ASSOCIATION CANADIENNE DES PAIEMENTS

CANADIAN PAYMENTS ASSOCIATION

NORME 018

NORME DE SÉCURITÉ DE L'INFORMATION SUR LES EFFETS DE PAIEMENT

Norme 018 - Norme de sécurité de l’information sur les effets de paiement

Mise en œuvre et révisions

Mise en œuvre

Modifications

Norme 018 - Norme de sécurité de l'information sur les effets de paiement

Table des matières

Norme 018 - Norme de sécurité de l'information sur les effets de paiement

1. Introduction et portée

La présente norme énonce les exigences minimales en matière de sécurité pour le traitement des effets de paiement (« effets ») sous forme électronique et d'image de chèque, qui sont échangés, compensés ou réglés par le biais des systèmes automatisés de compensation et de règlement (SACR), en rapport avec leur confidentialité, leur intégrité, leur disponibilité et leur non-refus.

La présente Norme s'applique aux effets chaque fois que des renseignements pertinents sont utilisés par un membre ou pour son compte pour l'un ou l'autre des processus définis à l'article 4 ci-après. Par conséquent, le membre qui confie un processus quelconque à un tiers ou à un autre agent ou transmet des données doit veiller à ce que le tiers ou l'autre agent se conforme aux exigences fixées dans la présente Norme.

Cette norme s'appuie sur des sources dignes de foi pour la création, la gestion et l'examen d'une infrastructure de sécurité comme :

- Le Guide d'examen de juillet 2006 du Federal Financial Institutions Examination Council (FFIEC) intitulé « Information Security IT Examination Handbook »
- La norme ISO/IEC 27002:2013 Code de bonne pratique pour le management de la sécurité de l'information
- La norme ISO/IEC 27015:2012 Lignes directrices pour le management de la sécurité de l'information pour les services financiers
- Conseils sur l'autoévaluation en matière de cybersécurité du Bureau du surintendant des institutions financières (BSIF)

2. Définitions

Les définitions suivantes s'appliquent à la présente Norme :

2.1 « Démagnétisation » Application d'une force magnétique suffisante pour effacer toutes les données sur un support de stockage de données magnétique.

2.2 « Institution d'origine » Le membre qui fournit l'effet à un autre membre aux fins d'échange, de compensation ou de règlement.

2.3 « Principe du moindre privilège » Accorder le moins de privilèges possibles nécessaires à une action légitime, afin d'accroître la protection des données et des fonctionnalités contre les anomales et les comportements malveillants.

2.4 « Institution de réception » Le membre qui reçoit des effets d'un autre membre aux fins d'échange, de compensation et de règlement.

2.5 « Environnement protégé » Système qui met en œuvre le stockage et l'utilisation contrôlés et protégés de l'information.

2.6 « Écrasement de sécurité » Écrasement du support de stockage et de ses parties non utilisées, au moyen de données aléatoires et structurées afin de rendre pratiquement impossible la récupération des données d'origine.

2.7 « Périmètre de sécurité » Zone délimitée par l'endroit où un membre peut exercer un contrôle complet sur son matériel informatique, son matériel de réseau, ses locaux et ses images, y compris les endroits où les membres font appel à des tiers pour effectuer le traitement.

2.8 « Reprise » Retour d'un effet qui a déjà été traité.

2.9 « Transmission » Échange d'effets entre emplacements physiques (p. ex., entre emplacements d'adhérent, entre sites régionaux et centraux, entre adhérents et sous-adhérents, et entre institutions membres de l'ACP et clients.)

3. Principes de sécurité

Chaque membre qui établit ou qui est censé établir, transmettre ou échanger, ou stocker des effets doit veiller à ce que l'établissement, la transmission ou l'échange, et le stockage se fassent dans un environnement protégé et à avoir en place des contrôles et des processus suffisants pour maintenir l'intégrité, la confidentialité, le non-refus et la disponibilité de ces effets.

