Liste des contrôles de conformités

Botium Toys

☐ La Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)

La réglementation FERC-NERC s’applique aux entreprises du secteur de l'électricité ou impliquées dans le réseau électrique aux Etats-Unis et en Amérique du Nord. Les entreprises ont l’obligation de se préparer, d’atténuer et de signaler tout incident de sécurité potentiel susceptible d’avoir un impact négatif sur le réseau électrique. Les entreprises sont légalement tenues d’adhérer aux normes de fiabilité relatives à la protection des infrastructures critiques (CIP) définies par le FERC.

Explication : Non applicable

☑ Règlement général sur la protection des données (RGPD)

Le RGPD est un règlement européen sur les données, qui encadre le traitement des données des citoyens de l’Union Européenne (UE) et leur droit à la confidentialité au sein et hors de l’U.E. Par ailleurs, si une violation se produit et que les données d’un citoyen de l’UE sont compromises, celui-ci doit être informé dans les 72 heures suivant l’incident.

Explication : Botium Toys doit adhérer au RGPD parce qu’elle exerce des activités commerciales et collecte des informations personnelles auprès de personnes du monde entier, y compris l’Union Européenne.

☑ Norme de sécurité de l’industrie des cartes de paiement (PCI-DSS)

La PCI DSS est une norme de sécurité internationale visant à garantir que les entreprises qui stockent, acceptent, traitent et transmettent des informations relatives aux cartes de crédit le fassent au sein d’un environnement sécurisé.

Explication : Botium Toys doit adhérer au PCI DSS parce qu'elle stocke, accepte, traite et transmet des informations relatives aux cartes de crédit en personne et en ligne.

☐ Le Health Insurance Portability and Accountability Act (HIPAA)

L'HIPAA est une loi fédérale établie en 1996 pour protéger les informations de santé des patients américains. Cette loi interdit le partage d'informations sur les patients sans leur consentement. Les entreprises ont l'obligation légale d'informer les patients d'une violation.

Explication : Non applicable

☑ Contrôle des systèmes et des organisations (System and Organization Controls, SOC type 1, SOC type 2)

Les rapports SOC1 et SOC2 portent sur les politiques d'accès des utilisateurs à différents niveaux de l'entreprise. Ils sont utilisés pour évaluer la conformité financière et les niveaux de risque des entreprises. Ils couvrent également la confidentialité, le respect de la vie privée, l'intégrité, la disponibilité, la sécurité et la sûreté de l'ensemble des données. Les défaillances de contrôle dans ces domaines peuvent conduire à des fraudes.

Explication : Botium Toys doit établir et appliquer un accès utilisateur approprié pour le personnel interne et externe (fournisseur tiers) afin d'atténuer les risques et de garantir la sécurité des données.