Déclaration de sécurité

Cette déclaration de sécurité vise à vous fournir plus de renseignements sur notre infrastructure et nos pratiques de sécurité. Notre politique de confidentialité contient plus de renseignements sur la façon dont nous traitons les données que nous recueillons.

Politique de sécurité des renseignements

Cision maintient une politique écrite de sécurité des renseignements qui définit les responsabilités de l'employé et l'utilisation acceptable des ressources du système de renseignements. L'organisation reçoit un accusé de réception signé des utilisateurs indiquant qu'ils ont lu, compris et accepté de respecter les règles de comportement, avant de fournir un accès autorisé aux systèmes de renseignements Cision. Cette politique est périodiquement révisée et mise à jour au besoin.

Nos politiques de sécurité couvrent un large éventail de sujets liés à la sécurité, allant des normes générales auxquelles chaque employé doit se conformer, telles que les comptes, les données et la sécurité physique, aux normes de sécurité plus spécialisées couvrant les applications internes et les systèmes de renseignements.

Sécurité organisationnelle

Les rôles et les responsabilités en matière de sécurité de renseignements sont définis au sein de l'organisation. L'équipe de sécurité se concentre sur la sécurité des renseignements, la vérification de sécurité mondiale et la conformité, ainsi que sur la définition des contrôles de sécurité pour la protection de l'infrastructure matérielle de Cision. L'équipe de sécurité reçoit régulièrement des avis de sécurité du système de renseignements et distribue régulièrement des alertes de sécurité et des renseignements consultatifs à l'organisation après avoir évalué le risque et l'impact, le cas échéant.

Cision suit le cadre de cybersécurité du NIST avec des contrôles de sécurité en couches pour aider à déceler, prévenir, détecter des incidents de sécurité et y répondre. Le responsable de la sécurité de renseignements est également responsable du suivi des incidents, des évaluations de la vulnérabilité, de l'atténuation des menaces et de la gestion des risques.

Gestion des actifs

Les actifs du système de données et de renseignements de Cision sont composés des actifs des clients et des utilisateurs finaux ainsi que des actifs de l'entreprise. Ces types d'actifs sont gérés en vertu de nos politiques et procédures de sécurité. Le personnel autorisé de Cision qui gère ces actifs est tenu de se conformer aux procédures et directives définies par les politiques de sécurité de Cision.

Sécurité du personnel

Les employés de Cision sont tenus de se conduire d'une manière conforme aux directives de l'entreprise, y compris celles concernant la confidentialité, l'éthique commerciale, l'utilisation appropriée et les normes professionnelles. Tous les employés nouvellement embauchés sont tenus de signer des ententes de confidentialité et de reconnaître la politique du code de conduite de Cision. Le code décrit l'attente de l'entreprise que chaque employé mènera ses activités légalement, éthiquement, avec intégrité et dans le respect des autres et des utilisateurs, partenaires et concurrents de l'entreprise. Des processus et des procédures sont en place pour traiter les employés qui sont embauchés ou qui quittent l'entreprise.

Les employés reçoivent une formation sur la sécurité dans le cadre de l'orientation sur les nouveaux employés. De plus, chaque employé de Cision est tenu de lire, de comprendre et de suivre un cours de formation sur le code de conduite de l'entreprise.

Sécurité physique et environnementale

Cision dispose de politiques, de procédures et d'infrastructures pour gérer à la fois la sécurité physique de ses centres de données ainsi que l'environnement à partir duquel les centres de données opèrent.

Nos systèmes de renseignements et notre infrastructure sont hébergés dans des centres de données de classe mondiale qui sont géographiquement dispersés pour fournir une haute disponibilité et redondance à Cision et à ses clients. Les contrôles de sécurité physique normalisés mis en œuvre dans chaque centre de données comprennent des systèmes de contrôle d'accès par carte électronique, des systèmes d'alarme incendie et d'extinction, des caméras intérieures et extérieures et des gardes de sécurité. L'accès physique est géré de manière centralisée et strictement contrôlé par le personnel du centre de données. Tous les visiteurs et les sous-traitants sont tenus de présenter une pièce d'identité, sont tenus de se connecter et d'être escortés par le personnel autorisé à travers le centre de données.

