for information purposes to assist in general awareness/assessment of information security issues.

de la Défense nationale, on entend par lieu sûr un classeur doté d'un fermoir intégré ou d'une barre de sécurité et fermé par un cadenas de catégorie 3 (p. ex. Abloy), ou un classeur équipé d'une serrure à combinaison Sargent & Greenleaf®. L'information relative aux cartes de crédit est considérée comme « de l'information personnelle de nature particulièrement délicate » et doit donc porter la cote « Protégé B », ce qui signifie que les renseignements personnels relatifs à une carte de crédit doivent être protégés contre toute divulgation non autorisée. Comme il est indiqué à l'annexe A, intitulée « Procédure générale relative à la protection de l'information dans les bureaux », et comme le veut la cote « Protégé B », les « critères d'accès » doivent être rigoureusement respectés. La présente fait référence aux politiques sur la sécurité du MDN dans le but de renseigner et d'orienter le personnel sur les problèmes liés à la sécurité de l'information et d'aider celui-ci à les évaluer.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

14. As outlined below, the Payment Card Industry (PCI) has mandated data security industry standards which have been adopted by CFMWS.

15. The PCI DSS is comprised of twelve mandated security requirements:

a. Install and maintain a firewall configuration to protect data;

b. Do not use vendor-supplied defaults for system passwords

NORME DE SÉCURITÉ DES DONNÉES DE L'INDUSTRIE DES CARTES DE PAIEMENT (PCI DSS)

14. Comme mentionné dans le paragraphe suivant, l'industrie des cartes de paiement (ICP) a prescrit des normes de sécurité des données que les SBMFC ont adoptées.

15. Les douze conditions de sécurité suivantes constituent la norme PCI DSS :

a. Installer et gérer une configuration de pare-feu pour protéger les données de titulaires de carte;

b. Ne pas utiliser les mots de passe système et autres

and other security parameters;

c. Protect stored data;

d. Encrypt transmission of cardholder data and sensitive information across the public networks;

e. Use and regularly update anti-virus software;

f. Develop and maintain secure systems and applications;

g. Restrict access to data by business need-to-know;

h. Assign a unique ID to each person with computer access;

i. Restrict physical access to cardholder data;

j. Track and monitor all access to network resources and cardholder data;

k. Regularly test security systems and processes; and

l. Maintain a policy that addresses information security.

paramètres de sécurité par défaut définis par le fournisseur;

c. Protéger les données de titulaires de carte stockées;

d. Crypter la transmission des données de titulaires de carte sur les réseaux publics ouverts;

e. Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels anti-virus ou programmes

f. Développer et maintenir des systèmes et des applications sécurisés;

g. Restreindre l'accès aux données de titulaires de carte aux seuls individus qui doivent les connaître;

h. Identifier et authentifier l'accès aux composants de système;

i. Restreindre l'accès physique aux données de titulaires de carte;

j. Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaires de carte

k. Tester régulièrement les processus et les systèmes de sécurité;

l. Maintenir une politique qui porte sur les informations de sécurité pour l'ensemble du personnel.

16. These security requirements are both the responsibility of the Information Services (IS) Division and all other operational divisions. IS Division requirements include ensuring that the NPP network has the appropriate firewalls, tracking/monitoring of all access to network resources, and regular update of anti-virus software. Operational requirements include ensuring personnel are aware of the importance of properly securing credit card information.

16. Il est de la responsabilité de la Division des services d'information (DSI) et de toutes les autres divisions opérationnelles de veiller à ce que ces conditions soient respectées. La DSI doit notamment s'assurer que le réseau des BNP soit équipé des pare-feu adéquats, que l'accès aux ressources du réseau soit surveillé et que le logiciel antivirus soit mis à jour régulièrement. Parmi les exigences opérationnelles, mentionnons la nécessité que le personnel prenne conscience de l'importance de bien protéger l'information relative aux cartes de crédit.

17. This policy is especially pertinent to the protection of stored data and the restriction of physical access to cardholder data. It is acceptable to store with the appropriate protection (refer to paragraph 13), the account number, cardholder name, and expiration date only for those individuals that have a business requirement to do so. At no time is it acceptable to store the credit verification value code.

17. La présente politique revêt une importance particulière quant à la protection de l'information conservée et à la restriction de l'accès physique aux données des titulaires de carte. Si les mesures de protection appropriées sont mises en place (voir le paragraphe 13), les personnes autorisées peuvent conserver, à des fins professionnelles, le numéro de compte, le nom du titulaire de la carte ainsi que la date d'expiration de la carte. Le code de vérification de la carte de crédit ne doit être enregistré sous aucun prétexte.

18. Training has been developed and is available on the Defence Learning Network (DLN) under the course description of "NPP Policy on Credit Card Management". Training on the importance of credit card handling shall be completed on an annual basis by all individuals who handle customer credit card information.

18. Une formation est accessible sur le Réseau d'apprentissage de la Défense (RAD), sous la description « Cours des BNP sur la gestion des cartes de crédit ». Toute personne qui traite de l'information relative aux cartes de crédit de clients doit suivre une formation annuelle portant sur les précautions nécessaires quant aux cartes de crédit.

PROHIBITED CONTENT OF ELECTRONICALLY STORED DATA

INTERDICTION PAR RAPPORT AU CONTENU DES DONNÉES STOCKÉES PAR VOIE ÉLECTRONIQUE

19. At no time is it acceptable to include complete credit card information on electronically stored data, such as

19. Il est en tout temps interdit de stocker les données complètes relatives aux cartes de crédit dans un système de

Docushare. One example of where credit card information can be found is on NPP Corporate Credit Card (NPP CCC) statements. Any individual who submits their NPP CCC statement received from the Bank of Montreal (current issuer of the NPP CCC) to the local accounting office must mask the credit card number (all numbers with the exception of the last four digits (five for American Express) must be blacked out) on the supporting documentation before it is sent. The Base Card Administrator for the NPP CCC, shall also ensure that if any documents are printed that include credit card information that this information is masked out. Another example of where credit card information can be found is on NPP Pay Deduction Authorization forms. Regardless of the nature of the source document, any credit card information is to be masked prior to scanning to Docushare.