En particulier, les principes de sécurité suivants doivent être respectés en rapport avec le traitement des effets :

a) Moindre privilège – L'accès à l'information est fondé sur le principe du besoin de savoir en fonction de la position de l'organisation.

b) Information sur la vérification – Tous les renseignements concernant un événement de sécurité important sont conservés en vue de constituer des archives des activités pour future reddition de compte et comme preuve de décisions ou d'actions.

c) Hostilité – L'organisation et ses systèmes fonctionnent et interagissent dans un milieu hostile. Sauf indication contraire, les systèmes et les réseaux devraient être considérés comme non sécuritaires et non fiables.

d) Protection contre une menace interne et externe – Le même niveau de protection est appliqué à toutes les menaces, quelle que soit son origine (p. ex., interne ou externe).

e) Sécurité intégrée – En cas de défaillance, les systèmes doivent interdire l'accès plutôt que l'autoriser.

f) Uniformisation des fonctions de sécurité – Les membres exigent que les services critiques d'origine externe, comme le traitement des données et des opérations, les services de réseaux et la production de logiciels, soient soumis au même niveau de contrôle et de protection de l'information que les activités traitées au sein de l'institution elle-même.

g) Application implicite de la classification la plus élevée de la sensibilité des données – Si un effet, un document, un fichier ou une base de données comporte diverses classifications de sensibilité, celui-ci ou celle-ci est traité selon la classification la plus élevée de l'information qu'il renferme.

h) Séparation des tâches – Les responsabilités en matière d'établissement, de réception, de stockage, de transmission, de récupération et de suppression des effets incombent à différentes personnes.

i) Double contrôle – L'organisation doit, au minimum, assurer un double contrôle dans le traitement des effets, selon les tolérances de risque (p. ex., que le traitement des renseignements financiers ou des transactions et la vérification des résultats soient effectués par différentes personnes, ou respectivement par une personne et un processus automatisé).

j) Responsabilité – Tous les membres sont responsables de la sécurité des systèmes et réseaux d'information sous leur contrôle.

k) Intervention – Dans la mesure du possible, les membres agissent de manière opportune et coopérative en vue de prévenir et déceler les incidents de sécurité et d'y répondre.

Norme 018 - Norme de sécurité de l'information sur les effets de paiement

4. Processus

Les processus suivants sont décrits dans cette norme :

4.1 Établissement

Le processus d'établissement concerne la création d'un effet (p. ex., un effet ISO 20022 dans le format ISO 20022 est décrit dans les Lignes directrices d'utilisation TAF ISO.)

4.2 Réception

Le processus de réception concerne la récupération et le traitement d'un effet (p. ex., un effet EDI dans le format décrit dans la norme 023).

4.3 Stockage

Le stockage comporte l'enregistrement des effets sur un support pour utilisation à court terme.

4.4 Transmission

La transmission est l'échange d'effets entre lieux physiques.

4.5 Archivage

Le processus d'archivage déplace ou copie des effets dans un dépôt servant au stockage et à l'indexation à long terme des messages ou fichiers et de l'information associée à une succursale du membre ou à un centre de données. Le processus d'archivage se termine lorsqu'un effet est supprimé.

4.6 Récupération

La récupération comporte une demande de récupération d'un effet donné, à partir des archives, qui est reçue et autorisée pour traitement. La récupération se termine lorsque l'effet est récupéré et transmis au demandeur.

4.7 Suppression

Le processus de suppression correspond à l'effacement des effets. La suppression est terminée lorsqu'il n'est plus possible d'avoir accès aux effets.

4.8 Sauvegarde/Stockage amovible

Le processus de sauvegarde créée et conserve des copies des effets.

5. Exigences en matière de sécurité

Les exigences qui s'appliquent aux effets dans cet article sont regroupés sous les rubriques suivantes :

A. Contrôle d'accès logique et administratif;
B. Codes malveillants;
C. Consignation;
D. Détection des incidents et interventions;
E. Tiers;
F. Sécurité du réseau;
G. Vérification.

Norme 018 - Norme de sécurité de l'information sur les effets de paiement

Les membres doivent veiller au respect des exigences de sécurité énoncées ci-dessous à tous les sites, y compris les sites de sauvegarde et de récupération. Les membres ont cette responsabilité même lorsqu'ils confient les services à des tiers ou à un autre membre pour leur compte.

Remarque : Les références entre parenthèses qui suivent les exigences de sécurité énumérées ci-après sont fournies **à titre d'information seulement**, et pour indiquer des exigences comparables figurant dans des normes courantes de l'industrie.