L’accès aux zones où les systèmes, ou les composants du système, sont installés ou stockés sont séparés des bureaux généraux et des zones publiques. Les caméras et les alarmes pour chacune de ces zones sont surveillées centralement 24 heures sur 24, 7 jours sur 7 pour toute activité suspecte, et les installations sont régulièrement patrouillées par des gardes de sécurité. Les serveurs ont des blocs d’alimentation internes et externes redondants. Les centres de données ont des alimentations de secours et peuvent tirer l’énergie des générateurs diesel et des batteries de secours. Ces centres de données ont effectué une vérification de type II des contrôles de l’organisation des services (SOC) 2.

Sécurité opérationnelle

Gestion du changement

Cision maintient un processus de gestion du changement pour s’assurer que toutes les modifications apportées à l’environnement de production sont appliquées de manière délibérée. Les modifications apportées aux systèmes d’information, aux périphériques réseau et à d’autres composants du système, ainsi que les modifications physiques et environnementales sont surveillées et contrôlées au moyen d’un processus officiel de contrôle des modifications. Les changements sont examinés, approuvés, mis à l’essai et surveillés après la mise en œuvre pour s’assurer que les changements prévus fonctionnent comme prévu.

Relations avec les fournisseurs

Cision aime s’associer avec des fournisseurs qui opèrent avec les mêmes valeurs ou des valeurs similaires en matière de légalité, d’éthique et d’intégrité que Cision. Dans le cadre de son processus d’évaluation, nous examinons nos fournisseurs et les lions à des obligations de confidentialité et de sécurité appropriées, en particulier s’ils gèrent les données des clients.

Notre service d'approvisionnement peut effectuer des vérifications de temps à autre sur les fournisseurs de Cision dans le but d'assurer la confidentialité, l'intégrité et la disponibilité des données que nos fournisseurs tiers peuvent traiter.

Vérification et journalisation

Nous tenons des journaux de vérification sur les systèmes. Ces journaux fournissent un compte rendu du personnel qui a accédé à quels systèmes. L'accès à notre outil de vérification et d'enregistrement est contrôlé en limitant l'accès aux personnes autorisées. Les incidents de sécurité sont enregistrés, surveillés et traités par des membres de l'équipe de sécurité formés. Les composants réseau, les postes de travail, les applications et tous les outils de surveillance sont activés pour surveiller l'activité des utilisateurs.

Les responsabilités organisationnelles en matière d'intervention en cas d'événement sont définies. Les incidents de sécurité enregistrent des modifications de configuration système critiques et les administrateurs sont alertés au moment de la modification. Les calendriers de conservation pour les différents journaux sont définis dans nos directives de contrôle de sécurité.

Protection antivirus et contre les logiciels malveillants

L'antivirus et la protection contre les logiciels malveillants sont gérés de manière centralisée et configurés de manière à récupérer les signatures et définitions mises à jour existantes. Les stratégies de protection contre les logiciels malveillants appliquent automatiquement les mises à jour à ces mécanismes de protection. Les outils antivirus sont configurés pour exécuter des analyses, la détection de virus, l'activité d'écriture de fichiers en temps réel et les mises à jour des fichiers de signatures. Les utilisateurs d'ordinateurs portables et distants sont couverts par la protection contre les virus.

Sauvegardes du système

Cision a des normes et des directives de sauvegarde et des procédures associées pour effectuer la sauvegarde et la restauration des données de manière planifiée et en temps opportun. Des contrôles sont établis pour aider à protéger les données sauvegardées (sur place et hors site). Nous veillons également à ce que les données des clients soient transférées ou transportées en toute sécurité vers et depuis des sites de sauvegarde. Des tests périodiques sont effectués pour vérifier si les données peuvent être récupérées en toute sécurité à partir d'un dispositif de sauvegarde.

