MANPOWERGROUP

Politique Relative aux Cadeaux, Divertissements et Parrainages

ManpowerGroup BeLux
PR/21/0/FR – 01/08/2022

ManpowerGroup®

TABLE DES Matières

I. Introduction

Cette politique est prévue pour vous aider à déterminer s'il est approprié d'octroyer des cadeaux, repas, divertissements, hébergements, parrainages et avantages relatifs aux voyages, en particulier lorsque des agents publics sont impliqués. Elle énonce également les procédures à suivre. Elle doit être lue et comprise conjointement avec la Politique anti-corruption de ManpowerGroup. Cette politique s'applique à tous les employés, agents, membres du conseil d'administration et tiers agissant pour le compte de ManpowerGroup.

Les agents publics peuvent inclure :

- ✓ Les chefs d'Etat, ministres et autres figures politiques
- ✓ Les fonctionnaires
- ✓ Les autres agents publics travaillant à temps plein ou à temps partiel
- ✓ Les citoyens agissant à titre officiel (élus ou représentants d'association par exemple)
- ✓ Le personnel de sécurité (militaires, policiers et agents des renseignements)
- ✓ Les juges et parlementaires
- ✓ Les agents et employés d'entreprises publiques ou gérées par l'Etat (par exemple, une société de pétrole ou compagnie aérienne publique)
- ✓ Les employés d'autres institutions publiques, y compris les universités, laboratoires, hôpitaux, etc

La politique anti-corruption de ManpowerGroup interdit formellement tout type de corruption relative à l'activité de la société. L'octroi de cadeaux, divertissements, hébergement, ou autres avantages de voyage fait partie intégrante des affaires. Ces activités peuvent toutefois être considérées comme des pratiques corruptives dans certaines circonstances, et elles peuvent en outre engager la responsabilité pénale des personnes impliquées. Elles peuvent aussi être réglementées par le gouvernement du pays ou de la région où les prestations sont fournies, ou limitées par la règlementation interne de la société du destinataire. Cela est particulièrement vrai lorsque les prestations sont reçues par des individus considérés comme agents publics en vertu des lois prévues à cet effet. « Agents publics » est une définition large qui peut également inclure les agents de sociétés détenues ou gérées par l'Etat. En toute hypothèse, ManpowerGroup est tenu de procéder à des contrôles internes appropriés ainsi que de tenir des livres et registres précis en ce qui concerne ces avantages.

Les règles et les limites de dépenses de la présente politique régissent vos actions avec les tiers, tels que des clients, des fournisseurs et des agents publics. Les dépenses internes relatives aux cadeaux, repas et divertissements effectués au profit de vos collègues et vos équipes - ne sont pas soumises à cette politique groupe. Cependant vous devez toujours faire appel à votre bon sens et vous conformer au process d'approbation local pour ces activités

Tout employé qui apprend ou soupçonne une violation de cette politique doit immédiatement :

- ✓ Informer son manager ou superviseur,
- ✓ Informer le directeur juridique ou la Directrice de l'Ethique et de la Conformité Monde, ou
- ✓ Signaler des préoccupations via la ligne d'assistance téléphonique en matière d'éthique professionnelle de ManpowerGroup

II. Règles générales applicables à tous les types d'avantages

Les cadeaux, repas, divertissement, hébergement ainsi que les parrainages et autres avantages y compris la prise en charge de voyages sont ci-après dénommés "Avantages".

Les règles suivantes sont applicables :

1. Les Avantages ne sont **jamais** acceptables lorsqu'ils sont attribués à des agents publics, des partenaires commerciaux, des clients ou prospects afin d'influencer leurs actes ou décisions dans le cadre de leur fonction officielle ou professionnelle.

2. Il est attendu des employés de ManpowerGroup de faire appel à leur bon jugement lors d'une prise de décision quant à l'octroi d'Avantages, et d'être prêts à identifier l'objectif commercial légitime des Avantages accordés. Les sections spécifiques suivantes apportent quelques exemples d'activités légitimes.

3. Toutes les conditions de la loi locale et les règles de l'organisation du bénéficiaire doivent être respectées. De nombreuses entreprises limitent les cadeaux ou invitations que leurs employés peuvent accepter et les contrats clients peuvent imposer des restrictions supplémentaires. Avant d'octroyer des Avantages à un tiers, il est de votre responsabilité d'obtenir toute approbation requise de ManpowerGroup, et également de vous assurer que la règlementation locale, ainsi que les politiques de votre bénéficiaire, sont respectées.

4. Cette politique comprend des limites monétaires globales. **Votre pays a peut-être adopté des limites de dépenses inférieures pour refléter les pratiques locales.** Il vous incombe de comprendre et de vous conformer aux exigences mondiales et spécifiques à chaque pays.

5. Les Avantages doivent **toujours** être d'un montant raisonnable et d'une nature appropriée.

6. Certains types d'Avantages ne doivent jamais être accordés. Ceux-ci incluent les avantages en espèces, les avantages associés à une ou plusieurs activités illégales pouvant porter atteinte à la réputation de la société, telles que les services d'escortes, les lieux de divertissements pour adultes ou les jeux d'argent.

7. Les apparences doivent être prises en considération. Les Avantages que la plupart des gens considéreraient comme généreux, extravagants ou à caractère personnel (des bijoux ou objets de luxe, par exemple), les tickets pour des évènements hauts de gamme ou les séjours vers des destinations de loisirs ne doivent pas être accordés.

8. Les Avantages, tels que les cadeaux, accordés alors que des décisions commerciales ou contractuelles au bénéfice de ManpowerGroup sont pendantes, peuvent également soulever des problèmes de légalité et d'apparence et doivent de ce fait être évités

9. La fréquence des Avantages à des bénéficiaires spécifiques doit être surveillée. Même les Avantages relativement modestes, tels que les repas, lorsqu'ils sont offerts fréquemment, peuvent soulever des problèmes de légalité ou d'apparence et doivent de ce fait être évités.

10. La valeur totale des Avantages aux bénéficiaires spécifiques doit également être prise en compte. Si la valeur totale des cadeaux, repas et divertissements offerts à une personne donnée au cours d'une année dépasse **250 $**, il convient d'être prudent avant d'accorder d'autres Avantages à cette personne.

