

Une fiche d'information pour identifier les documents à détruire

Les violations de données coûtent des millions aux entreprises.

IBM a indiqué que le coût total moyen d'une violation de données en 2022 s'élevait à 4,35 millions de dollars.

Il est donc essentiel de détruire les informations confidentielles en toute sécurité. Toutefois, il n'est pas toujours évident de déterminer quels documents doivent être détruits en toute sécurité.

Exemples d'informations confidentielles à détruire



Documents confidentiels:

- ✓ Dossiers financiers
- ✓ Enregistrements de données client
- ✓ Documents juridiques
- ✓ Dossiers des employés
- ✓ Informations exclusives
- ✓ Propriété intellectuelle

Média:

- ✓ Disques durs
- ✓ Supports optiques
- ✓ Clés USB

Cartes:

- ✓ Cartes d'identité
- ✓ Badges d'identification des employés

✓ Clés

✓ Bancaires

Uniformes portant la marque de l'entreprise

Le processus de destruction

Shred-it utilise les mêmes procédures de traçabilité pour la destruction des supports spécifiques que pour la destruction des documents ou des disques durs. Vous avez ainsi la garantie que vos supports sont détruits de manière fiable et sécurisée avec:

- ▶ Une programmation facile et à la demande de votre service.
- ▶ Représentants à la clientèle certifiés et experts en sécurité de l'information.
- ▶ Traçabilité assurée grâce à un système d'enregistrement et de code-barres à chaque étape du processus.
- ▶ Certificat de destruction Shred-it remis après chaque service.

Cliquez ici pour en savoir plus sur nos services sécurisés de déchiquetage de documents et de destruction de disques durs. | shredit.fr

Nous protégeons ce qui compte