Sécurité du réseau

Nos serveurs d'infrastructure résident derrière des pare-feu de haute disponibilité et sont surveillés pour la détection et la prévention de diverses menaces à la sécurité du réseau. Les pare-feu sont utilisés pour aider à restreindre l'accès aux systèmes à partir de réseaux externes et entre les systèmes internes. Par défaut, tous les accès sont refusés et seuls les ports et protocoles explicitement autorisés sont autorisés en fonction des besoins de l'entreprise.

Cision maintient des environnements de développement et de production distincts. Nos pare-feu de nouvelle génération (NGFW) fournissent une segmentation adéquate du réseau grâce à la mise en place de zones de sécurité qui contrôlent le flux de trafic réseau. Ces flux de trafic sont définis par des stratégies de sécurité de pare-feu strictes.

Des outils automatisés sont déployés au sein du réseau pour prendre en charge l'analyse en temps quasi réel des événements afin de prendre en charge la détection des attaques au niveau du système. Les pare-feu de nouvelle génération déployés dans le centre de données ainsi que dans les sites de bureau distants surveillent les communications sortantes pour les activités inhabituelles ou non autorisées, ce qui peut être un indicateur de la présence de logiciels malveillants (par exemple, code malveillant, logiciels espions, logiciels publicitaires).

Protection des données

Cision travaille continuellement à développer des produits qui prennent en charge les dernières suites et protocoles de chiffrement sécurisés recommandés pour crypter le trafic pendant le transport. Nous surveillons de près l'évolution du paysage cryptographique et travaillons à la mise à niveau de nos produits pour répondre aux nouvelles faiblesses cryptographiques à mesure qu'elles sont découvertes et mettons en œuvre les meilleures pratiques à mesure qu'elles évoluent. Pour le chiffrement en transit, nous le faisons tout en équilibrant le besoin de compatibilité pour les clients plus anciens.

Gestion des vulnérabilités

Des évaluations de sécurité sont effectuées pour déceler les vulnérabilités et déterminer l'efficacité du programme de gestion des correctifs. Chaque vulnérabilité est examinée pour déterminer si elle est applicable, classée en fonction du risque et attribuée à l'équipe appropriée pour correction.

Gestion des correctifs

Cision s'efforce d'appliquer les derniers correctifs et mises à jour de sécurité aux systèmes d'exploitation, aux applications et à l'infrastructure réseau afin d'atténuer l'exposition aux vulnérabilités. Des processus de gestion des correctifs sont en place pour implémenter des mises à jour de correctifs de sécurité au fur et à mesure qu'elles sont publiées par les fournisseurs. Les correctifs sont testés avant d'être déployés en production.

Connexions réseau sécurisées

Le chiffrement HTTPS est configuré pour l'accès aux applications Web client. Cela permet de s'assurer que les données utilisateur en transit sont sûres, sécurisées et disponibles uniquement pour les destinataires prévus. Le niveau de chiffrement est négocié avec le chiffrage SSL ou TLS et dépend de ce que le navigateur Web peut prendre en charge.

Contrôles d’accès

Accès à base de rôles

Des contrôles d’accès à base de rôles sont mis en œuvre pour les systèmes d’accès aux renseignements. Des méthodes et des procédures sont en place pour traiter les cas de licenciement volontaire ou involontaire des employés. Les contrôles d’accès aux données sensibles dans nos bases de données, systèmes et environnements sont définis sur la base du besoin de savoir/du principe du minimum de connaissances nécessaires. Les listes de contrôle d’accès définissent le comportement de tout utilisateur au sein de nos systèmes d’information, et les politiques de sécurité les limitent aux comportements autorisés.

Authentification et autorisation

Nous exigeons que les utilisateurs autorisés soient approvisionnés avec des identifiants de compte uniques. Notre politique de mot de passe couvre tous les systèmes de renseignements, applications et bases de données applicables. Nos politiques de mot de passe imposent l’utilisation de mots de passe complexes, qui sont déployés pour protéger contre l’utilisation non autorisée de mots de passe.