11. L'utilisation de fonds personnels pour offrir des Avantages est interdite.

12. Les dépenses liées à un Avantage doivent être précises, complètes et correctement documentées. Une documentation appropriée inclut des notes de frais, des informations sur tous les participants et bénéficiaires (y compris le nom et le lieu de travail) et une explication de l'objectif commercial.

13. Toutes les dépenses liées aux Avantages doivent être approuvées en vertu de la Section VII ci-dessous.

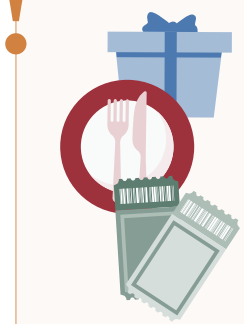
14. Les opérationnels qui estiment que leurs activités justifient des seuils ou des approches différents de ceux énoncés dans cette politique doivent discuter de leurs besoins avec la Directrice de l'Ethique et de la Conformité Monde.

III. Cadeaux

Tous les cadeaux doivent être adaptés à l'occasion, être d'un montant raisonnable et offerts uniquement par courtoisie ou témoignage d'estime. Un cadeau ne doit pas être offert pour influencer le choix des services de la société, ou encore influencer ou inciter une action d'un "agent public" ou d'un partenaire commercial. **ManpowerGroup a fixé pour les cadeaux une limite globale de 150 USD**. Vous ne pouvez pas dépasser cette limite globale sans autorisation écrite préalable. Pour obtenir une autorisation, veuillez vous référer au Tableau des approbations dans la Section VII. En plus des limites globales, des limites spécifiques de dépenses pour les cadeaux ont été fixées par chaque responsable pays. Vérifiez la limite spécifique à votre pays avant d'offrir un cadeau.

Outre les règles générales stipulées dans la section II, les directives suivantes s'appliquent aux cadeaux faits à des agents publics, partenaires commerciaux, clients ou prospects.

- ✓ Les cadeaux doivent être offerts ouvertement et en toute transparence ; ils doivent être en adéquation avec l'occasion célébrée. Si vous ne vous sentez pas à l'aise de le faire, c'est le signe d'un éventuel problème.
- ✓ Les coutumes et pratiques locales dans certaines régions peuvent différer, et cela doit être pris en compte
- ✓ Les espèces et équivalents tels que les cartes-cadeaux, les chèques de voyage, les unités de recharge pour mobile et les chèque ne sont jamais acceptables en tant que cadeaux.
- ✓ Les cadeaux aux sociétés ou groupes qui sont prévus pour être partagés entre collègues (des paniers alimentaires, par exemple) sont préférables aux cadeaux individuels.
- ✓ Une attention particulière doit être attribuée aux cadeaux faits à l'attention des responsables des achats et autres ayant l'autorité d'accorder des contrats à la société. Les cadeaux attribués lorsqu'un contrat est en cours de négociation peuvent donner l'impression d'une intention illégitime d'influencer ; ils doivent donc être évités.
- ✓ Les cadeaux d'objets pour un usage personnel ou pour les membres de la famille ou amis d'agents publics ou partenaires commerciaux sont moins adaptés que les objets promotionnels de la société, mais peuvent parfois être adaptés (des fleurs ou un «cadeau pour les "hôtes")



quelques exemples de cadeaux appropriés :

- ✓ Des cadeaux pour célébrer les fêtes généralement associées avec la remise de cadeaux, y compris Noël, le nouvel an chinois et autres évènements similaires.
- ✓ Des cadeaux pour commémorer des événements spéciaux, comme un anniversaire de la société, la clôture d'une transaction commerciale, une retraite etc,
- ✓ Les objets promotionnels marqués du logo de la Société, tels que les verres, les accessoires de bureau, les stylos, tasses à café, t-shirts, chapeaux, etc., constituent généralement des cadeaux appropriés.

IV. Repas et invitations

Tel qu'employé dans cette section, les repas et invitations comprennent à la fois les repas au restaurant ainsi que les événements culturels et sportifs, en personne ou virtuels, où nous pourrions acheter des billets d'entrée, de la nourriture et des boissons. Notez que les repas ou divertissements faisant partie d'un voyage parrainé sont couverts par la Section V ci-dessous, Voyage. **ManpowerGroup a une limite globale pour les repas et invitations de 200 USD**. Vous ne pouvez pas dépasser cette limite globale sans autorisation préalable. Pour obtenir une autorisation, veuillez vous référer au Tableau des approbations dans la Section VII. En plus des limites globales, des limites de dépenses spécifiques à chaque pays pour les repas et les invitations ont été définies par chaque responsable de pays. Vérifiez les limites spécifiques à votre pays avant de proposer des repas et/ou invitations.

Quelques exemples de repas et invitations légitimes :

- ✓ Un déjeuner annexe à une réunion d'affaires avec un client.
- ✓ Un dîner pour célébrer le début d'une nouvelle relation commerciale.
- ✓ Inviter un partenaire commercial ou un client à se joindre à un employé lors d'un match de football. Notez que les dépenses totales de l'événement, y compris les billets et toute nourriture et/ou boisson fournie, ne doivent pas dépasser la limite globale.
- ✓ Vous avez une réunion planifiée sur deux jours avec un client ou un prospect. Le deuxième jour, vous organisez un dîner-croisière de clôture.

Outre les règles générales stipulées dans la section II ci-dessus, les directives suivantes s'appliquent à la provision de repas et des invitations à des "agents publics", partenaires commerciaux, clients ou prospects.

