COMMENT PUBLICIS COLLABORE

SÉCURITÉ *DE L'INFORMATION*

POURQUOI ?

Au sein de Publicis Groupe, la protection des informations que nous détenons, tant pour nous-mêmes que pour nos clients, est de **la responsabilité de chacun**. Un programme formel de sécurité de l'information a été mis en place pour répondre aux exigences de sécurité de Publicis Groupe et de ses clients.

POUR QUI ?

La Politique de sécurité informatique de Publicis Groupe s'applique à tous les employés, intérimaires, stagiaires et autres collaborateurs de Publicis Groupe, de ses agences, Business Units et SSC, ainsi qu'aux tiers autorisés (prestataires indépendants, entrepreneurs, consultants, fournisseurs, etc.) collectivement appelés les « Personnes » dans ce document. Publicis Groupe et ses agences (y compris les Business Units et SSC) sont collectivement appelés « Groupe » dans ce document.

QUOI ?

Le Groupe a adopté les principes et objectifs suivants pour assurer et promouvoir la sécurité :

Principes de sécurité

1. Respect des droits et intérêts légitimes d'autrui (utilisation éthique de la sécurité).
2. Transparence dans la réalisation des objectifs de sécurité.
3. Proportionnalité des contrôles de sécurité aux risques évalués ou perçus.
4. Propriété et responsabilité des informations et des systèmes d'information.
5. Excellence au travers de la collaboration et l'intégration des métiers.
6. Collaboration entre métier et les parties prenantes externes.
7. Sensibilisation et promotion de la sécurité.

Objectifs de sécurité

1. Protéger les informations nécessaires au fonctionnement de l'entreprise et à l'atteinte de nos buts et objectifs stratégiques.
2. Protéger les informations que nos clients nous confient et répondre à leurs exigences de sécurité.
3. Respecter les lois, règlements et exigences contractuelles applicables.
4. Maintenir les risques de sécurité à des niveaux acceptables.

Cadre de sécurité

Publicis Groupe a adopté la norme de sécurité de l'information ISO 27001, reconnue par l'industrie, comme base de référence sur laquelle le programme de sécurité global a été construit. Certains secteurs d'activité critiques sont officiellement certifiés ISO 27 001 et subissent des audits internes et externes périodiques.

COMMENT ?

Global Security Office (GSO)

Une organisation dédiée à la sécurité, le « Global Security Office » (également appelé GSO), est chargée de mettre en œuvre la charte du programme. Cette organisation est composée de plus de 100 professionnels de la sécurité qui détiennent des certifications reconnues dans le secteur, telles que CISSP, CISM, CISA, etc. Le GSO est une organisation de services partagés commune à toutes les agences de Publicis Groupe dans le monde et est présent dans toutes les régions géographiques, à savoir les Amériques, l'Europe et l'Asie-Pacifique. La vision, la mission et les services du GSO sont les suivants :

Vision

Créer un avantage concurrentiel pour Publicis Groupe en promouvant de manière transparente la sécurité par la collaboration.

Mission

- Faire du GSO un expert en la matière, non seulement au sein du Groupe, mais aussi dans le secteur de la sécurité de l'information.
- Travailler en partenariat avec les agences, les clients et les autres parties prenantes afin de bien comprendre leurs besoins, leurs attentes et leurs priorités en matière de sécurité.
- Simplifier la manière dont les agences et les équipes interagissent avec le GSO.
- Collaborer et diffuser la sensibilisation à la sécurité à tout moment.

Services

Le GSO fournit les services suivants aux Business Units de Publicis Groupe afin de mettre en œuvre la charte du programme de sécurité de l'information du Groupe :

- Gestion du cycle de vie de la politique de sécurité de l'information.
- Formation et sensibilisation à la sécurité.
- Adoption, mise en œuvre et certifications des normes de sécurité (par ex., ISO 27001).
- Soutien aux exigences de sécurité des clients.
- Adoption, mise en œuvre et certifications du plan de continuité des activités (par ex., ISO 22301).
- Gestion des risques de sécurité, y compris les risques liés aux tiers.
- Tests de sécurité, par ex. analyse de vulnérabilité, tests de pénétration, etc.
- Examen et orientation de l'architecture de sécurité.
- Gestion des incidents de sécurité.
- Opérations de sécurité.

Le Groupe dispose également d'un **Security Operations Center (SOC) dédié, fonctionnant 24 heures sur 24 et 7 jours sur 7**, sous l'égide de l'organisation informatique, qui analyse les incidents de sécurité pour détecter tout impact négatif potentiel sur le réseau ou l'infrastructure du Groupe.