Les employés de Cision bénéficient d’un ensemble limité d’autorisations par défaut pour accéder aux ressources de l’entreprise, telles que leur messagerie et l’intranet de l’entreprise. Les employés ont accès à certaines ressources supplémentaires selon leur fonction spécifique. Les demandes d’accès supplémentaire suivent un processus formel qui implique une demande et une approbation d’un propriétaire de données ou de système, d’un gestionnaire ou d’autres cadres, tels que définis par nos directives de sécurité. Les approbations sont gérées par des outils de flux de travail qui tiennent à jour les enregistrements de vérification des modifications.

Cycle de vie du développement logiciel

Nous suivons une méthodologie définie pour développer un logiciel sécurisé conçu pour augmenter la résilience et la fiabilité de nos produits. Nos produits sont déployés sur un cycle de vie de développement itératif et rapide. La sécurité et les tests de sécurité sont mis en œuvre tout au long de la méthodologie de développement des logiciels. L'assurance de la qualité est impliquée à chaque phase du cycle de vie et les meilleures pratiques de sécurité sont un aspect obligatoire de toutes les activités de développement.

Notre cycle de vie de développement sécurisé suit les pratiques de sécurité normalisées, y compris les tests de vulnérabilité, les tests de régression, les tests de pénétration et les évaluations de la sécurité des produits. Les équipes d'architecture de Cision examinent régulièrement notre méthodologie de développement afin d'intégrer l'évolution de la sensibilisation à la sécurité, des pratiques de l'industrie et de mesurer son efficacité.

Gestion des incidents

Cision dispose d'un plan officiel d'intervention en cas d'incident (plan d'intervention en cas d'incident) et de procédures connexes en cas d'incident de sécurité des renseignements. Le plan d'intervention en cas d'incident définit les responsabilités du personnel clé et définit les processus et les procédures de notification. Le personnel d'intervention en cas d'incident est formé et l'exécution du plan d'intervention en cas d'incident est mise à l'essai périodiquement.

Une équipe d'intervention en cas d'incident est chargée de fournir une capacité de traitement des incidents de sécurité qui comprend la préparation, la détection et l'analyse, le confinement, l'éradication et le rétablissement.

Continuité des activités et reprise après sinistre

Pour minimiser les interruptions de service dues à une défaillance matérielle, à une catastrophe naturelle ou à une autre catastrophe, nous mettons en œuvre un programme de reprise après sinistre dans tous nos centres de données. Ce programme comprend plusieurs composantes afin de minimiser le risque d'un point de défaillance unique. Pour les applications stratégique pour l'entreprise, les données d'application sont répliquées sur plusieurs systèmes au sein du centre de données et, dans certains cas, répliquées vers des centres de données secondaires ou de sauvegarde qui sont géographiquement dispersés pour fournir une redondance adéquate et une haute disponibilité. Les connexions haute vitesse entre nos centres de données aident à prendre en charge le basculement rapide.

Protection des données

Nous appliquons un ensemble commun de principes de gestion des données personnelles aux données des clients que nous pouvons traiter et stocker. Nous protégeons les données personnelles à l'aide de mesures de sécurité physiques, techniques et organisationnelles appropriées. Toute information non publique que Cision peut traiter ou stocker est chiffrée au repos. Les éditeurs qui peuvent avoir accès à ces renseignements utilisent des postes de travail spécialement renforcés, y compris l'utilisation d'un logiciel de liste blanche qui permet uniquement l'utilisation d'applications approuvées.

Nous accordons une attention et un soin supplémentaires aux données personnelles sensibles et respectons les lois et coutumes locales, le cas échéant.

Cision ne traite les renseignements personnels que d'une manière compatible et pertinente aux fins pour lesquelles ils ont été recueillis ou autorisés conformément à notre politique de confidentialité. Nous prenons toutes les mesures raisonnables pour protéger les renseignements que nous recevons de nos utilisateurs contre la perte, l'utilisation abusive ou l'accès non autorisé, la divulgation, l'altération et/ou la destruction.

Préoccupations relatives à la protection de la vie privée :

privacy@cision.com