- ✓ Les repas d'affaires doivent être rares, conformes aux normes du pays et des pratiques commerciales locales, et jamais extravagants.
- ✓ Les Employés de ManpowerGroup sont tenus de choisir des lieux de repas et de divertissement qui relèvent de cette Politique. Si vous laissez le choix du lieu à la personne invitée, vous êtes potentiellement en train de créer une situation dans laquelle vous serez incapable de respecter cette Politique. Planifiez à l'avance et évitez toute situation dificile et embarassante !
- ✓ Les membres de la famille ou les amis d'un "agent public", partenaire commercial, client ou d'un client potentiel n'assisteront pas à un repas, évènement sportif ou divertissement aux frais de la société, à moins qu'il s'agisse d'un évènement auquel les conjoint(e)s / ami(e)s des employés de ManpowerGroup sont également conviés ou que l'autorisation préalable a été obtenue auprès de la Directrice conformité et éthique monde.
- ✓ Le divertissement peut faire partie d'une rencontre commerciale légitime, à condition que l'objectif principal de la rencontre porte sur les affaires et le développement commercial. Les divertissements individuels sans lien avec les objectifs commerciaux, tels qu'un week-end de Golf, ne sont généralement pas considérés comme appropriés et requièrent une autorisation préalable spécifique de la part de la Directrice Conformité et Ethique Monde.
- ✓ Un employé ou un représentant de la société est tenu d'assister aux évènements sportifs ou divertissement avec l'agent public, partenaire commercial, client ou prospect qu'il invite. Par exemple, l'octroi de tickets pour un évènement sportif afin que l'individu y assiste seul ou accompagné d'une personne de son choix n'est généralement pas approprié.
- ✓ Dans la mesure du possible, le paiement du repas ou de l'invitation doit être effectué directement par les employés de ManpowerGroup aux fournisseurs de services
- ✓ Dans les cas plus rares où le remboursement à un agent public ou à un partenaire commercial des frais de repas et de divertissements est adapté, le remboursement doit être justifié par des reçus adaptés reflétant la nature et le montant des dépenses remboursées.

V. Parrainages de voyages

En règle générale, les agents publics, les partenaires commerciaux, les clients ou les prospects doivent payer les frais de leur propre voyage. Cependant, dans certaines circonstances, la Société peut payer les frais de déplacement d'un agent public, d'un partenaire commercial, d'un client ou d'un prospect pour se rendre sur le site de l'entreprise, pour une réunion conjointe ou pour d'autres objectifs commerciaux appropriés. Les frais de déplacement peuvent inclure le transport, l'hébergement et les repas, ainsi que d'autres frais accessoires. La prise en charge des frais de déplacement par la Société peut impliquer des dépenses importantes et nécessiter une autorisation. Pour obtenir une autorisation, veuillez vous référer au tableau des approbations dans la Section VII.

Exemples dans lesquels la Société peut payer les frais de déplacement :

- ✓ Une réunion du conseil d'administration d'une joint-venture dans laquelle le partenaire de la Société est une entreprise d'État.
- ✓ Un contrat avec un client vous oblige à payer les déplacements du personnel à des fins de formation.
- ✓ Un client potentiel veut observer comment les services sont fournis dans un lieu particulier.
- ✓ Une visite au siège de la Société pour comprendre les capacités de ManpowerGroup.

Outre les exigences générales de la section II ci-dessus, les directives suivantes s'appliquent à la prise en charge des **frais de déplacement** des agents publics, des partenaires commerciaux, des clients ou des prospects :

- ✓ Tous les voyages pris en charge par la Société doivent supposer un objectif commercial légitime. La prise en charge de frais de déplacement destinés uniquement aux loisirs ou au divertissement ne seront pas autorisés.
- ✓ Les paiements sous la forme d'une indemnité journalière pour les personnes dont le voyage est pris en charge, par exemple, les paiements en espèces ne seront généralement pas autorisés.
- ✓ Dans la mesure du possible, le paiement des frais de déplacement doit être effectué directement au fournisseur de services, par exemple, compagnie aérienne, hôtel, restaurant.
- ✓ Si le remboursement des frais de déplacement est approprié, ce remboursement doit être justifié par des reçus appropriés reflétant la nature et le montant de la dépense.
- ✓ En règle générale, c'est à l'entreprise, l'agence ou l'organisation bénéficiaire de sélectionner les personnes dont le voyage sera parrainé plutôt que ManpowerGroup.
- ✓ Les personnes parrainées doivent pouvoir justifier qu'elles ont reçu toutes les autorisations internes leur permettant de voyager.
- ✓ Aucun membre de la famille ou ami ne peut accompagner l'agent public, le partenaire commercial, le client ou le prospect lors du voyage aux frais de la Société, à moins que la famille et/ou les amis soient indépendamment éligibles pour recevoir un tel hébergement.

VI. Sponsoring des Evenements

Le sponsoring et le mécénat peuvent prendre diverses formes, par exemple, lorsque la Société parraine une exposition, une activité, un programme ou autre. Le sponsoring et mécénat permettent généralement à la Société de promouvoir ses services ou de gagner en visibilité et bienveillance. Les événements qui sont étroitement liés à des “agents publics”, des partenaires commerciaux, des clients ou prospects (par exemple, le parrainage est demandé par un “agent public”, ou l’organisation parrainée est réputée liée à un “agent public” ou un membre de sa famille proche) posent des problèmes particuliers, tout comme les parrainages réalisés dans le cadre d'un contrat en cours. Pour obtenir une autorisation dans une telle situation, veuillez vous référer au tableau des approbations dans la Section VII.

Outre les règles générales stipulées dans la section II ci-dessus, les directives suivantes s'appliquent au sponsoring et mécénat au profit des "agents publics" ou des partenaires commerciaux.

- ✓ Les parrainages d'événements doivent avoir pour objectif principal la promotion des services de la Société, de la bonne citoyenneté d'entreprise ou une autre justification commerciale légitime.
- ✓ Le service qui souhaite parrainer l'événement doit mener une diligence raisonnable sur l'organisme bénéficiaire et les personnes qui sollicitent le parrainage de la société et doit documenter et conserver ces résultats. Dans la mesure du possible, les paiements doivent être versés directement à l'organisme bénéficiaire. Les parrainages ne doivent pas être effectués en espèces.
- ✓ Les employés de la société sont tenus de prendre des mesures afin de vérifier que les fonds ainsi versés sont utilisés aux fins prévues, et que la société reçoit les prestations accordées en échange du parrainage.
- ✓ Tout voyage lié au parrainage de l'événement doit être conforme aux exigences de la Section Voyage de la présente Politique, énoncées dans la Section V.
- ✓ Les cadeaux offerts dans le cadre de l'opération de sponsoring et/ou mécénat doivent être conformes aux exigences de la section "Cadeaux" de cette politique, énoncée dans la Section III.

VII. Autorisations et approbations

Le tableau ci-dessous décrit les exigences d'approbation en vertu de la présente politique Groupe N'oubliez pas de vous conformer aux limites locales ou aux exigences d'approbation.

