

## **Prestations spéciales: politique en matière de sécurité de l'information**

La sécurité de l'information revêt une grande importance pour le domaine Prestations spéciales et fait partie intégrante de la stratégie et des objectifs commerciaux, raison pour laquelle un système de gestion de la sécurité de l'information (SGSI) est exploité conformément à la norme ISO 27001. Les rôles et les compétences sont définis en conséquence.

### **Responsabilité**

La sécurité de l'information est l'affaire de tous: à tous les niveaux, les collaborateurs sont formés et encouragés à prendre conscience de leur responsabilité en matière de sécurité de l'information. Le domaine Prestations spéciales s'engage à utiliser la meilleure technologie disponible tout en tenant compte des possibilités économiques. Le respect de toutes les exigences (légal, administratives et des clients) va de soi. En outre, le domaine Prestations spéciales s'engage à améliorer la sécurité de l'information en permanence.

La direction soutient les activités en lien avec la sécurité de l'information en fournissant les ressources nécessaires. Elle vérifie en outre le respect des règles et prend les mesures qui s'imposent en cas d'écarts.

Le responsable de la sécurité de l'information (CISO – *Chief Information Security Officer*) est responsable du SGSI, le surveille, l'améliore, met en œuvre les objectifs définis et établit un rapport correspondant à l'intention de la direction.

À tous les niveaux, les collaborateurs sont tenus de respecter la sécurité de l'information. Ils sont soutenus et formés par leurs supérieurs hiérarchiques.

Les collaborateurs externes sont tenus de respecter la sécurité de l'information dans le champ d'application des prestations qu'ils fournissent. Ils sont soutenus et formés par le mandant interne.

### **Objectifs**

Le domaine Prestations spéciales a défini les objectifs suivants dans le domaine de la sécurité de l'information:

- mise en place et développement de sa propre organisation en matière de sécurité;
- formation sur le comportement conforme aux règles de sécurité à adopter sur le lieu de travail;
- protection contre les attaques provenant d'Internet, les logiciels malveillants et autres parasites;
- possibilité de travailler en toute sécurité (travail mobile et télétravail);
- autorisations limitées au rôle des collaborateurs et des administrateurs;
- réduction des dommages causés par de potentiels incidents;
- respect des directives et des dispositions relatives à la protection et à la sécurité des données (confidentialité, disponibilité, intégrité et traçabilité);
- respect des lois et des exigences contractuelles.

## **Système de gestion de la sécurité de l'information (SGSI)**

Le domaine Prestations spéciales exploite un SGSI, l'objectif étant de promouvoir de manière ciblée la sécurité de l'information et d'améliorer les performances de l'entreprise en continu. Le SGSI fait partie intégrante du QMS. Les processus et les procédures sont définis de manière à ce que la sécurité de l'information soit garantie.

Le système complet, y compris les prestations de tiers, fait l'objet d'audits réguliers. Si un objectif n'est pas respecté ou atteint, le système est corrigé pour obtenir un changement durable de la culture et des méthodes de travail au sein de l'entreprise, ce qui garantit également une amélioration continue pour l'avenir et crée une valeur ajoutée durable pour l'entreprise.

### **Tiers**

La sécurité de l'information est un critère essentiel lorsque le domaine Prestations spéciales collabore avec des tiers ou sélectionne ses fournisseurs; ceux-ci doivent en effet appliquer les directives du domaine Prestations spéciales. Des règles contractuelles sont établies à cet effet. Le domaine Prestations spéciales se réserve le droit de les auditer à tout moment et sans préavis.

### **Violations**

Les violations des dispositions relatives à la sécurité de l'information ne sont pas tolérées et sont sanctionnées. Les tiers risquent des mesures pénales et les collaborateurs des sanctions.