RPM International Inc.

Feuille de route de signalement des incidents de données

Alerté d'un incident

Prenez des mesures immédiates d'atténuation et **informez le service informatique local**. Limiter la communication écrite, opérer sur la base du besoin de savoir et éviter d'utiliser des termes juridiques définis comme « violation ». **Le service informatique local doit informer le directeur de RPM d'Info Sec .**

Où se trouve le point d'accès ?

Identifiez la cause profonde ou le point d'accès initial**. Regrouper le service informatique avec le directeur Info Sec de RPM pour isoler et atténuer l'incident.**

Des systèmes critiques ont-ils été affectés ?

Le service informatique déterminera la gravité de l'impact. **Le directeur d'Info Sec de RPM informera le directeur juridique de RPM et le directeur financier de RPM.** Le GC et le CFO détermineront si/quand alerter le RPM BoD.

Opérations, relations ou finances affectées ?

Si oui, déterminez lesquels, comment ils ont été affectés et le **directeur de Info Sec pour informer le vice-président des opérations de RPM et le vice-président de la société. Gestion des avantages et des risques.** VP Corp. Les prestations détermineront si/quand alerter l'assureur.

Des obligations légales de signalement ?

Cela est déterminé par le service juridique et de conformité de RPM en collaboration avec un conseiller externe en matière de confidentialité et de sécurité des données. **Ne signalez pas un incident en externe sans consulter le service juridique de RPM.**

Événement à signaler dans un fichier (RE)

Les RE doivent être déposés **immédiatement** après avoir pris connaissance de l'incident lié aux données. **Le directeur de RPM Info Sec et l'équipe de protection des données sont notifiés via l'événement à signaler.**

Quelles sont les données impliquées ?

Le directeur de RPM Info Sec informera le conseiller juridique du groupe concerné. Inclure les avocats internes de l'UE/du Royaume-Uni si des données provenant d'Europe sont impliquées. Les données sensibles augmenteront tout impact potentiel.

Des systèmes financiers ont-ils été affectés ?

Si oui, le service informatique doit identifier la portée de l'impact. **Le directeur d'Info Sec doit informer les auditeurs internes de RPM**. L'audit interne déterminera si/quand alerter les auditeurs externes.

Y a-t-il des dommages potentiels à la réputation ?

Si oui, le service informatique en collaboration avec l'entreprise détermine l'étendue des dommages et **informe l'équipe de communication de RPM.**

L'incident était-il important ?

Le service juridique de RPM déterminera l'importance, les rapports appropriés, les communiqués de presse et autres communications nécessaires.

Ne faites pas de commentaires externes sur un incident sans approbation préalable.