Approbations de cadeaux, divertissements et parrainages

Type d'avantage fourni	L'approbation est requise pour :
Cadeaux	Cadeaux supérieurs à **150 $** par bénéficiaire.
Repas et divertissement	Repas et divertissements dépassant **200 $** par bénéficiaire.
Sorties de divertissement autonome sans objectif commercial particulier	Toutes les sorties.
Voyages	Toutes les prises en charge de frais de déplacement.
Parrainer des événements étroitement liés à des agents publics, des partenaires commerciaux, des clients ou des partenaires commerciaux ou prospects	Tous les événements.

Processus d'approbation

Toutes les demandes d'autorisation doivent être envoyées par courrier électronique à :

giftsandentertainment.authorization@manpowergroup.com.

Veuillez inclure des détails concernant les dépenses proposées, y compris le nom, le titre et l'affiliation des participants proposés, le budget, les prestataires de services. Vous devez également indiquer l'objectif commercial.

La Direction de l'Ethique et la Conformité Monde examinera votre demande. Toutes les approbations seront faites par écrit. Dans l'hypothèse où une dépense approuvée serait différente de la proposition soumise (à savoir, si la dépense réelle dépasse de manière significative le budget proposé, ou si les participants changent), une nouvelle approbation est requise.

Tenue de registres

Vous devez conserver les registres des dépenses. Tous les rapports de frais ou dépenses doivent stipuler, par écrit, les noms, les titres et les affiliations des participants ainsi que l'objectif commercial à l'origine de la dépense.

VIII. Administration et demandes de renseignements

Le Directeur Juridique Monde, **Richard Buchband**, supervise le respect de la présente politique et du programme anti-corruption de la Société. Sous sa direction, **Shannon Kobylarczyk**, Directrice de l'Ethique et la Conformité Monde gèrent les demandes de renseignements et les approbations.

Si vous avez des questions, veuillez contacter Shannon au **414.906.7024** ou veuillez écrire à notre équipe à ethics.training@manpowergroup.com ou generalcounsel@manpowergroup.com.

ManpowerGroup

ESG/DURABILITÉ

ENVIRONNEMENT

POLITIQUE ENVIRONNEMENTALE

« C'est maintenant le moment d'agir pour le climat. »

#TheChangeStartsWithYouAndMe

NOTRE ENGAGEMENT

ManpowerGroup s'est engagé dans la lutte contre le réchauffement climatique.
En 2021, nous avons fait valider nos objectifs climatiques par l'organisation 'Science Based Targets (SBTi)', l'autorité de référence en matière d'action climatique dans le monde de l'entreprise.

Nous avons l'ambition d'atteindre l'objectif de zéro émission nette d'ici 2045 au plus tard et dans cette transition nous nous sommes engagés d'ici 2030 à :

- **réduire de 60% les émissions liées à nos activités opérationnelles** (Objectif 1 & 2 – consommation d'énergie et d'électricité dans les bâtiments, voitures de sociétés etc.)
- **réduire de 30% les émissions de la chaîne d'approvisionnement** (Objectif 3 – gestion des déchets, voyages, mobilité, fournisseurs).

Notre plan d'action se concentre sur les domaines ayant le plus d'impact sur le climat et nous mesurons chaque année nos progrès à partir des données récoltées selon une méthodologie rigoureuse.

ManpowerGroup Belgium partage la même ambition.
Pour concrétiser notre stratégie mondiale, nous avons fixé les objectifs suivants :

ÉNERGIE

- 100% d'énergie renouvelable pour nos agences et nos bureaux d'ici 2030.
- Transition progressive de notre réseau d'agences vers des bâtiments à faible empreinte carbone.
- Diminution de notre consommation d'énergie

MOBILITÉ

- Zéro émission de CO2 par nos voitures de société d'ici 2030.
- Mise en place d'actions visant à réduire l'impact environnemental de nos déplacements (plan de mobilité, horaires de travail flexibles, modes de travail hybrides, limitation des voyages professionnels).

ZÉRO PAPIER / ZÉRO DÉCHETS / RECYCLAGE

- 95% de nos documents externes sous forme électronique d'ici 2024 et réduction de nos impressions internes de documents se rapprocher du 'Zéro Papier'.
- 100% Tri & Recyclage : procédures en place pour garantir une réduction et un tri optimal des déchets internes, ainsi qu'un recyclage des matériaux (mobilier de bureau, matériel informatique, matériel électrique, cartouches d'encre etc.).

ACHATS DURABLES

- Utilisation de produits durables dans la gestion quotidienne de l'entreprise (fournitures de bureau, sacs, matériel promotionnel, gobelets, etc.).
- Imposition de normes environnementales à nos fournisseurs.

Nous sensibilisons toutes les parties prenantes aux enjeux environnementaux.

Tout le personnel de ManpowerGroup participe à la réalisation de nos objectifs climatiques en adoptant quotidiennement des comportements éco-responsables.

'The Change Starts With You And Me'

ManpowerGroup BeLux

ManpowerGroup BeLux
PR/10/3/FR – 01/10/2025

ManpowerGroup

ESG/DURABILITÉ

DIALOGUE SOCIAL

POLITIQUE DIALOGUE SOCIAL

“Nous sommes convaincus que le maintien d’un climat social sain est nécessaire pour garantir un climat économique sain.”

Nous veillons à établir des relations de confiance avec les partenaires sociaux et nous respectons le rôle des organisations syndicales, dans le cadre de leur mission légale.

La direction des Ressources Humaines de ManpowerGroup BeLux, en étroite collaboration avec le responsable des relations sociales et le responsable du département légal, assure la gestion et l’animation des relations professionnelles, syndicales et institutionnelles de ManpowerGroup.

Ils accompagnent et pilotent :

- la gestion du calendrier social et les réunions des institutions représentatives du personnel;
- les négociations avec les organisations syndicales représentatives;
- la gestion individuelle et collective des représentants du personnel;
- les élections sociales.

