Politique de la

Sécurité des Systèmes

d'Information

Exemple Label Cyber-Safe

Avertissement : le présent document est fourni dans le cadre de la labellisation Cyber-Safe et nécessite d'être adapté à votre situation. Son usage ne garantit pas la conformité aux exigences du Label.

1 Introduction

L'objet de ce document est de définir la Politique de Sécurité de l'Information du Label Cyber-Safe.

1.1 Définition

La Sécurité de l'Information est la protection des informations d'un ensemble de menaces, pour assurer la continuité des affaires, réduire au minimum les risques et maximiser le retour sur investissement et les opportunités d'affaires.

Système de Management de la Sécurité de l'Information (SMSI) : Partie de l'ensemble du système de gestion, basée sur une approche en termes de risques d'affaire, permettant d'établir, de mettre en œuvre, de faire fonctionner, de contrôler, de réviser, de maintenir et d'améliorer la sécurité de l'information.

1.2 Périmètre et application

La présente politique s'applique à tous les utilisateurs. L'utilisation des outils informatiques par un utilisateur constitue en soi une acceptation tacite de la politique.

Il incombe aux responsables, en coopération avec la direction du Label Cyber-Safe, de veiller au respect de cette politique et de prendre les mesures nécessaires pour la faire appliquer.

1.3 Objectifs

La présente politique a pour but de clarifier la stratégie de l'organisation Label Cyber-Safe en matière de Sécurité des Systèmes d'Information.

- S'assurer que les informations appropriées et les actifs critiques sont protégés des menaces.
- S'assurer qu'en cas d'erreur du système ou de toute menace, toutes les informations appropriées et les actifs critiques gardent un niveau satisfaisant de confidentialité, d'intégrité et de disponibilité, déterminé par la direction.
- S'assurer qu'en cas d'erreur, catastrophe ou tout autre problème qui peut menacer le Label Cyber-Safe, ses opérations commerciales continuent à opérer avec un niveau de gêne minimum.
- Créer une culture de sécurité impliquant les employés.

2 Politique

2.1 Contrôle des accès

Toute l'information critique du Label Cyber-Safe doit être protégée de toutes les menaces, qu'elles soient internes ou externes, délibérées ou accidentelles. L'information critique comprend mais n'est pas limitée à :

- Les données stockées sur les ordinateurs et serveurs
- L'information imprimée ou écrite sur papier
- Les échanges à travers les réseaux, par email ou envoyée par fax
- Les données stockées sur des supports amovibles
- Les informations orales issue de conversations et d'appel téléphonique ou tout autre moyen de communication à distance

Un contrôle d'accès adéquat doit être mis en place et l'information doit être protégée contre les accès non autorisés.

Toute autorisation d'accès à l'information donnée à une personne doit être définie et approuvée par le responsable de cette personne.

2.2 Disponibilité, Intégrité et Confidentialité

L'information et les services vitaux doivent être disponibles aux utilisateurs autorisés quand et où ils en ont besoin avec un niveau d'interruption le plus faible possible.

L'intégrité de l'information doit être maintenue et assurée pour que l'information ne puisse subir aucune altération ou destruction de façon erronée ou sans autorisation, et ce afin d'être considéré exacte et complète lors de son utilisation.

La confidentialité de l'information doit être assurée. Les données des communications humaines ou électroniques doivent être protégées afin d'assurer que l'information de valeur ou sensible est protégée des divulgations non autorisées.

2.3 Cadre réglementaire

L'organisation doit être en conformité avec toutes les exigences réglementaires ou légales relatives à la sécurité de l'information et à la protection des données afin d'éviter toute amende ou coût financier causé par la non-conformité à ces exigences.

2.4 Sensibilisation et documentation

Label Cyber-Safe doit sensibiliser ses employés à l'importance de la sécurité de l'information à travers la mise en place d'un programme de sensibilisation continue et assurer la mise à disposition et la participation aux formations nécessaires.

Toutes les politiques, les procédures et les directives qui constituent le SMSI doivent être disponibles pour les personnes autorisées, sous format papier ou électronique à travers un système de réseau interne (intranet), afin de supporter la politique de Sécurité des Systèmes d'Information.

2.5 Management des incidents

Les brèches de sécurité réelles ou suspectées doivent être étudiées et rapportées aux autorités compétentes.

Un cadre de gestion de la continuité des affaires doit être fourni à travers un plan de continuité des affaires afin de contrecarrer les interruptions d'activités et de protéger les processus d'affaires critiques en cas d'erreur ou de désastre. Le plan de continuité des affaires doit être maintenu, testé et révisé afin d'être efficace en cas d'évènement pouvant causer des dommages au Label Cyber-Safe.

2.6 Rôles et responsabilité

Toute l'équipe de management de cyber-safe.ch est responsable de mettre en œuvre la Politique de Sécurité des Systèmes d'Information dans leur service.

Chaque membre du personnel a la responsabilité d'adhérer à la PSSI.

En cas de problème lié à la Sécurité de l'Information, la situation doit être évaluée avec la personne Responsable de la gestion de la Sécurité des Système d'Information. Ce dernier est responsable de définir les mesures de remédiation et d'informer la direction.

Lieu et date :

Signature de la direction :