partage de données électronique, tel que DocuShare. Par exemple, on trouve de l'information relative aux cartes de crédit dans les documents portant sur les cartes de crédit des BNP (CC BNP). Toute personne qui présente son relevé de CC BNP de la Banque de Montréal, l'émetteur actuel des cartes, au bureau de la comptabilité local doit masquer le numéro de sa carte de crédit (c.-à-d., tous les numéros, sauf les quatre derniers, ou les cinq derniers dans le cas d'une carte American Express) sur les pièces justificatives avant qu'elles soient envoyées. De plus, si des documents contenant des renseignements relatifs à une carte de crédit sont imprimés, le coordonnateur des cartes de la base responsable des CC BNP doit s'assurer que ces renseignements sont masqués. Le formulaire Autorisation de prélèvement par les BNP constitue un autre exemple de document dans lequel est conservée l'information relative aux cartes de crédit. Peu importe la nature du document source, toute information relative aux cartes de crédit doit être masquée avant que le document ne soit numérisé et versé dans DocuShare.

20. At no time will credit card numbers or sensitive information be stored on the NPP network including, but not limited to, EXCEL, WORD, test files, e-mail content, etc.

20. À aucun moment les numéros de carte de crédit ou l'information de nature délicate ne peuvent être stockés sur le réseau des BNP, y compris, sans toutefois s'y limiter, dans les documents Excel ou Word, les fichiers d'essai, les courriels, etc.

DATA COLLECTED AT OUTLET LEVEL

INFORMATION RECUEILLIE DANS LES POINTS DE VENTE

21. As retail and service providers, the collection of credit card information is part of the day to day operations whether it be a CANEX outlet, SISIP Financial office, Mess operation, Base Fund activity or specialty interest operations such as a Golf Club. The key is to maintain strict

21. La collecte de l'information relative aux cartes de crédit fait partie des activités quotidiennes des fournisseurs de produits et de services, qu'il s'agisse d'un point de vente CANEX, d'une succursale de la Financière SISIP ou des activités des mess, du fonds des bases ou d'intérêt

adherence to security procedures for the collection of this data.

particulier comme un club de golf. Il est essentiel de respecter à la lettre la procédure régissant la collecte de ce type d'information.

NOTE: Outlet Managers or any other parties shall not maintain a list of credit cardholder names, numbers, and expiry dates to manually action monthly payments or for any other reason. Recurring transactions or automatic billings can be set up by the local NPP Accounting Office as described in paragraphs 24 to 26.

REMARQUE : Personne, y compris les gérants de point de vente, ne doit conserver une liste de noms de titulaires de cartes de crédit ou de numéros ou de dates d'expiration de cartes de crédit, que ce soit pour effectuer des paiements mensuels manuellement ou pour quelque raison que ce soit. Le bureau local de la comptabilité des BNP peut établir une procédure pour la facturation automatique ou les transactions récurrentes, comme il est mentionné dans les paragraphes 24 à 26.

22. Any credit card sales done on authorized Point of Sale (POS) devices will be automatically masked on the register receipt to the customer and sales slip maintained on the POS. There is no requirement to maintain the complete credit card information. To ensure the appropriate credit/debit card device is in use, all entities must ensure the device is ordered from the local NPP accounting office as per A-FN-105 Chapter 52 (Credit Card and Credit Plan Sales).

22. Lors d'une vente par carte de crédit effectuée à un terminal de point de vente (TPV) autorisé, le numéro de carte est masqué automatiquement sur le reçu remis au client ainsi que sur le bordereau conservé dans le TPV. Il n'y a aucune de raison de conserver l'information complète relative à la carte de crédit. Pour s'assurer d'utiliser le bon terminal pour cartes de crédit et débit, chaque entité doit commander ce terminal auprès du bureau local de la comptabilité des BNP, conformément au chapitre 52 (Ventes effectuées par carte de crédit et au terme du plan de crédit de CANEX) du manuel A-FN-105.

TOKENIZATION

SEGMENTATION EN UNITÉS

23. The Finance Division has developed a "tokenization" approach to replace credit card information that would be maintained within PROPHET for recurring payments. All customer credit card information will be maintained by the credit card service provider (currently Chase Merchant Services) who will not only maintain the credit card information in a secure environment but will have access

23. La Division des finances a élaboré une méthode de segmentation en unités pour remplacer par une valeur de substitution appelée « jeton » (*token*, en anglais) l'information relative aux cartes de crédit qui sera conservée dans PROPHÈTE pour les paiements récurrents. Toute information relative à la carte de crédit d'un client est conservée par le fournisseur de services de carte de crédit

to the token number to ensure the correct credit card number is processed for payments. Once the token number has been created, there is no requirement for the Non-Public Property Accounting Manager (NPPAM) to maintain the credit card information.

(Services aux commerçants Chase, à l'heure actuelle), qui assure non seulement la sauvegarde de cette information en lieu sûr, mais qui a également accès aux jetons. Ainsi, il peut veiller à ce que le montant soit imputé à la bonne carte de crédit. Une fois le jeton créé, le gestionnaire de la comptabilité des BNP (GCBNP) n'a plus de raison de conserver l'information relative à la carte de crédit.

RECURRING TRANSACTIONS/AUTOMATIC BILLINGS

TRANSACTIONS RÉCURRENTES ET FACTURATION AUTOMATIQUE

NON-PUBLIC PROPERTY PAYMENT DEDUCTION AUTHORIZATION (PDA)

AUTORISATION DE PRÉLÈVEMENT PAR LES BIENS NON PUBLICS

24. The PDA form, found at A-FN-105 Chapter 18 (Cash and Other Receipts) Annex A, shall be used for this purpose and may also be used for voluntary payments to Support Our Troops Funds.

24. Le formulaire Autorisation de prélèvement des BNP, qui figure à l'annexe A du chapitre 18 (Encaissements et autres recettes) du manuel A-FN-105, doit être utilisé pour les transactions récurrentes et la facturation automatique. Il peut également servir à recueillir les dons versés au Fonds Appuyons nos troupes.