ManpowerGroup BeLux

ManpowerGroup BeLux
PR/10/3/FR – 01/10/2025

MANPOWERGROUP'S INFORMATION SECURITY POLICY

TODAY'S CONTEXT: RAPID DIGITAL TRANSFORMATION

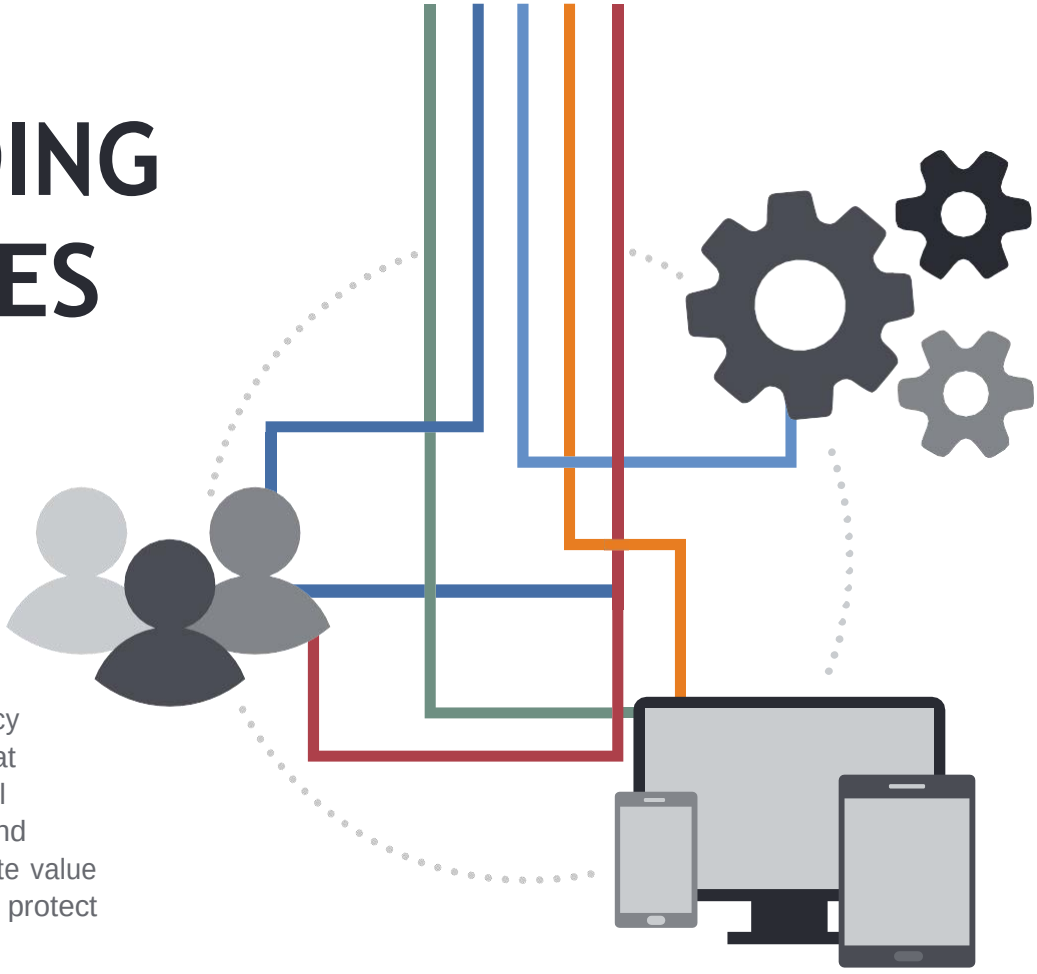
The severity, frequency and impact of cyber-crime has been on the rise for a number of years. Now, with the acceleration of remote working and rapid digitization organizations will require even greater prioritization of information security capabilities. Business and security leaders are being challenged with advanced operational speed, unprecedented resilience and increasing regulatory oversight.

"As technology evolves and we adopt new tools and expand our use of data and analytics to deliver more value to clients and candidates, we are committed to being good stewards of the information entrusted to us. Managing our information security is vital to ensuring trust and transparency with our employees, clients, candidates, associates and partners. At the same time, the frequency and sophistication of cyber attacks are rising and we take our responsibility to be vigilant and to educate our people seriously."

Randy L. Herold
Chief Information Security Officer and Chief Privacy Officer

ManpowerGroup BeLux
PR/22/0/ENG – 01/08/2022

OUR GUIDING PRINCIPLES



Keeping information safe requires constant risk assessment. Our Information Security and Privacy Program is a global framework that goes beyond just preventative tool sets, combining people, process and technology to reduce risk and create value for our clients. Our top priority is to protect the data people entrust to us.

Our commitment to the highest standards of information security and data privacy are outlined in our global Code of Business Conduct and Ethics. Available in 20 languages our Code is shared with every employee and may be available to our stakeholders around the world.

PEOPLE

- Recognizing the best line of defense is not a tool or platform - it's our people.
- Understanding and influencing user behavior by knowing where information resides, how it moves across our systems, and who has access to it throughout the full information lifecycle, so that we can protect the data of our employees, clients, candidates, associates and third-parties.
- Leveraging collective threat intelligence through relationships with industry partners like the FS ISAC which allows us to share practices and maximize our security capabilities.

PROCESSES

- Positioning information security as a governing body – Information Security provides the oversight necessary to align our technology services with business, legal and regulatory requirements.
- Focusing on situational awareness and response time by targeting our monitoring capabilities specifically on ways we can improve our awareness.