Le GSO travaille en étroite collaboration avec le Global Data Privacy Office (GDPO) et le département Juridique du Groupe afin de comprendre et de respecter les exigences légales, contractuelles et réglementaires du monde entier en matière de protection des données. Grâce à l'étroit partenariat entre le GSO et le GDPO, Publicis Groupe est bien préparé à répondre aux exigences réglementaires telles que le règlement général européen sur la protection des données (RGPD) ou la loi californienne sur la protection des consommateurs (CCPA).

Gouvernance de la sécurité

Le GSO dispose d'un leadership fort qui rend compte à la direction du Groupe. L'équipe est dirigée par le bureau du CISO (Chief Information Technology Security Officer) et rend compte directement au Chief Executive Officer de Re:Sources, l'organisation de services partagés de Publicis Groupe. La sécurité de l'information est supervisée par les dirigeants de Publicis Groupe, c'est-à-dire la Secrétaire Générale, membre du Directoire, et le Chief Executive Officer des Plateformes Partagées, membre du Management Committeee, qui donnent une orientation stratégique au programme de sécurité de l'information et contrôlent également son efficacité.
Des rapports exécutifs sur la santé globale du programme de sécurité de l'information et sa maturité sont fournis chaque trimestre par le GSO au Comité stratégique et des risques du Conseil de surveillance.

Politiques de sécurité

Publicis Groupe suit un modèle multicouche pour la mise en œuvre de la sécurité qui consiste en une combinaison de contrôles de sécurité administratifs, physiques et techniques reconnus par l'industrie, également appelés « mesures techniques et organisationnelles » au niveau de l'organisation, du système et du réseau.

Au niveau le plus élevé de ce dispositif se trouvent les politiques de sécurité de l'information élaborées d'afin d'aligner le Groupe sur le cadre ISO 27001 reconnu par l'industrie. Ces politiques de sécurité donnent une orientation et un socle à la direction pour les objectifs de sécurité de l'information. Elles définissent également les normes minimales qui doivent être respectées pour maintenir et améliorer la sécurité de l'information chez Publicis Groupe. Le présent paragraphe donne une vue d'ensemble de tous les documents relatifs à la politique de sécurité de l'information qui sont à la disposition de tous les employés et qui sont régulièrement mis à jour pour répondre aux exigences commerciales en constante évolution.

La violation de toute politique de sécurité constitue une violation de Janus. Les conséquences d'une violation confirmée peuvent inclure des mesures disciplinaires pouvant aller jusqu'à un licenciement, ainsi que des actions civiles ou pénales, ou des poursuites judiciaires pour chaque infraction.

Programme de sensibilisation à la sécurité

Le programme de sensibilisation à la sécurité du Groupe a été développé pour conscientiser les employés sur l'importance de ce sujet et pour minimiser les risques de cybersécurité pour le Groupe. Chaque employé est tenu de suivre annuellement la formation obligatoire de sensibilisation à la sécurité dans le cadre de l'engagement de Publicis Groupe envers la sécurité de l'information et la protection des données. La stratégie consiste à fournir des expériences de micro-apprentissage conviviales (sessions de formations en ligne, courtes et ciblées) aux Personnes et un contenu adapté aux groupes à haut risque afin d'encourager les comportements conscients de la sécurité. Le programme de sensibilisation à la sécurité vise à :

- Sensibiliser les personnes à leurs responsabilités en matière de protection des informations des clients et du Groupe, telles que définies dans les politiques de sécurité du Groupe.
- Former les personnes sur les meilleures pratiques de sécurité, les normes de sécurité applicables, les exigences de sécurité contractuelles et légales.
- Former les personnes à reconnaître les incidents présumés ou réels qui ont un impact sur les informations du client ou du Groupe et à signaler ces incidents.

Des supports de sensibilisation à la sécurité sont créés et diffusés via de multiples canaux de communication (internes et externes) tels que : des campagnes de formation et de sensibilisation en ligne et hors ligne, y compris des articles sur la sécurité, des affiches, des vidéos sur mesure, des annonces, des canaux de collaboration, etc. Ces supports encouragent et renforcent l'importance des bonnes pratiques de sécurité de l'information par le biais d'un message cohérent et d'un engagement des personnes sur la façon dont elles peuvent contribuer à protéger les informations des clients et du Groupe. L'efficacité du programme de sensibilisation à la sécurité est mesurée par des tests de phishing (courriels simulant des messages malveillants réels), qui sont menés régulièrement tout au long de l'année.