25. Outlet Managers must ensure that credit card information is masked on any copies of the PDA maintained at the outlet level. The accounting copy will have the credit card information and if for any reason this information is required by the Outlet Manager, the Outlet Manager can request this information through their local NPP accounting office.

25. Les gérants des points de vente doivent s'assurer que l'information relative aux cartes de crédit est masquée dans chaque copie du formulaire Autorisation de prélèvement des BNP conservée sur place au point de vente. Le bureau local de la comptabilité des BNP conserve la copie renfermant l'information relative aux cartes de crédit. Si le gérant du point de vente en a besoin pour quelque raison que ce soit, il peut en faire la demande auprès du bureau local de la comptabilité des BNP.

26. If a customer has opted for monthly recurring charges, the Outlet Manager will include the completed authorized PDA form with the daily sales report (DSR) and will promptly send to the local NPP accounting office for processing in a gum

26. Si un client a choisi un paiement mensuel récurrent, le gérant du point de vente envoie immédiatement aux fins de traitement le formulaire rempli et autorisé accompagné du rapport quotidien des ventes (RQV) au bureau local de la

sealed envelope (with no security markings and properly addressed). The completed authorized PDA form will not be accepted by the local NPP accounting office if received via e-mail. At the local NPP accounting office, the PDA documentation shall remain in a secure filing cabinet with limited access until such time that the information is entered into the PROPHET accounting system and credit card service provider systems. Once the PDAs have been entered into PROPHET, the supporting document verified, the PROPHET register is posted, token number created, and credit card service provider notified of token then all credit card information is to be masked. Monthly repayment via repayment option on the PDA will be actioned based on the token number maintained within PROPHET. Credit card service provider will maintain the actual credit card number.

comptabilité des BNP dans une enveloppe scellée (adressée correctement, sans cote de sécurité). L'envoi par courriel n'est pas permis. Au bureau local de la comptabilité des BNP, le formulaire Autorisation de prélèvement par les BNP doit être rangé dans un classeur verrouillé auquel l'accès est limité jusqu'à ce que l'information puisse être versée dans le système de comptabilité PROPHÈTE et dans celui du fournisseur de services de la carte de crédit. Une fois l'information entrée dans PROPHÈTE et la pièce justificative vérifiée, les écritures sont consignées dans PROPHÈTE, un jeton est créé et le fournisseur de services de cartes de crédit en est informé. Dès lors, toute l'information relative à la carte de crédit doit être masquée. Les versements mensuels, prélevés de la manière indiquée sur le formulaire prévu à cette fin, sont effectués au moyen du jeton conservé dans PROPHÈTE. Le fournisseur de services de cartes de crédit est le seul à conserver l'information exacte relative à la carte de crédit.

PAYMENTS MADE VIA INTERNET

27. Currently, our website allows for the payment of merchandise (e.g. CANEX.ca) and donations (e.g. Support Our Troops). The payment process for these activities is the same in that the network lines are secured and no credit card information is produced within our organization. All credit card information is electronically sent to the credit card service provider for processing. Confirmation by credit card service provider report to this organization indicates payment received (full credit card is not disclosed). This report is included with the DSR and sent to the local NPP accounting office for action.

PAIEMENTS EFFECTUÉS EN LIGNE

27. Il est actuellement possible d'acheter de la marchandise (p. ex. sur le site CANEX.ca) et de faire des dons (p. ex. sur le site appuyonsnostroupes.ca) sur nos sites Web. La procédure de paiement est la même pour ces activités, car le réseau est protégé et aucune information relative aux cartes de crédit n'est conservée au sein de notre organisation. Tous les renseignements relatifs aux cartes de crédit sont transmis par voie électronique au fournisseur de services de cartes de crédit en vue d'être traités. Celui-ci nous envoie un rapport de confirmation lorsque le paiement a été reçu (le numéro complet de la carte de crédit n'est pas divulgué). Ce rapport est joint au RQV et envoyé au

28. Establishment of website payment procedures outside of these parameters puts NPP assets and our customers unnecessarily at risk and is prohibited. Information Services (IS) Procurement is the sole authority responsible for NPP purchasing, leasing, or licensing IM/IT-related goods, services, and contractors including requirements for new web pages or any modifications to existing web pages dealing with NPP business. For more information, contact ISProcurement@cfmws.com.

bureau local de la comptabilité des BNP aux fins de traitement.

28. Il est interdit d'établir une procédure de paiement en ligne qui ne respecte pas les paramètres de la présente et qui exposerait inutilement à des risques les clients et les biens des BNP. Pour ce qui est des BNP, le service d'approvisionnement de la DSI est la seule autorité habilitée à acheter ou à louer des biens ou des services liés à la technologie de l'information et à la gestion de l'information (GI/TI) ou à obtenir des services d'entrepreneurs en GI/TI, ou à attribuer ou à obtenir des licences ou permis connexes, notamment la création de pages Web ou la modification d'une page Web liée aux activités des BNP. Pour de plus amples renseignements, écrivez à ISProcurement@sbmfc.com.

MANUALLY KEY ENTERED TRANSACTIONS

TRANSACTIONS MANUELLES

GENERAL

GÉNÉRALITÉS

29. The security authentication data that helps to identify the cardholder when swiping the magnetic strip or inserting chip cards is not available when manually keyed transactions are completed. **Thus, manually keyed transactions carry a higher risk of fraud and a higher cost per transaction to the entity.** These transactions need to be minimized at all cost.

29. Une transaction effectuée manuellement ne produit pas les données d'authentification permettant d'identifier le titulaire de la carte lorsque dernier fait glisser la bande magnétique de sa carte dans le lecteur ou qu'il y insère sa carte à puce. **Les transactions manuelles exposent donc l'entité à un risque accru de fraude et à des coûts plus élevés par transaction.** Par conséquent, elles doivent à tout prix être réduites au minimum.

