http://www.ja-psi.fr

La politique de sécurité informatique

JA-PSI Jérôme ATHIAS Consultant sécurité des systèmes d'information

La politique de sécurité informatique

« L'information s'impose comme un capital des plus précieux pour l'Organisation .»

Le système d'information, constituer de moyens informatiques, est essentiel à l'activité de l'organisation.
L'utilisation inappropriée du SI, ou son mal fonctionnement peuvent menacer l'existence de l'organisation.

En analysant et définissant les risques, l'on peut construire une politique de sécurité du SI, définissant le cadre d'utilisation des moyens informatiques.

But de la politique de sécurité

La politique de sécurité informatique fixe les principes visant à garantir la protection des ressources informatiques et de télécommunications en tenant compte des intérêts de l'organisation et de la protection des utilisateurs.

Les ressources informatiques et de télécommunications doivent être protégées afin de garantir **confidentialité**, **intégrité** et **disponibilité** des informations qu'elles traitent, dans le respect de la législation en vigueur.

Périmètre et domaine d'application

La politique de sécurité informatique s'applique à toute personne utilisant les ressources informatiques et de télécommunications de l'organisation.

L'utilisation des ressources informatiques et de télécommunications est étendue au matériel personnel connecté au réseau informatique, dans la mesure où une telle connexion aura été dument autorisée.

Utilisation des ressources informatiques et accès utilisateurs

Les ressources informatiques et de télécommunications sont destinées à un usage strictement professionnel. L'autorisation éventuelle de leur utilisation à des fins personnelles est définie dans les règles de procédures spécifiques à chacune des ressources telles que la messagerie électronique, internet, la téléphonie, etc dans la mesure où elle n'est pas déjà autorisée par le droit en vigueur.

Les ressources informatiques et de télécommunications autorisées sont définies de manière exhaustive par l'organe compétent désigné.
Toute utilisation ou accès aux ressources informatiques et de télécommunications sont soumis à autorisation préalable et explicite. L'autorisation est strictement personnelle, liée à la fonction et intransmissible. Pour des raisons de sécurité ou d'exploitation, celle-ci peut être suspendue ou révoquée selon la procédure spécifiquement édictée à cette fin.

Toute utilisation d'une information doit respecter la confidentialité de cette dernière, en se conférant aux lois, règlement ou directives internes en vigueur.

Contrôles

Autant que possible, des dispositifs de prévention sont mis en place pour éviter les utilisations abusives des ressources informatiques et de télécommunications.

Les contrôles destinés à assurer le bon usage de ces ressources devront être effectués dans le respect des règles de la protection de la vie privée.

Mesures en cas de violation

La violation volontaire ou par négligence grave des règles issues de la présente politique de sécurité peut entrainer la prise par le service compétent, de mesures technologiques et organisationnelles permettant d'éviter la répétition de la violation. Sauf cas d'urgence, la personne concernée, ou son répondant est préalablement entendue.

Communication

La politique de sécurité informatique de l'organisation, ainsi que les règles et procédures qui en découlent sont communiquées à l'ensemble du personnel , et font partie intégrante du statut du personnel (règlement intérieur), ainsi qu'aux intervenants extérieurs avant leur première intervention.

Rôles et responsabilités

- L'organe compétent édicte les règles et procédures relatives à l'utilisation des différentes ressources informatiques et de télécommunications nécessaires à la concrétisation de la présente politique de sécurité informatique.
- Les responsables de chaque service sont responsables du bon respect, par les utilisateurs, de la politique de sécurité informatique, ainsi que des règles et procédures de sécurité.
- L'organe compétent en la matière vérifie la bonne application des règles et procédures.
- Les utilisateurs doivent assurer la confidentialité, intégrité et disponibilité des ressources informatiques qu'ils utilisent.