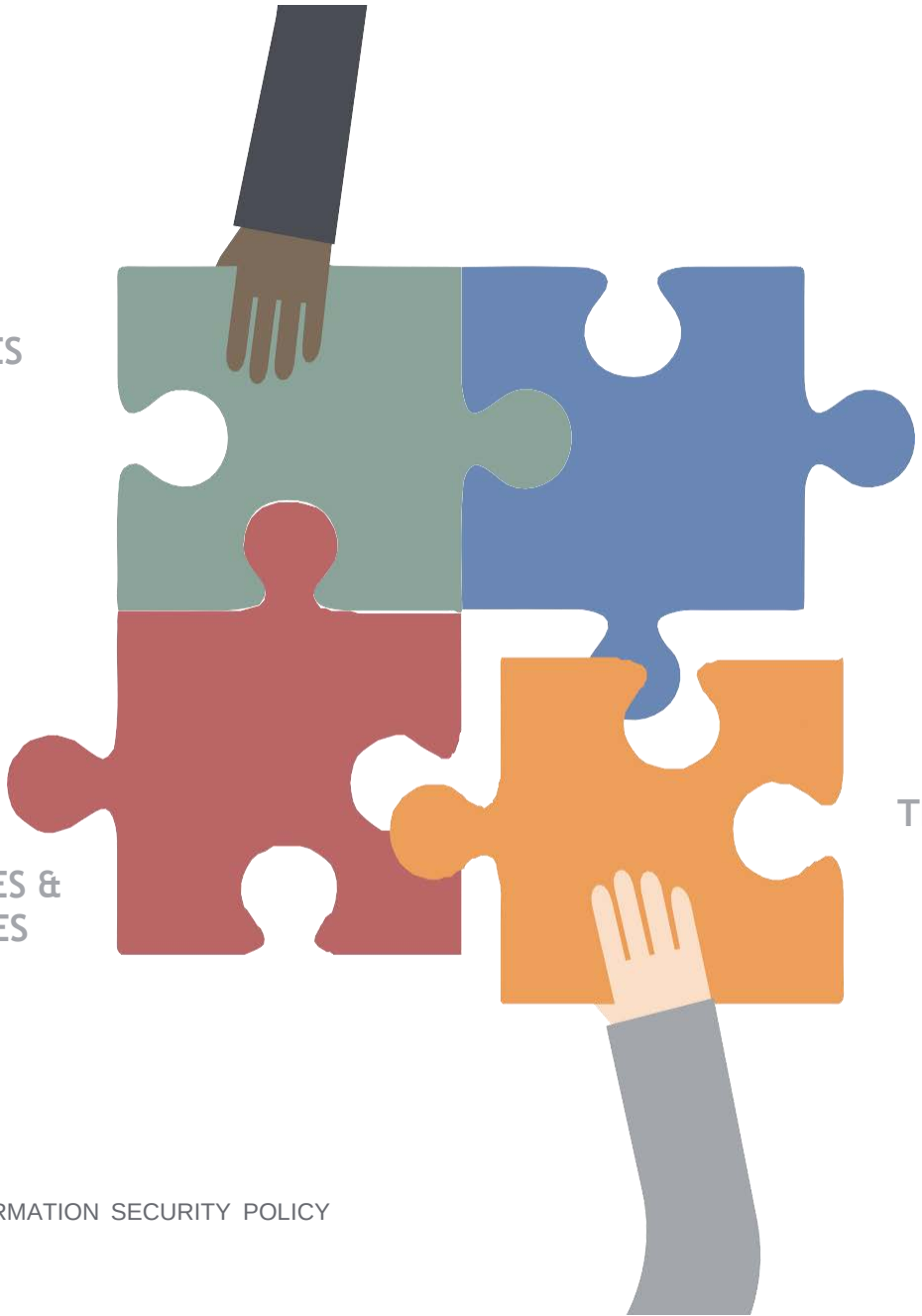
TECHNOLOGY

- Recognizing that preventative technology is not enough to keep a determined attacker at bay, we've expanded our detection and response capabilities throughout the organization.
- Preventing credential theft by prioritizing privileged access management capabilities.

PEOPLE

PROTECTING WHAT MATTERS: OUR EMPLOYEES, CLIENTS AND ASSOCIATES

At ManpowerGroup, our impact extends far beyond our own internal operations. Our clients and associates entrust us with their business-sensitive data, and we take that responsibility seriously. Our Global Privacy Policy describes the types of personal information we collect from employees, clients, candidates, associates and third parties, how we use it, with whom we share it, and the rights and choices available to individuals regarding our use of their information. All privacy policies, maintained at the country level, align with our global standards and comply with local laws and regulations.



LEADING FROM THE TOP

Our Information Security philosophy is led from the top with our Board's oversight capacity to ensure key security threats are managed through an effective governance and management structure. The Chief Information Security Officer (CISO) meets quarterly with the Audit Committee of the Board of Directors to review and discuss security strategy and progress around our investments. Under the direction of the CISO, responsibility for our global security program resides at the highest levels of executive leadership reporting to the Chief Financial Officer.

A MULTI-LAYERED APPROACH TO GOVERNANCE

While our CISO maintains a regular reporting cadence with the ManpowerGroup Board of Directors, including an annual report outlining our compliance and adherence to this Information Security Policy, the Security function operates independently from Information Technology (IT). Regular updates are provided to both the Board and Executive Leadership Team, as well as various steering and working committees. The Information Security Program is assessed annually by an independent third party to ensure alignment with the current threat landscape.

Our organizational structure utilizes a functional approach where strategy, business alignment and oversight are direct responsibilities of the CISO. Functions, such as architecture, operations and vendor management, resident within the CISO's team of direct reports, which includes third-party contractors and managed service providers.

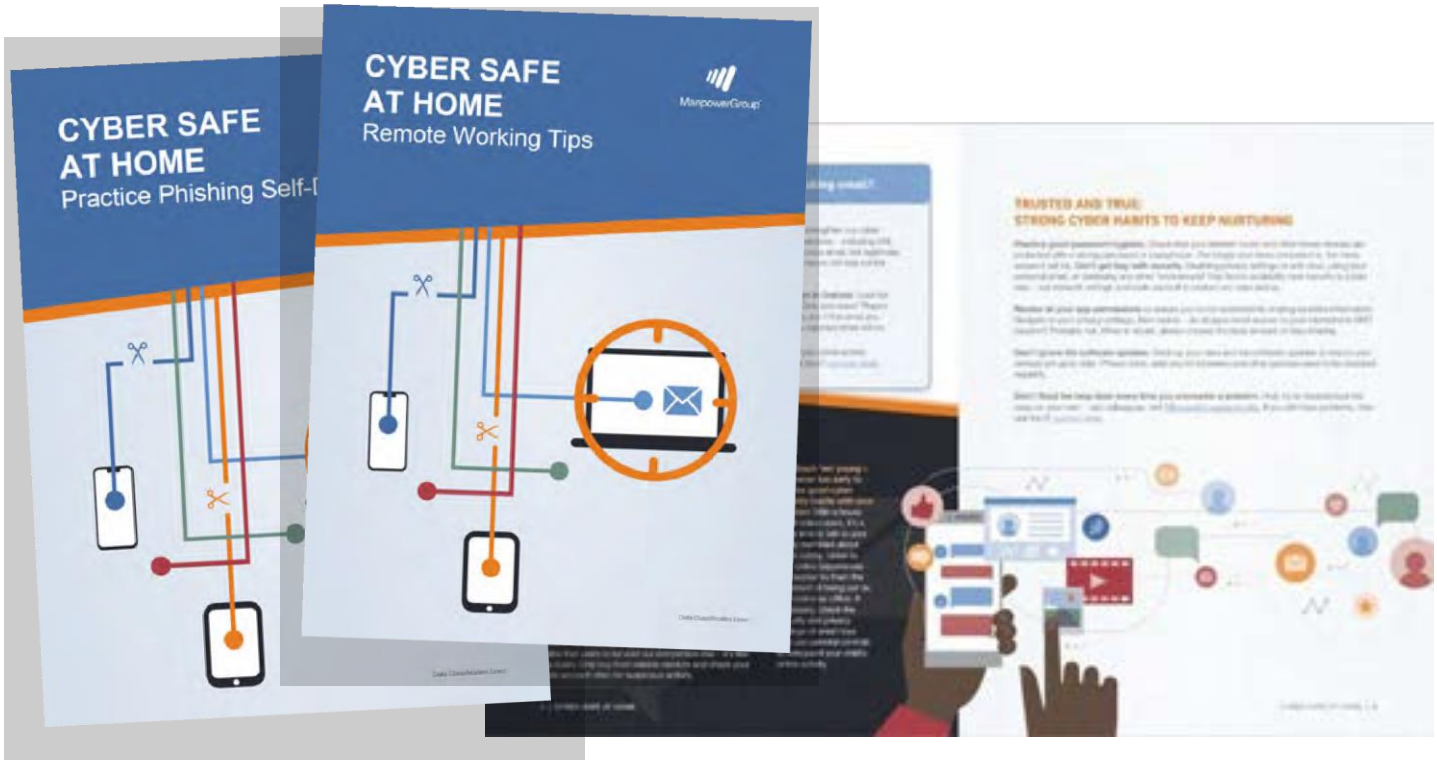
Our talented team dedicated to information security and data privacy has increased in size significantly over recent years. Our people are strategically positioned at the global, regional and local market levels to provide consistent policies, processes and technology solutions. Our highly trained staff maintains industry certifications that include: CISSP, CISM, CISA, CRISC, CSCP, CCISO, CCSP, CASP, CPDSE, ISO 27001 Lead Auditor, ISO/IEC 27005 Risk, Manager, CIPM, CIPP/E, FIP.