CUSTOMER ON-SITE MANUAL TRANSACTIONS

TRANSACTIONS MANUELLES EFFECTUÉES SUR PLACE AVEC LE CLIENT

30. When a credit/debit card device is down, best practices include the use of a manual imprinter machine to obtain an imprint of the card and, in all

30. Lorsqu'un lecteur de cartes de paiement est en panne, les meilleures pratiques doivent être mises en œuvre. Ainsi, il faut utiliser une imprimante à carte

circumstances, the outlet must ensure that the date, details of the transaction, total dollar value of the transaction (including taxes and other charges), cardholder's signature, authorization number and the merchant number are all recorded on the sales draft document. The authorization number must be obtained by calling our credit card service provider. This information must be secure at all times.

manuelle pour obtenir une impression de la carte. En toutes circonstances, l'employé du point de vente doit veiller à ce que la date, les détails, la valeur monétaire totale de la transaction (taxes et autres frais compris), la signature du titulaire, le numéro d'autorisation et le numéro du commerçant sont consignés sur le document de vente. De plus, il faut appeler la compagnie de carte de crédit pour obtenir un numéro d'autorisation. Les renseignements ainsi obtenus doivent être protégés en tout temps.

31. The sales draft document shall be distributed as follows:

a. Customer Copy – to be given to the customer;

b. Merchant Copy – to be securely stored until such time the information can be manually entered into the credit/debit card device (see paragraph 32 below for completing the transaction); and

c. Processing Copy – to be securely stored until such time the information can be manually entered into the credit/debit card device (see paragraph 32 below for completing the transaction).

31. Le document de vente est distribué comme suit :

a. Copie du client – remise au client;

b. Copie du commerçant – conservée en lieu sûr jusqu'à ce que l'on puisse entrer manuellement les données dans le lecteur de cartes de paiement (se référer au paragraphe 32 ci-dessous pour conclure la transaction);

c. Copie de traitement – conservée en lieu sûr jusqu'à ce que l'on puisse entrer manuellement les données dans le lecteur de cartes de paiement (se référer au paragraphe 32 ci-dessous pour conclure la transaction).

32. Once the credit/debit card service is available again, the data from the sales draft form will be manually entered into the credit/debit card device and the POS. In addition, the merchant and processing copies of the sales draft will be annotated "manual key entered" and the credit card information masked. The merchant and

32. Une fois le lecteur de cartes de paiement remis en marche, les renseignements du document de vente doivent être entrés manuellement dans ce dernier ainsi que dans le TPV. En outre, il faut inscrire « transaction manuelle » sur la copie du commerçant et la copie de traitement du document de vente et

processing copies will be attached to the DSR. Collection of the payment information and processing in the credit/debit card information shall be done on the same day to ensure the POS and credit/debit card device reconcile.

masquer l'information relative à la carte de crédit. Ces deux copies doivent être jointes au RQV. La collecte des renseignements relatifs au paiement et le traitement de l'information relative à la carte de crédit ou de débit doivent être effectués la même journée, de sorte que le solde du TPV et celui du terminal de carte de débit ou de crédit concordent.

REMOTE MANUAL TRANSACTIONS

33. When accepting payment over the phone, documentation used to capture the customer credit card information shall be securely stored. The data will be manually entered into the credit/debit card device and the POS. The source document used to capture the credit card information shall be shredded immediately after processing and cannot be discarded in regular garbage. Collection of the payment information and processing the credit/debit card information shall be done on the same day to ensure the POS and credit/debit card device reconcile.

TRANSACTIONS MANUELLES À DISTANCE

33. Dans le cas d'un paiement par téléphone, il faut toujours conserver en lieu sûr les documents sur lesquels sont inscrits les renseignements relatifs à la carte de crédit du client. Ces renseignements sont ensuite entrés manuellement dans le lecteur de cartes de paiement et le TPV. Après la saisie des données, le document sur lequel est transcrite l'information relative à la carte de crédit ou de débit doit être immédiatement déchiqueté; il ne doit pas être jeté avec les déchets ordinaires. La collecte des renseignements sur les paiements et le traitement de l'information relative à la carte de crédit ou de débit doivent être effectués la même journée, de sorte que le solde du TPV et celui du lecteur de cartes de paiement concordent.

NOTE: Never send unmasked credit card information by end-user messaging technologies such as e-mail, instant messaging, chat, etc., as they can be easily intercepted by packet-sniffing during delivery travel across internal and public networks. If an email is received unsolicited by a customer with credit card information, then follow the instructions at Annex B to delete from the server. No payment shall be processed from email requests. Contact customer via phone and enter credit card information directly into credit card device.

REMARQUE : Il ne faut jamais envoyer de l'information relative aux cartes de crédit non masquée par le biais de technologies de messagerie utilisées par les utilisateurs finaux, comme le courriel, la messagerie instantanée, le clavardage, etc., car cette information peut être interceptée facilement par reniflage de paquets pendant sa transmission sur les réseaux internes et publics. Si vous recevez un courriel non sollicité contenant des renseignements relatifs à la carte de crédit d'un client, vous devez suivre les indications figurant à l'annexe B afin que ceux-ci soient supprimés du serveur. Aucun paiement ne

sera traité à la suite d'une demande formulée par courriel. Dans ce cas, il faut communiquer avec le client par téléphone et saisir l'information relative à la carte de crédit directement dans le lecteur de cartes de paiement.

LOCAL NPP ACCOUNTING OFFICE RESPONSIBILITIES FOR DOCUMENTATION

34. Once the DSR with the supporting documents are received from the outlet, the information is to be stored in a secure filing cabinet/safe. Once the data has been entered into PROPHET, the supporting documents verified, and the PROPHET register is posted, token number created, and credit card service provider notified of token then credit card information is to be masked. A review of the supplier number will include the token number corresponding to the credit card. Any request pertaining to the credit card information must be submitted to the Accounting Information System support section for action.

35. Prior to scanning accounting documentation to Docushare, the NPPAM must ensure that all documentation does not include any supporting documentation that provides a complete credit card number (masking the number as per paragraph 19 above is acceptable).

