Corrigé Activité P1C5

La démarche initiale de l'équipe consistant à collecter des numéros de sécurité sociale ou à stocker inutilement des cartes de crédit entières expose TechNova à des risques immenses et évitables. Plus vous possédez de données critiques, plus la surface d'attaque s'élargit et plus les conséquences légales d'une faille cryptographique s'alourdissent.

Pour imposer un cadre de protection sécurisé dès la conception, vous devez rédiger et faire appliquer la directive de gestion de la donnée sensible suivante :

"Le système ne DOIT collecter et stocker que les données strictement nécessaires au fonctionnement du métier. Les données superflues, telles que les numéros de sécurité sociale, doivent être retirées du modèle de données. Toute donnée conservée et classifiée comme sensible (ex : données financières, mots de passe, historiques privés) doit être systématiquement chiffrée au repos à l'aide d'algorithmes modernes et standards de l'industrie."

N'inventez jamais votre propre algorithme de chiffrement (une pratique connue sous le nom de Custom Crypto). La cryptographie est une science mathématique extrêmement complexe. Seuls les algorithmes ouverts, standards et longuement éprouvés par la communauté internationale de la cybersécurité (comme AES-256 pour le chiffrement ou Argon2 pour les mots de passe) doivent être validés et utilisés dans le code de TechNova.