A. Contrôle d'accès logique et administratif

Processus	Exigences en matière de sécurité - Contrôle d'accès logique et administratif
Généralités	i) Les effets doivent être protégés contre tout accès non autorisé et toute altération au moyen d'une politique et de mécanismes documentés de contrôle d'accès. Cette protection est assurée du point d'établissement par le membre ou de réception par l'entreprise cliente jusqu'au point de suppression. (ISO/IEC 27002:2013 9.4.1) ii) L'accès aux effets et les autorisations doivent être gérés en appliquant les principes de moindre privilège, de moindre fonctionnalité et de séparation des tâches. (ISO/IEC 27002:2013 9.1.2) iii) Les droits d'accès sont soumis à des examens réguliers (chaque année au moins). Lorsque l'accès est accordé, modifié ou révoqué, il faut le vérifier en fonction des approbations. La suppression des droits, lorsque ceux-ci ne sont plus nécessaires, est effectuée au moment opportun. (ISO/IEC 27002:2013 9.2.5) iv) L'information servant à authentifier les utilisateurs doit être assignée et contrôlée au moyen d'un processus officiel. (ISO/IEC 27002:2013 9.2.4) v) L'accès aux systèmes et applications qui traitent l'effet est contrôlé au moyen d'une procédure d'ouverture de session sécurisée. (ISO/IEC 27002:2013 9.4.2) vi) Il faut mettre en place une politique relative aux mots de passe et à l'authentification pour établir, au minimum, des contrôles des mots de passe pour les utilisateurs. (ISO/IEC 27002:2013 9.4.3) vii) Les utilisateurs suivent les pratiques utilisées par les membres pour protéger l'information servant à l'authentification. (ISO/IEC 27002:2013 9.3.1)
Établissement	i) Le logiciel employé pour établir les effets doit être protégé de tout accès non autorisé. (ISO/IEC 27002:2013 14.2.4) ii) Les activités menées par le personnel de maintenance ou de réparation à la succursale, au GAP, au centre de données ou à tout autre système utilisé pour l'établissement des effets sont autorisées et consignées selon le profil de risque de sécurité du membre. (ISO/IEC 27002:2013 15.1.1)

Norme 018 - Norme de sécurité de l'information sur les effets de paiement

Transmission	i) Toutes les transmissions d'effets se font dans un environnement sécurisé. (ISO/IEC 27002:2013 14.1.2) ii) Les renseignements liés au paiement contenus dans les effets sont protégés afin d'empêcher toute transmission incomplète, tout mauvais acheminement, toute modification non autorisée du message, toute divulgation non autorisée, toute reproduction non autorisée du message ou toute reprise non autorisée. (ISO/IEC 27002:2013 14.1.3)
Stockage	L'accès logique et physique aux appareils de stockage et aux logiciels doit être réservé aux personnes et aux logiciels autorisés et authentifiés. (ISO/IEC 27002:2013 9.1.2)
Archivage	L'accès logique et physique aux effets archivés doit être restreint aux personnes selon le principe du moindre privilège. (ISO/IEC 27002:2013 9.1.2)
Récupération	L'accès aux effets est restreint aux logiciels et au personnel autorisés et authentifiés. (ISO/IEC 27002:2013 9.1.2)
Suppression	Lorsqu'on supprime ou qu'on n'utilise plus un support (y compris les copies papier) du périmètre de sécurité de l'entité qui a pu servir à stocker des effets, les règles suivantes s'appliquent : (ISO/IEC 27002:2013 8.3.2) i) Si le support peut être réécrit, il doit être effacé par écrasement logiciel sécurisé ou faire l'objet d'une démagnétisation. Le recours à la suppression sécurisée des logiciels doit respecter les normes reconnues de l'industrie, comme les publications ITSG-06 du CST – Écrasement et déclassification des supports d'information électroniques ou NIST SP 800-88 - Guidelines for Media Sanitation; ii) Si le support ne peut être réécrit, il doit être physiquement détruit. Cela comprend l'incinération ou le déchiquetage du support de stockage de façon à rendre impossible la récupération des données d'origine.
Sauvegarde/Stockage amovible	L'accès logique et physique aux copies des effets renfermant de l'information, y compris les ordinateurs portables (p. ex., clés USB, CD/DVD, cartes mémoire, bandes, etc.) doit être protégé et limité à certaines personnes selon le *principe du moindre privilège*. Les supports amovibles et de stockage hors ligne renfermant des renseignements sur les paiements doivent être gérés en accord avec le profil de risque de sécurité du membre. (ISO/IEC 27002:2013 12.3.1)

B. Codes malveillants

Processus	Exigences en matière de sécurité - Codes malveillants
Généralités	Les systèmes servant à créer, stocker, archiver et transmettre des effets doivent être protégés contre les codes malveillants, afin d'empêcher les modifications non autorisées et les incidents de sécurité. (ISO/IEC 27002:2013 12.2.1)