RESPONSABILITÉS DU BUREAU LOCAL DE LA COMPTABILITÉ DES BNP RELATIVEMENT AUX PIÈCES JUSTIFICATIVES

34. Dès que le personnel du bureau de la comptabilité reçoit le RQV et les pièces justificatives du point de vente, il doit les ranger dans un classeur ou un coffre sécuritaire. Une fois l'information entrée dans PROPHÈTE, les pièces justificatives vérifiées, les écritures consignées dans PROPHÈTE, le jeton créé et le fournisseur de services de cartes de crédit informé de la création du jeton, l'information relative à la carte de crédit doit être masquée. Le compte de fournisseur n'affichera que le jeton qui correspond à la carte de crédit. Toute demande portant sur l'information relative à la carte de crédit doit être soumise au service de soutien du système de gestion de l'information financière.

35. Avant de numériser les documents comptables et de les verser dans DocuShare, le GCBNP doit veiller à ce que les pièces justificatives qui les accompagnent ne renferment pas d'information dévoilant un numéro de carte de crédit complet (il est acceptable de masquer le numéro conformément à la procédure indiquée au paragraphe 19).

ALL OUTLETS AND NPP ACCOUNTING MANAGER'S RESPONSIBILITIES

36. The Outlet Manager and local NPP Accounting Manager must ensure the following is adhered to if in possession of

RESPONSABILITÉS DES GÉRANTS DES POINTS DE VENTE ET DU GCBNP

36. Les gérants des points de vente et le GCBNP doivent veiller au respect des règles suivantes s'ils sont en possession

cardholder information:

a. All POS reports mask all credit card numbers;

b. DSRs with credit card information are stored securely at all times when not required;

c. If credit card information is no longer required, it must be shredded immediately and cannot be discarded in regular garbage;

d. Credit card numbers shall not be saved anywhere on the local network or on an electronic device such as USB memory stick;

e. If manual imprinters are used the carbon from these slips must be shredded immediately after processing and cannot be discarded in regular garbage;

f. All written notes with cardholder information must be treated in the same manner as above sub paragraphs a through e above;

g. If receiving information over the phone for one time payments, information needs to be stored securely at all times and then shredded immediately after processing and cannot be

d'information relative aux titulaires de cartes de crédit :

a. Il faut masquer tous les numéros de carte dans tous les rapports de TPV;

b. Il faut toujours conserver dans un lieu sûr les RQV renfermant de l'information relative aux cartes de crédit lorsque l'on ne s'en sert pas;

c. Dès que l'information n'est plus requise, il faut la déchiqueter immédiatement – il ne faut pas la jeter avec les déchets ordinaires;

d. Il ne faut pas enregistrer les numéros de carte de crédit sur un réseau local ou un dispositif électronique comme une clé USB;

e. S'il est nécessaire d'utiliser une imprimante à carte manuelle, il faut déchiqueter immédiatement le papier carbone des bordereaux après l'impression – il ne faut pas le jeter avec les déchets ordinaires;

f. Il faut traiter toute note manuscrite comportant de l'information sur les détenteurs de carte comme il est décrit aux points a. à e.;

g. Il faut conserver l'information reçue par téléphone à l'égard de paiements ponctuels dans un lieu sûr en tout temps et la déchiqueter immédiatement après le traitement – il ne faut

discarded in regular garbage; and

h. Credit card information from unsolicited e-mails are not actioned.

37. It is everyone's responsibility to ensure that credit card information regardless of medium is held at a minimum, stored securely, and disposed of properly to maintain privacy of individual's credit card information and to protect against fraud and other malicious acts.

PROTECTION OF CREDIT/DEBIT CARD DEVICES

38. Criminals are increasingly targeting POS systems as a way of stealing payment card data. One way criminals access data is by planting a "bug" that can read Personal Information Number (PIN) and cardholder information. Others have successfully used miniature cameras or video recording devices to obtain the information they are seeking. To help avoid being compromised the following should be followed on a regular basis:

a. Protect your equipment;

b. Safeguard the equipment in the POS area; and

c. Recognize and prevent equipment tampering.

pas la jeter avec les déchets ordinaires;

h. L'information relative à une carte de crédit reçue par l'entremise de courriels non sollicités ne doit pas être traitée.

37. Il incombe à chaque personne de veiller à ce que l'information relative aux cartes de crédit, peu importe le support au moyen duquel elle est transmise, soit, au minimum, entreposée en lieu sûr et détruite conformément à la procédure afin de protéger les renseignements personnels des titulaires de carte contre la fraude et d'autres actes malveillants.

PROTECTION DES DISPOSITIFS DE CARTES DE CRÉDIT ET DE DÉBIT

38. Les criminels ciblent de plus en plus les systèmes de TPV pour voler les données des cartes de paiement. Certains accèdent aux données en implantant un « dispositif d'écoute » qui peut lire les numéros d'identification personnels (NIP) et les renseignements relatifs au titulaire d'une carte. D'autres sont parvenus à utiliser des caméras ou des dispositifs d'enregistrement vidéo miniatures pour obtenir les renseignements recherchés. Pour éviter que votre équipement ne soit altéré, vous devriez suivre les recommandations suivantes de façon régulière :

a. Protégez votre équipement;

b. Protégez l'équipement dans les points de vente;

c. Sachez reconnaître et prévenir l'altération de l'équipement.

39. Further details can be found at Annex C.

REPORTING A SECURITY INCIDENT

40. In the event that you suspect a transaction data has been accessed or retrieved (tampering of machines) by any unauthorized individual/business, report the event to your manager. The National Accounting office should be notified at 1-888-748-8233 and e-mail to reconciliations@cfmws.com in addition to credit card service provider. Reporting will not only minimize risk to the payment system, but also protect customers in the most responsible and expedient manner. Systems and procedures are in place to immediately curtail the unauthorized use of compromised data, but are effective only when we fulfill our responsibility to promptly report a security incident. Any security incident (misuse of card or access to information) is to be reported to the Regional Accounting Manager (RAM) through the local NPP Accounting Manager. RAM will ensure proper chain of command is notified.

NPP NETWORK PASSWORD REQUIREMENTS

41. The IS Division has outlined specific requirements for managing and protecting network accounts. Individuals with NPP network accounts should be aware and understand the requirements. A summary of the password requirements can be found at Annex D of this document.

