	DOCUMENTATION ISMS	
LOTERIE ROMANDE	**Type de document :** Directive	**Propriétaire : Responsable Sécurité**
	Classification : Interne	

ISMS_173_MAITRISE DES DONNEES ECHANGEES VERS L'EXTERIEUR_V3.0.DOCX

Rôles & Responsabilités dans le cadre de ce document

Responsable	Responsable Sécurité
Auditeurs	Auditeurs
Participants	DOSI-Secteur Projets & Développements, Spécialiste des Systèmes de Tirages
Informés	DOSI Secteur Infrastructures informatiques
Demandeur	Responsable Sécurité
Ecrivain, éditeur	Responsable Sécurité

Table des matières

1 Sommaire à l'intention du lecteur

1.1 Description et objectifs du document

- Ce document décrit les mesures de protection des données échangées entre la LoRo et les tiers par des interfaces électroniques. Il s'agit avant tout des échanges de fichiers entre la LoRo et ses partenaires (par exemple PMC, IGS, TI Info, Swisslos,…).
- Il a pour objectif de traiter les risques suivants relatifs aux échanges de données :
  - Interception et reproduction,
  - Modification des données (fichiers corrompus, introduction de malware)
  - Non remise des données au destinataire (Erreurs d'acheminement, Destruction;)

1.2 Périmètre d'application

Font partie du périmètre d'application :

- Les données échangées entre la LoRo et les tiers par des interfaces électroniques.

Ne font pas partie du périmètre :

- Les emails envoyés par les collaborateurs et les fichiers échangés via l'application files.loro.ch sont traités dans la politique ISMS #27 d'utilisation des systèmes d'information et des biens de l'organisation.

1.3 Association avec la norme ISO 27001

Cette directive supporte l'ensemble des éléments de gestion et de traitement des risques requis par la norme ISO 27001 suivants :

A.13.2.1 Politiques et procédures de transfert de l'information

A.13.2.2 Accords en matière de transfert d'information

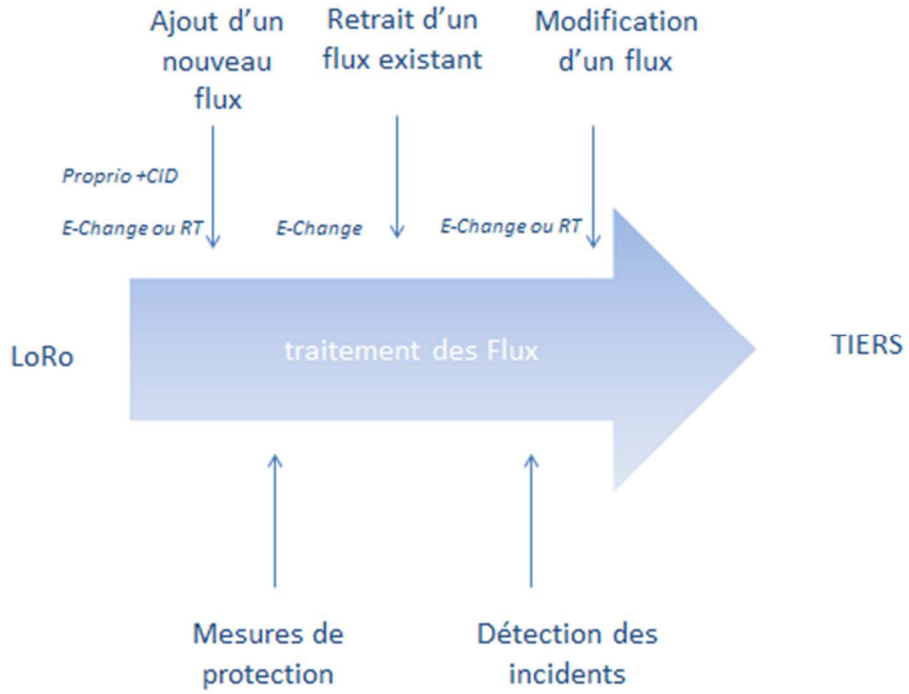
2 Directive

2.1 Principes

- Les données échangées avec l'extérieur correspondent à un actif de la LoRo avec une classification CID (Confidentialité, intégrité, Disponibilité) et un propriétaire (se référer au registre des actifs de la LoRo)
- Toute transmission de données à un tiers doit être autorisée par leur propriétaire.
- Les échanges de données avec l'extérieur doivent être revus chaque année par leur propriétaire.
- Les flux de données doivent être gérés de préférence avec les outils prescrits dans le document « Bonnes pratiques » de l'ADI.