BUILDING THE CAPABILITIES AND SKILLS OF OUR PEOPLE

We recognize that preventative technology is not enough to keep a determined adversary at bay and acknowledge that our best line of defense against security threats is not a technology tool or platform – it's our people.

That's why we continuously develop updated employee education and awareness programs including online training, regular anti-phishing exercises and company-wide Cyber Month Campaign, offering daily bite-size training, instructor-led seminars, team activities and security related quizzes and competitions. All members of the Executive Leadership Team are included in all cyber training and phishing awareness campaigns alongside the whole organization. Through this awareness training, employees are educated on how to report suspicious activities they identify in their workplace environment or in the technology they use. As an example, seamless security integration enables employees to report suspected phishing emails with one click. Additionally, third party service providers and partners with access to sensitive data or systems are required to participate in security awareness training equivalent to that provided to ManpowerGroup employees.

Through these enhanced and targeted awareness efforts, employee engagement and digital learning campaigns, and regular communications from the CISO and Information Security teams, we are nurturing a risk-aware culture across our organization and our resilience to social engineering continues to demonstrate measured improvement year on year.

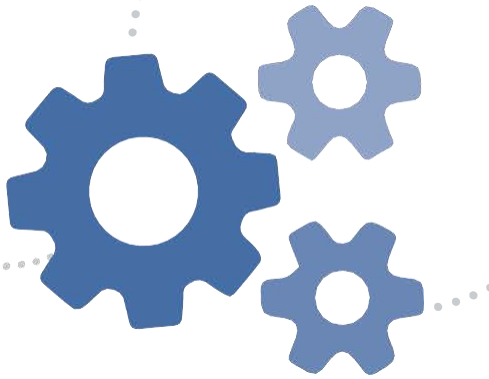


Embedding Security into our People & Culture Practices

ManpowerGroup ensures that industry-acknowledged security practices are incorporated into our People and Culture (P&C) employee management practices, including:

- Defining, documenting, and communicating the information security roles and responsibilitiesof employees, contractors and third-party users through the security awareness program
- Signing confidentiality agreements as part of an employment contract
- Requiring third parties to maintain compliance with information security requirements
- Ensuring that employees have access to current security policies, standards and procedures
- Providing employees – including Executive Leadership and CISO - with regular information security awareness training
- Ensuring that ManpowerGroup information assets are returned upon engagement termination
- Removing access rights to information upon engagement termination

PROCESSES



MAINTAINING PROTOCOL

We have established a comprehensive global information security framework, aligned with the NIST CSF (National Institute of Standards and Technology Cyber Security Framework) and internationally recognized ISO 27001 standard, which all of our operations around the world are required to adopt. All policies, procedures, controls and standards have been documented, communicated and operationalized; each has a dedicated owner and are reviewed at least annually for appropriateness and adequacy. ManpowerGroup uses multiple technologies as well as manual verification processes to enforce compliance with internal policies as well as regulatory and contractual requirements.

Policies: to align with industry standards.

Controls: to confirm policies are enforced.

Standards: to ensure contractual, legal and regulatory compliance.

Procedures: to utilize the standards.

SECURE, BY DESIGN

Recognizing preventive technology is not enough, all of our processes are designed with a defense-in-depth philosophy; if one layer of the process fails, a subsequent process is designed to mitigate the risk. Security controls are implemented across multiple layers and are integrated into a centralized monitoring solution, which ensures that we are able to monitor and respond efficiently 24x7. Through all our processes, we work to prevent credential theft by leveraging the principles of “least privilege” and “need to know” to minimize access risk and limit lateral movement within our environment.

OVERSEEING OUTSOURCED INFORMATION SECURITY SERVICES

Some daily operational security activities are outsourced to provide us with access to new skillsets and maximize our financial investment. All third-party resources leveraged for information security expertise are vetted prior to contract engagement and must meet or exceed ManpowerGroup's own policy standards. To ensure continued quality and information security assurance, these suppliers are held to contractually binding service level agreements, regular business reviews, and audits of their practices.