39. Pour obtenir de plus amples renseignements, consultez l'annexe C.

DÉCLARATION D'UNE ATTEINTE À LA SÉCURITÉ

40. Si vous croyez que des personnes ou des entreprises non autorisées ont pu accéder à des données transactionnelles ou les récupérer par suite d'une altération des dispositifs, faites part de vos soupçons à votre gestionnaire. De plus, veuillez en informer le bureau national de la comptabilité au 1-888-748-8233 et faire parvenir un courriel à reconciliations@sbmfc.com de même qu'au fournisseur de services de cartes de crédit. Dénoncer un potentiel incident aura pour effet non seulement de minimiser les risques d'altération du système de paiement, mais aussi de protéger les clients de la manière la plus responsable et adéquate qui soit. Des mesures sont en place pour restreindre immédiatement l'usage non autorisé des données compromises, mais elles ne sont efficaces que lorsque chacun assume sa responsabilité de signaler promptement une atteinte à la sécurité. Toute atteinte à la sécurité (usage abusif d'une carte ou accès non autorisé à des renseignements) doit être communiquée au gestionnaire régional de la comptabilité (GRC) par l'intermédiaire du GCBNP. Il incombe au GRC de communiquer l'information à la chaîne de commandement.

EXIGENCES RELATIVES AUX MOTS DE PASSE DU RÉSEAU DES BNP

41. La DSI a établi des exigences particulières en matière de gestion et de protection des comptes réseau. Les personnes disposant d'un compte réseau des BNP devraient connaître ces exigences et s'assurer de bien les comprendre. Un résumé des exigences

relatives aux mots de passe figure à l'annexe D de la présente.

ANNEX

Annex A – General Office – Information Security Procedures

Annex B – Permanent Deletion of Emails

Annex C – Protect your Credit/Debit Equipment

Annex D – NPP Network Password – Key Points

ANNEXES

Annexe A – Procédure générale relative à la protection de l'information dans les bureaux

Annexe B – Suppression définitive des courriels

Annexe C – Protection de l'équipement de paiement

Annexe D – Mots de passe pour accès au réseau des BNP – Éléments clés

GENERAL OFFICE - INFORMATION SECURITY PROCEDURES

1. When sensitive matter such as credit card information is removed from storage containers for working purposes, it is to be kept under constant surveillance and placed face down or covered in the presence of visitors or others who do not have a need-to-know.

2. At the end of each working day, supervisors and others responsible for the custody of sensitive matter are to ensure that a security check is made to confirm that:

   a. Classified and/or Designated (C/D) matter has been appropriately secured with particular attention being paid to desk drawers, bookcases and filing trays where such matter may have been placed and overlooked;

   b. C/D waste has been collected and secured in accordance with the highest sensitivity of matter in the waste; and

   c. Doors and windows have been secured in accordance with local procedures.

3. Forms DND 1063, Security Check Warning Card (NSN 9905-21-903- 0274) and DND 1064, Desk Top Security Check

PROCÉDURE GÉNÉRALE RELATIVE À LA PROTECTION DE L'INFORMATION DANS LES BUREAUX

1. Lorsque du matériel de nature délicate comme des renseignements de cartes de crédit est retiré des coffres de sécurité dans le cadre du travail, il doit être constamment surveillé et placé à l'envers ou couvert en présence de visiteurs ou d'autres personnes qui n'ont pas « besoin de savoir ».

2. À la fin de la journée de travail, les surveillants et les autres personnes responsables d'assurer la garde du matériel de nature délicate doivent veiller à ce qu'un contrôle de sécurité soit effectué afin de confirmer que :

   a. les documents classifiés ou désignés sont protégés correctement. Il faut porter une attention particulière aux tiroirs de bureau, aux bibliothèques et aux bacs à papier où de tels documents pourraient avoir été rangés et oubliés;

   b. les documents classifiés ou désignés jetés sont recueillis et protégés selon les normes propres aux documents portant la cote de sécurité la plus élevée;

   c. les portes et les fenêtres sont verrouillées conformément aux procédures de l'établissement.

3. La carte « Attention – Contrôle de sécurité », soit la formule DND 1063 (NNO 9905-21-903-0274) ou DND 1064

Warning Card (NSN 7530-21-903-1229) are to be displayed in a prominent position inside the entrance to areas in which sensitive matter is stored. These forms serve as a constant reminder to personnel to conduct a security check of their areas before vacating the premises, and identify the designated area security officer.

(NNO 7530-21-903-1229), doit être affichée bien à la vue à l'entrée des lieux où sont conservés des documents de nature délicate. Cette carte sert à rappeler aux membres du personnel qu'ils doivent procéder à un contrôle de sécurité de leur secteur avant de quitter les lieux et indiquer le nom du responsable de la sécurité pour ce secteur.

4. DND/CAF Security Branch personnel and appointed unit security officers will conduct periodic 'no notice' security checks during working and silent hours to ensure compliance with security regulations and the proper security protection is being afforded to sensitive assets.

4. Le personnel et les agents de la sécurité du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC) effectueront périodiquement des contrôles de sécurité sans préavis pendant et après les heures de travail afin de s'assurer que les normes en matière de sécurité sont respectées et que le matériel de nature délicate est protégé conformément aux règles de sécurité.

5. In the event of a fire, bomb threat, or other situation requiring emergency evacuation of personnel from classified or designated work areas, consideration must be given to the safety of personnel first. If time permits, sensitive matter should be secured by the quickest means possible. Under these conditions, individual files may not be secured at the proper level of protection; however, some degree of protection should be afforded to large holdings of sensitive matter.

5. Dans le cas d'un incendie, d'une alerte à la bombe ou de toute autre situation nécessitant l'évacuation d'urgence du personnel des aires de travail classifiées ou désignées, il faut veiller d'abord à la sécurité du personnel. Si le temps le permet, il faut mettre les documents de nature délicate en lieu sûr selon la méthode la plus rapide possible. Dans de telles conditions, il n'est pas toujours possible d'assurer le niveau de protection approprié pour tous les documents; toutefois, un certain degré de protection sera accordé aux recueils importants d'information de nature délicate.