- La transmission de données à l'étranger doit donner lieu à une procédure spéciale du fait du changement de législation applicable.

2.2 Cycle de vie des flux de données



Ajout d'un nouveau flux :

- La création d'un nouveau flux est suivie via la procédure de gestion du changement ou via la création d'un ticket Request Tracker lié à un eChange existant.
- Il convient de prendre en compte les implications commerciales, légales et en termes de sécurité liées à l'échange de données électroniques, au commerce électronique et aux communications électroniques, ainsi que les exigences en matière de contrôles.
- Les chefs de projets qui mettent en place des nouveaux flux doivent informer l'ADI des nouveaux flux.
- L'ADI inventorie les flux et les données associées. Les flux de données qui dépassent le périmètre de la LoRo doivent être signalés en tant que tel.
- Le responsable de la demande de changement analyse les flux liés au changement, et détermine le propriétaire et la valeur des données échangées en matière de sécurité puis propose les mesures en conséquence.

Modification d'un flux :

- La modification d'un flux est suivie via la procédure de gestion du changement ou via la création d'un ticket Request Tracker.

Retraits de flux :

- Les flux qui ne sont plus nécessaires aux activités de la LoRo doivent être identifiés. Pour cela,
    - Les propriétaires de flux reconfirment leurs flux de manière annuelle.
    - L'ADI effectue une surveillance des flux pour lesquels aucun transfert dans Control-M n'a été effectué pendant une période donnée.
- Le retrait d'un flux obéit à la procédure de gestion du changement.

2.3 Mesures de protection préventives

Chiffrage :

- D'une façon générale, les flux de données doivent être protégés en conformité avec la directive ISMS 47 d'utilisation des mesures cryptographiques (par exemple SSH ou SFTP) lorsque l'information est transportée de ou vers l'extérieur.
- Les fichiers classés « Secret » doivent être chiffrés (par exemple PGP) avant leur transfert. Ces fichiers sont désignés comme tels dans l'inventaire des transferts.
- Les exceptions doivent être documentées et être autorisées par la Direction

Protection de l'intégrité

- Les fichiers dont les exigences de protection de l'intégrité sont élevées font l'objet d'un contrôle à l'aide d'un Checksum. Ces fichiers sont désignés comme tels dans l'inventaire des transferts.

Protection de la disponibilité

- Des mesures de contingences doivent être mises en place pour garantir la disponibilité des flux liés aux processus critiques en matière de disponibilité.

Protection de l'administration des flux :

- Les accès aux serveurs Control-M et aux serveurs FTP associés doivent être maîtrisés (Autorisations et contrôles réguliers)
- Lorsque les flux ne sont pas gérés via Control-M, les accès aux serveurs d'échange de fichiers doivent être protégés.

2.4 Mesures de détection et de traitement des incidents

Détection :

- Les transferts de données effectués via Control-M doivent être surveillés par la LoRo.

- Les logs des fichiers transférés par Control-M doivent être conservés à des fins d'analyse pendant une durée cohérente avec la directive ISMS 142 de conservation des documents et informations de la Loterie Romande.
- Pour les flux de tirage Euro Millions, le bon fonctionnement des échanges de fichiers doit être surveillé via des quittances.

Traitement :

- La gestion des incidents lors des échanges avec l'extérieur est conforme à a procédure ISMS #133 de gestion des incidents DOSI.
- Des procédures d'exception doivent prévoir les cas d'anomalie.
- En cas de détection de flux non maîtrisé, le DOSI a la possibilité de couper les flux.

2.5 Inventaire des transferts

Un inventaire des transferts effectués par Control-M est maintenu par l'ADI. Cet inventaire contient au moins les informations suivantes :

- Nom du fichier à la source et à la destination s'il change pendant le transfert
- Le nom du serveur source
- Le nom du serveur de destination
- L'indication « Checksum » si l'intégrité du fichier fait l'objet d'un contrôle
- L'indication « Chiffrement » si le contenu du fichier doit être chiffré

L'inventaire est accessible à l'ADI et aux Opérateurs en lecture seule. La modification de l'inventaire est réservée à l'équipe Control-M.

3 Documentation complémentaire

Les documents complémentaires suivants viennent appuyer cette directive :

- Registre ISMS 172 des actifs
- Procédure ISMS 133 de Gestion des incidents DOSI
- Directive ISMS 47 d'utilisation des mesures cryptographiques
- Directive ISMS 142 de conservation des documents et informations de la Loterie Romande

4 Points de contrôle

- eChanges et tickets Request Tracker qui ponctuent les cycles de vie des flux de données échangés avec les tiers
- Journaux d'accès aux serveurs FTP associés à Control-M