Nom de la politique	Objectif
Politique de sécurité de l'information	*Donne des directives sur les principes, les objectifs, les contrôles et la gouvernance globale de la sécurité de l'information*
Politique de contrôle d'accès	*Donne des directives sur le contrôle de l'accès aux informations et aux installations du Groupe*
Politique de sécurité du réseau	Donne des directives sur la protection et la sécurisation du réseau du Groupe
Politique de sécurité du Cloud	Donne des directives sur l'hébergement ou l'utilisation en toute sécurité de solutions de Cloud computing internes ou externes
Politique d'utilisation acceptable	Donne des directives sur l'utilisation acceptable des actifs informationnels et encourage un comportement responsable pour la sauvegarde des informations
Politique relative aux appareils mobiles	Donne des directives sur l'utilisation sécurisée des appareils mobiles et sur les dispositions relatives au BYOD (Bring Your Own Device – Travaillez en utilisant votre matériel personnel)
Politique de réponse aux incidents	Donne des directives sur la manière de traiter une fuite d'informations sensibles conformément aux lois et réglementations internationales et locales

Certification ISO 27001 et vérification externe

Le programme et les politiques de sécurité de Publicis Groupe sont conçus pour aligner le Groupe sur les exigences de la norme mondiale de sécurité de l'information ISO 27001. Les domaines d'activité critiques de l'entreprise dans certains secteurs (par ex., l'infrastructure des services informatiques partagés backend, l'activité Epsilon, etc.) sont officiellement certifiés ISO 27001 et subissent des audits externes périodiques avec les organismes de certification.
Le système de gestion de la sécurité de l'information établi dans le cadre de la certification ISO 27001 est audité chaque année par les auditeurs externes de l'organisme de certification. Des analyses de vulnérabilité sont effectuées sur le périmètre du réseau du Groupe tous les quinze jours par l'organisation de sécurité du Groupe. Les vulnérabilités identifiées sont corrigées en fonction de leur priorité. Un test indépendant de notre réseau est également effectué par une tierce partie chaque année.

Gestion des incidents de sécurité

Publicis Groupe dispose d'un solide programme de gestion des incidents. Les employés peuvent signaler les incidents de sécurité par le biais du Helpdesk, ou en envoyant un e-mail à l'équipe de gestion des incidents du GSO. En fonction de la gravité de l'incident, la cellule de gestion des incidents est activée et l'équipe de gestion des incidents se mobilisent pour traiter le cas. Les parties prenantes pertinentes sont informées de l'incident et des mesures prises. Les incidents sont clôturés avec le rapport d'enquête et tout enseignement mis en évidence. Le contact de l'agence est chargé de communiquer les incidents de sécurité aux clients, le cas échéant.

Data center, serveurs et Cloud

Publicis Groupe a recours aux services de fournisseurs de data center renommés pour héberger ses informations. Ces opérateurs de data center sont soumis à des évaluations indépendantes régulières par des tiers accrédités et maintiennent des certifications industrielles telles que ISO 27001, SOC 1, SOC 2, etc. Les serveurs et autres infrastructures techniques sont situés dans des cages verrouillées au sein de ces centres de données. Un modèle de sécurité multicouche est mis en œuvre pour contrôler l'accès physique et logique à ces centres de données et serveurs. Les serveurs sont renforcés conformément aux meilleures pratiques du secteur et surveillés en permanence afin de garantir la confidentialité, l'intégrité et la disponibilité des informations. Au cours des dernières années, Publicis Groupe a franchi des étapes importantes dans son utilisation du Cloud. De nombreux services essentiels et applications sont aujourd'hui basés dans le Cloud et bénéficient du caractère évolutif, de la sécurité et de l'agilité de l'architecture Cloud.

Continuité des activités et reprise après sinistre

Publicis Groupe a mis en place des plans complets de continuité des activités et de reprise d'activité après sinistre. La stratégie adoptée pour la planification de la continuité des activités comprend l'activation du personnel mobile et le télétravail. Ceci est mis en œuvre en fournissant des capacités informatique mobile et de connectivité aux Personnes qui leur permettent de travailler à partir de sites «à distance», éliminant ainsi les dépendances aux installations de Publicis Groupe pour poursuivre l'activité. Des plans de reprise spécifiques à un projet ou à une opération, appelés Plans de continuité et de reprise des activités (BCRP), pour faire face aux pannes et aux catastrophes à long terme, spécifiques à un projet critique, à un travail pour un client, à nos activités opérationnelles et commerciales ou à une fonction, sont créés en fonction des besoins du client ou du projet.

QUI ?

Les Chief Executive Officers et Chief Financial Officers des Business Units et des Pays, les Chief Technology Officers, SSC, le Global Security Office et le département Informatique de Re:Sources.