BOWDEN

Politique de sécurité des systèmes d’information.

Auteur : Kévin GUILLEMINOT
Date : 23/02/2026
Version : 1.0
Classification : Publique

1. Objectif :

Bowden S.A.S est un fournisseur de premier rang de systèmes et d'assemblages mécaniques. Nous concevons, développons et fabriquons une gamme de produits que nous fournissons aux constructeurs automobiles.

Dans un environnement industriel exigeant, notre Politique de Sécurité des Systèmes d'Information (PSSI) matérialise notre engagement à protéger nos données et celles qui nous sont confiées afin de répondre aux exigences de nos clients et partenaires.

2. Engagement de la Direction

La Direction générale s'engage à :

- Mettre en œuvre une gouvernance sécurité via un Comité de pilotage constitué des instances dirigeantes et des directions métiers.
- Mettre à disposition les ressources humaines, techniques et financières nécessaires à la mise en œuvre de la politique de sécurité.
- Favoriser la culture de la sécurité auprès de l'ensemble du personnel et apporter son appui pour la mise en œuvre de la Politique de Sécurité.
- Respecter les exigences légales, contractuelles et réglementaires applicables à notre domaine d'activité, incluant les attentes spécifiques de nos clients.
- Prendre connaissance des risques et des incidents liés à la sécurité des informations de manière régulière.
- Prendre part à la démarche d'amélioration continue, notamment en prenant en compte les retours d'expérience, les audits, les incidents de sécurité, les demandes des clients ainsi que les évolutions technologiques.

3. Objectifs de sécurité :

- Disponibilité : Les données doivent être accessibles aux utilisateurs à tout moment.
- Intégrité : Les données n'ont pas été modifiées à l'insu de leur propriétaire.
- Confidentialité : Seules les personnes autorisées ont accès aux données qui leur sont réservées.
- Traçabilité : Assurer la responsabilité et la preuve des actions sur les systèmes d'information afin de détecter, analyser et démontrer tout événement de sécurité.

4. Champ d'application :

La Politique de Sécurité de l'Information couvre l'ensemble des activités, processus, systèmes d'informations, sites et personnels impliqués dans la conception ou la production de données internes ou liées à nos clients. Cela inclus les systèmes d'information, sur le site de BOWDEN, sur les sites partenaire ou hébergés ainsi que les services d'infrastructure, matériels et les logiciels utilisés pour leur mise en œuvre.
La PSSI concerne également tous les acteurs internes, externes, partenaires ou prestataires qui ont accès à n'importe lequel des services d'informations détenus par l'entreprise.

5. Rôles et Responsabilités :

Le pilotage du Systèmes de Management de la Sécurité de l'Information (SMSI) est assuré par :

- Le Responsable Sécurité : Anime le Systèmes de Management de la Sécurité de l'Information, définit les règles de sécurité, surveille les risques et sensibilise le personnel.
- Le Comité de sécurité : Composé des instances dirigeantes de l'entreprise, il supervise la mise en place du SMSI, valide les actions de protection, fournit les ressources nécessaires et suit les incidents. Et vérifie la cohérence des mesures mises en œuvre avec les orientations stratégiques de l'entreprise.
- Chaque utilisateur est responsable des données qu'il traite.
- Chaque prestataire ou partenaire est responsable de la sécurité des données auxquelles il accède.

6. Principes directeurs

6.1. Organisation et Politique de sécurité de l'information.

Ce principe insiste sur la nécessité d'une direction claire, de politiques établies et d'un processus d'apprentissage, d'amélioration continue pour faire face à l'évolution constante des menaces.

6.2. Ressources humaines.

Il est crucial d'assurer une sensibilisation régulière, C'est en faisant de chacun un acteur de la sécurité que l'on renforce les défenses.

6.3. Sécurité physique.

Protéger en permanence les personnes, les locaux, les équipements et les informations contre l'accès non autorisé, la dégradation ou la perte.

6.4. Identités et accès.

Ce principe est au cœur de la maîtrise des systèmes et des données. Il s'agit de garantir que seules les personnes et entités autorisées peuvent interagir avec les informations et les infrastructures critiques.

6.5. Sécurité informatique.

Ce principe couvre la manière dont les systèmes fonctionnent, les données sont traitées et les services sont délivrés et qu'ils intègrent des contrôles de sécurité tout au long de leur cycle de vie.

6.6. Fournisseurs.

La protection de l'information dépend aussi de la solidité des partenaires externes. Il est vital de s'assurer que les fournisseurs ou partenaires partagent notre engagement et nos standards de sécurité.

6.7. Conformité.

S’assurer que l’entreprise respecte toutes les exigences légales, réglementaires, contractuelles et internes liées à la sécurité de l’information.

7. Signalement

L’adresse signalement-securite@bowden.fr est disponible afin de signaler tout incident de sécurité. Ou en interne auprès du service informatique.