6. When fire or explosion occurs in an area containing sensitive matter, the area must be guarded until a search of the damaged area can be conducted to recover exposed or damaged classified matter and such matter can be returned to a secure facility.

6. Dans le cas d'un incendie ou d'une explosion dans un secteur où de l'information de nature délicate est conservée, il faut assurer la garde du secteur jusqu'à ce qu'il soit possible de fouiller les lieux endommagés afin de récupérer les documents classifiés exposés

ou endommagés et de les ranger à nouveau dans une installation protégée.

PROTECTED B INFORMATION – PERSONAL CREDIT CARD INFORMATION

INFORMATION DÉSIGNÉE « PROTÉGÉ B » – RENSEIGNEMENTS PERSONNELS RELATIFS AUX CARTES DE CRÉDIT

ACCESS CRITERIA

CRITÈRES D'ACCÈS

7. CFMWS employees and members of DND/CAF, regardless of rank or status, shall **NOT** be afforded access to personal credit card information unless the following three **mandatory criteria** are apparent:

a. demonstration of a need-to-know. (The application of the need-to-know principle is to limit the access to information to those whose duties require such access);

b. possession of the appropriate security screening level –"Enhanced Reliability Check" (ERC) or higher; and

c. access has been authorized by the local NPP Accounting Manager, NPP Activity Manager or higher Finance authority.

7. Les employés des SBMFC et du MDN, ainsi que les membres des FAC, peu importe leur grade ou leur statut, ne doivent **PAS** avoir accès à de l'information relative aux cartes de crédit, à moins de répondre aux trois **critères obligatoires** suivants :

a. prouver leur besoin de savoir (l'application du principe du besoin de savoir sert à limiter l'accès à l'information aux personnes qui nécessitent un tel accès pour s'acquitter de leurs fonctions);

b. détenir la cote de sécurité appropriée, soit la « vérification approfondie de la fiabilité » ou un niveau supérieur;

c. avoir obtenu l'autorisation du gestionnaire de la comptabilité des Biens non publics (BNP), du gestionnaire des activités des BNP ou d'une autorité supérieure.

PERMANENT DELETION OF E-MAILS

1. From time to time you may receive unsolicited emails with customer credit card information contained within. It is against CFMWS policy to keep credit card data anywhere on NPPnet. Simply deleting it from your inbox and emptying your deleted items folder is not enough. Deleted emails remain on the server for a minimum of 10 days before being purged.

2. Follow the steps below to securely delete any emails with credit card information:

   a. delete the email from your inbox folder;

   b. delete the email from your deleted items folder; and

   c. the “Actions” section of the “Home” tab you will see “Recover deleted items from server”. Click this box. The recover deleted items box will open. Highlight the email in the list of deleted emails. Click the “purge selected items” button and click OK. This will purge the email from the server permanently.

SUPPRESSION DÉFINITIVE DES COURRIELS

1. Il est possible que vous receviez de temps à autre des courriels non sollicités qui contiennent des renseignements relatifs à la carte de crédit d’un client. Conserver de tels renseignements sur le réseau des Biens non publics (BNP) contrevient à la politique adoptée par les Services de bien-être et moral des Forces canadiennes (SBMFC). Il n’est pas suffisant de simplement supprimer ces courriels de votre boîte de réception et de vider la corbeille. En effet, les courriels supprimés restent sur le serveur pendant un minimum de 10 jours avant d’être purgés.

2. Pour supprimer un courriel contenant des renseignements relatifs à une carte de crédit de manière sécuritaire, vous devez suivre la procédure ci-dessous :

   a. Supprimez le courriel de votre boîte de réception;

   b. Supprimez le courriel de votre corbeille;

   c. Dans la section « Actions », sous l’onglet « Accueil », vous verrez le bouton « Récupérer les éléments supprimés du serveur ». Cliquez sur ce bouton. Le dossier contenant les éléments supprimés s’ouvrira. Sélectionnez le courriel désiré dans la liste des courriels supprimés. Cochez « Effacer les éléments sélectionnés » et appuyez sur « OK ». Le courriel sélectionné sera

supprimé définitivement du serveur.

3. Complete these steps **every time** you receive an email that contains credit card data.

3. Assurez-vous de suivre cette procédure **chaque fois** que vous recevez un courriel contenant des renseignements relatifs à une carte de crédit.

PROTECT YOUR CREDIT/DEBIT CARD EQUIPMENT

1. Criminals are increasingly targeting POS systems as a way of stealing payment card data. One way criminals access data is by planting a “bug” that can read PINs and cardholder information. Others have successfully used miniature cameras or video recording devices to obtain the information they are seeking. To help avoid being compromised, we recommend the following:

a. **Protect your equipment:** Inspect your devices at the beginning and end of each day for signs of tampering, confirm serial numbers and ensure there are no missing screws or no new holes have been made to the devices.

b. **Safeguard the equipment in the POS area:** To help prevent criminals swapping your equipment for their own, use secure stands, tethers and security cables; you should install your own security cameras, plus check the space for hidden cameras or unauthorized recording devices.

PROTÉGEZ VOTRE ÉQUIPEMENT DE PAIEMENT

1. Les criminels ciblent de plus en plus les systèmes de terminaux de point de vente pour voler les données des cartes de paiement. Certains accèdent aux données en implantant un « dispositif d’écoute » qui peut lire les numéros d’identification personnels (NIP) et les renseignements relatifs au titulaire d’une carte. D’autres sont parvenus à utiliser des caméras ou des dispositifs d’enregistrement vidéo miniatures pour obtenir les renseignements recherchés. Les recommandations suivantes vous aideront à prévenir les compromissions.

a. **Protégez votre équipement :** Inspectez vos appareils au début et à la fin de chaque journée pour y déceler tout signe d’altération, vérifiez les numéros de série et assurez-vous qu’aucune vis ne manque ou qu’aucun nouveau trou n’a été pratiqué sur les appareils.

b. **Protégez l’équipement dans les points de vente :** Pour éviter que les criminels ne remplacent votre équipement par le leur, utilisez des supports sécurisés, des attaches et des câbles de sécurité, installez vos propres caméras de sécurité et vérifiez les alentours pour déceler la présence de caméras dissimulées ou de dispositifs d’enregistrement non autorisés.

c. **Recognize and prevent equipment tampering:** Help employees recognize the signs of equipment tampering; validate all equipment service and repair technicians.

i. Verify the identity of any third-party person claiming to repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices;

ii. Do not install replace, or return devices without verification; and

iii. Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices.)