Norme 018 - Norme de sécurité de l'information sur les effets de paiement

C. Consignation

Processus	Critère de sécurité - Consignation
Généralités	i) Les journaux des événements dans lesquels sont consignés les activités des utilisateurs, les exceptions, les défaillances et les événements de sécurité d'information doivent être produits, conservés et régulièrement examinés, conformément au profil de risque de sécurité du membre. (ISO/IEC 27002:2013 12.4.1) ii) Les dispositifs de consignation et les renseignements qu'ils renferment doivent être protégés contre tout accès et toute modification non autorisés. (ISO/IEC 27002:2013 12.4.2) iii) Il faut se servir d'un temps de référence pour synchroniser toutes les horloges reliées aux systèmes de traitement de l'information pertinents dans le domaine de sécurité d'un membre. (ISO/IEC 27002:2013 12.4.4)

D. Détection des incidents et interventions

Processus	Exigences en matière de sécurité - Détection des incidents et interventions
Généralités	i) Il doit y avoir des processus et procédures en place pour repérer les tentatives d'accès non autorisé ou les violations en rapport avec les systèmes utilisés pour transmettre les effets ou avec les effets eux-mêmes, et intervenir au besoin. (ISO/IEC 27002:2013 16.1.1) ii) Les événements de sécurité de l'information doivent être signalés le plus rapidement possible au moyen des procédures de gestion adéquates du membre. (ISO/IEC 27002:2013 16.1.2) iii) Il faut qu'une équipe d'intervention en cas d'incident soit en poste et habilitée à prendre des mesures officielles d'intervention afin de faire la lumière sur les événements non autorisés. (ISO/IEC 27002:2013 16.1.5) iv) Lorsqu'une violation ou toute autre défaillance des protections de sécurité d'un membre fait qu'un tiers a un accès non autorisé aux données des clients d'un autre membre, le membre victime de la violation ou de la défaillance doit en aviser l'autre membre dans les meilleurs délais possible après la constatation de cet accès non autorisé.

Norme 018 - Norme de sécurité de l'information sur les effets de paiement

E. Tiers

Processus	Exigence de sécurité – Tiers
Généralités	i) Un membre doit considérer les risques liés à la cybersécurité comme partie intégrante de son processus de diligence raisonnable pour les accords d'impartition importants et les fournisseurs de services de TI essentiels, y compris les accords de sous-traitance associés aux processus mentionnés plus haut. (BSIF 4.26) ii) Les membres doivent exiger que tous les accords d'impartition importants (y compris ceux touchant les fournisseurs de services de TI essentiels) liés aux processus mentionnés plus haut prévoient la sauvegarde de l'information sur les paiements du membre. (BSIF 4.27) iii) Un membre doit disposer des processus voulus permettant de signaler en temps opportun tout cyberincident touchant les fournisseurs de services de TI essentiels ou tout fournisseur de services avec lequel le membre a conclu un accord d'impartition important. (BSIF 4.27) iv) Il faut prendre les mesures voulues pour veiller à ce que les fournisseurs de services soient en mesure de suivre ou annuler les effets distribués dans plusieurs organisations, en cas de doute sur leur légitimité. (ISO/IEC 27015:2012 6.2.3)

F. Sécurité du réseau

Processus	Exigence de sécurité – Sécurité du réseau
Généralités	i) Il faut mettre en place des politiques, des procédures et des contrôles officiels de transfert afin de protéger la confidentialité et l'intégrité des effets transférés au moyen de tout mode de communication. (ISO/IEC 27002:2013 13.2.1) ii) Les réseaux de télécommunications doivent être contrôlés et gérés de manière à protéger l'information circulant dans tous les systèmes et toutes les applications. (ISO/IEC 27002:2013 13.1.1)
Transmission	Les renseignements figurant sur l'effet de paiement électronique doivent être protégés selon la tolérance de risque du membre. (ISO/IEC 27002:2013 13.2.3)

G. Vérification

Processus	Exigence de sécurité – Vérification
Généralités	i) Les dossiers doivent être protégés contre toute perte, toute destruction, toute falsification, tout accès non autorisé et toute émission non autorisée, conformément, au minimum, aux exigences législatives. (ISO/IEC 27002:2013 18.1.3) ii) Le membre doit veiller à ce que les exigences juridiques, réglementaires et contractuelles pertinentes soient régulièrement vérifiées en fonction de leur cadre respectif de gestion de la sécurité de l'information, dans le contexte du suivi de la conformité. (ISO/IEC 27015:2012 15.2.3)