2. If you suspect a device has been tampered with, contact your manager immediately. The National Accounting office should be notified at 1-888-748-8233 and email to reconciliations@cfmws.com and credit card service provider.

c. **Sachez reconnaître et prévenir l'altération de l'équipement :** Aidez les employés à déceler toute tentative d'altération de l'équipement; validez tous les techniciens de l'entretien et de la réparation de l'équipement.

i. Vérifiez l'identité de toute tierce personne qui prétend faire la réparation ou l'entretien des appareils avant de l'autoriser à modifier ou à réparer ces appareils;

ii. Ne procédez pas à l'installation, au remplacement ou au retour d'appareils sans avoir fait les vérifications nécessaires au préalable;

iii. Méfiez-vous des comportements suspects à proximité des appareils (p. ex. des inconnus qui tenteraient de débrancher ou d'ouvrir les appareils).

2. Si vous croyez qu'un appareil a pu subir une altération, communiquez immédiatement avec votre gestionnaire. De plus, veuillez en informer le bureau national de la comptabilité au 1-888-748-8233 et faire parvenir un courriel à reconciliations@sbmfc.com et au fournisseur de services de carte de crédit.

3. More information can be found at: https://en.chasepaymentech.ca/credit_card_fraud_prevention_and_security.html.

3. Pour obtenir d'autres renseignements à ce sujet, visitez le site https://fr.chasepaymentech.ca/?WT.mc_id=frflag_ca.

NPP NETWORK PASSWORD – KEY POINTS

General

1. All users will be issued a unique username to allow them access to system components based on their work requirements. Group/shared usernames shall not be established for critical functions such as point of sale equipment or the NPP network access.

Mandatory Requirements

2. All passwords are on a “need to know” basis and will not be revealed to anyone unless the IT Security Officer approves it in writing.

3. An individual shall not send passwords through an un-encrypted mail or any other form of electronic communication considered unsecure.

4. If you write your password down, then the following shall be observed:

   a. Seal the password in an envelope; and

   b. Keep the envelope locked up at all times.

5. If you suspect your password has been compromised, then change your password immediately.

Minimum Requirements

6. The minimum length of a password is 10 characters and must contain at least

MOTS DE PASSE POUR L’ACCÈS AU RÉSEAU DES BNP – ÉLÉMENTS CLÉS

Généralités

1. Tous les utilisateurs reçoivent un nom d’utilisateur personnalisé qui leur permet d’accéder aux composants du système en fonction de leurs tâches. Il n’est pas recommandé de recourir à un mot de passe de groupe ou à un mot de passe partagé pour accéder à des éléments importants, comme l’équipement du point de vente ou le réseau des Biens non publics (BNP).

Exigences impératives

2. Les mots de passe sont attribués uniquement selon le principe du besoin de savoir. Ils ne doivent être révélés à personne, à moins que le responsable de la sécurité des technologies de l’information (TI) n’approuve la demande de divulgation par écrit.

3. L’envoi de mots de passe par courriel non décrypté ou par tout autre moyen de communication électronique non sécurisé est prohibé.

4. Si vous devez noter votre mot de passe, assurez-vous de respecter la procédure suivante :

   a. scellez votre mot de passe dans une enveloppe;

   b. conservez l’enveloppe sous clé en tout temps.

5. Si vous croyez que votre mot de passe a pu être falsifié, changez-le immédiatement.

Exigences minimales

6. Votre mot de passe doit contenir un minimum de 10 caractères, dont au moins

one uppercase letter, one lowercase letter, one non-alphanumeric character, and one number. A user's name shall not be part of the password.

Guiding Principles

7. A poor or weak password has the following characteristics:

a. The password is found in the dictionary;

b. Password is a common usage word such as:

i. the name of the family, pets, friends, co-workers, fantasy characters, etc;

ii. computer terms and names, commands, sites, companies, hardware, software;

iii. birthdays and other personal information such as addresses and phone numbers;

iv. Word or number patterns similar to aaabbb, 12321, etc;

v. any of the above spelled backwards; and

une lettre majuscule, une lettre minuscule, un caractère non alphanumérique et un chiffre. Le nom d'utilisateur ne devrait pas être utilisé comme mot de passe.

Principes directeurs

7. On considère la force d'un mot de passe comme étant médiocre ou faible si celui-ci :

a. se trouve dans le dictionnaire;

b. est un mot d'usage courant, par exemple :

i. un nom de famille, le nom d'un animal de compagnie, celui d'un ami, d'un collègue de travail, d'un personnage de fiction, etc.;

ii. un terme informatique, le nom d'un ordinateur, d'une commande, d'un site, d'une entreprise, d'un matériel ou d'un logiciel;

iii. une date de naissance ou un autre renseignement personnel comme une adresse ou un numéro de téléphone;

iv. les. séquences de mots ou de chiffres comme aaabbb, 12321, etc;

v. un des éléments ci-dessus épelé à l'envers;

vi. any of the above preceded or followed by a digit.

8. A strong password has the following characteristics:

a. Contain both uppercase and lowercase characters;

b. Have digits and punctuation characters as well as letters;

c. Are at least 12 characters long;

d. Do not contain a word found in a dictionary; and

e. Are not based on personal information.

vi. un des éléments ci-dessus précédé ou suivi d'un chiffre.

8. On considère la force d'un mot de passe comme étant forte si celui-ci :

a. contient des lettres majuscules et minuscules;

b. comporte des chiffres, des signes de ponctuation et des lettres;

c. comporte au moins 12 caractères;

d. ne contient pas de mots que l'on trouve dans le dictionnaire;

e. ne repose pas sur des renseignements personnels.