We have established controls to protect the integrity, confidentiality, and availability of information assets that are accessible to outsourcers, partners, clients, and external suppliers, including:

- Requiring that agreements or contracts with third parties that create, access, store, transmit and / or process ManpowerGroup information include the Vendor Information Security Requirements (VISR) defined for the type of services provided
- Requiring CISO or delegate approval to changes to information security requirements
- Requiring remediation or implementation of mitigation controls for identified third-party business processing risks
- Ensuring signed confidentiality and non-disclosure agreements or equivalent documentation are in place
- Only granting third-party access to ManpowerGroup information assets upon business need and requiring written approval by an authorized ManpowerGroup executive or their delegate

SOFTWARE DEVELOPMENT LIFECYCLE (SDLC)

Application development efforts follow the defined secure SDLC process where security requirements are defined, documented, and tested. Application development ensures secure coding practices are utilized and evidenced via pre-promotion security assessments. Additionally, educational materials for developers on secure coding are published and a strict separation of duties has been implemented between production and non-production environments.

Assessing for Risks

INSIDE OUT:

We continuously assess ourselves and adjust our defenses in real-time.

1

Collecting Data & Identifying Information Assets

The first step in our risk assessment process is to gather information from our business and technical subject matter experts. Both technical and non-technical evidential documentation is gathered as well as key performance indicator (KPI) reports.

2

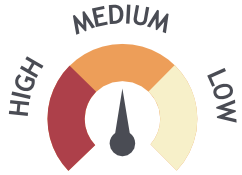
Analyzing Risks

ManpowerGroup's data classification standard allows us to quickly classify, and rank information assets based on their function, the criticality of the data they support, and the sensitivity of the data created, accessed, stored, transmitted or processed.

Controls are evaluated regularly to determine their protective and / or detective effectiveness. They are not assumed to be completely effective, therefore consistent reporting helps assess their impact. These reviews include physical and technical controls and apply to both ManpowerGroup operations as well as third party functions. Key performance indicators are used to identify which controls require attention and action is taken accordingly. And then the cycle repeats.

As part of the risk assessment process, we continually assess for potential threats and vulnerabilities.

- Vulnerabilities: solution weaknesses or control gaps that if exploited, could result in the authorized disclosure, misuse, alteration or destruction of information assets.
- Threats: potential agents for exploiting a vulnerability



3

Assigning Risk Ratings

The last step is assigning a rating (High, Medium or Low) for each information asset. The rating is a culmination of the information asset inventory, asset classification, threat and vulnerability assessment, and the control effectiveness evaluation.

4

Rinse, Repeat

The risk assessment process is a constant cycle of self-evaluation and remediation.

OUTSIDE IN: Staying Aligned with a Changing Threat Landscape

Each year an independent external assessor conducts a risk / threat assessment to evaluate the effectiveness of our program in the context of a fast-changing security landscape. This assessment, along with metrics and key performance indicators (KPIs), is reported to senior leadership and the Board. Additional independent assessments are also conducted throughout the year by third parties and clients as well as both internal and external audit. The results are shared with the Information Security team and remediation activities are developed and integrated into the on-going projects / daily activities of the Information Security team and their supporting partners.

Access Control

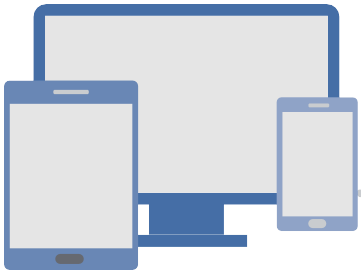
To safeguard our information assets, access is limited to authorized, business-justified entities with a “need to know.” We have taken thorough measures to prevent the inappropriate use of access credentials:

- Requiring strong authentication for and monitoring all access to sensitive information
- Issuing unique authentication credentials in accordance with “least privilege” and separate from standard user-level user IDs
- Disabling all system access after a period of inactivity
- Monitoring all network infrastructure, hardware and software while privileged access is in use
- Changing default access and configurations provided by hardware and software vendors
- Encrypting information shared in digital communications required by law, regulation or contractual agreement
- Requiring multi-factor authentication (MFA) for all remote access

Physical and Environmental Protection

Processes and procedures protect against unauthorized physical access, damage, and interference with business operations:

- Protecting secure areas with defined security barriers and entry controls
- Physically protecting all information assets such as paper files, end user devices, servers, network devices, databases, storage devices and backups from unauthorized access, damage, and interference
- Instructing employees to lock unattended systems and secure their workspace environment
- Securing facilities against unauthorized access per applicable local laws, regulations, and contractual requirements
- Ensuring that information retention and destruction follows ManpowerGroup’s Record Retention Policy



TECHNOLOGY

Monitoring Activity, Analyzing and Responding to Security Events

ACTIVITY MONITORING

ManpowerGroup has established an organization-wide Security Information and Event Monitoring (SIEM) solution that collects event information from ManpowerGroup devices (e.g. IDS/IPS, HIDs, system event logs and firewalls) and sends it to the Security Operations Center (SOC) for detailed analysis. The SOC correlates and analyzes the data to identify potential malicious behaviors / activity. The SOC also uses input from third-party threat analytics to assist in the identification of indicators of compromise (IOC) that may exist within the ManpowerGroup environment.

ANALYZING AND RESPONDING

ManpowerGroup uses an incident tracking system to document and track security events including:

Event Entry

Events reported to the Security team or identified by the SOC, where a designated member of the Security team assumes ownership of the event and the responsibility for updating the tracking system and escalations where necessary.

Tracking

Tracking occurs on all opened events to document investigation details, drive accountability and ensure timely closure. Escalation measures ensure appropriate parties are informed and necessary requirements are met, especially in a situation where timely escalation is required as part of regulatory compliance and / or the fulfillment of an established contractual agreement. Additionally, the root cause and responsible party are determined to assist in remediating the incident.

Remediation

Remediation may require participation from various teams and external parties. The Information Security team provides guidance or direction on appropriate corrective measures.

Incident Closure

An incident is classified as closed after evidence has been gathered to confirm that the required remedial actions and / or preventive measures have been performed or risk has been mitigated to an appropriate level which requires senior leadership sign-off.

Post-Closure Lessons Learned

After formal closure, a holistic review of the incident occurs, including root cause analysis, communications review and opportunities for improvement in the overall response / remediation process.

Encryption

Our encryption controls ensure that sensitive information remains confidential and protected while at rest or in motion. Protections include:

- Implementing an encryption standard that defines the requirements for encrypting sensitive information and ensures compliance with statutory, regulatory and contractual requirements
- Encrypting sensitive information when it is stored or transmitted across public networks
- Encrypting remote access connections into our ecosystem
- Requiring CISO approval for non-standard encryption methods

Malware

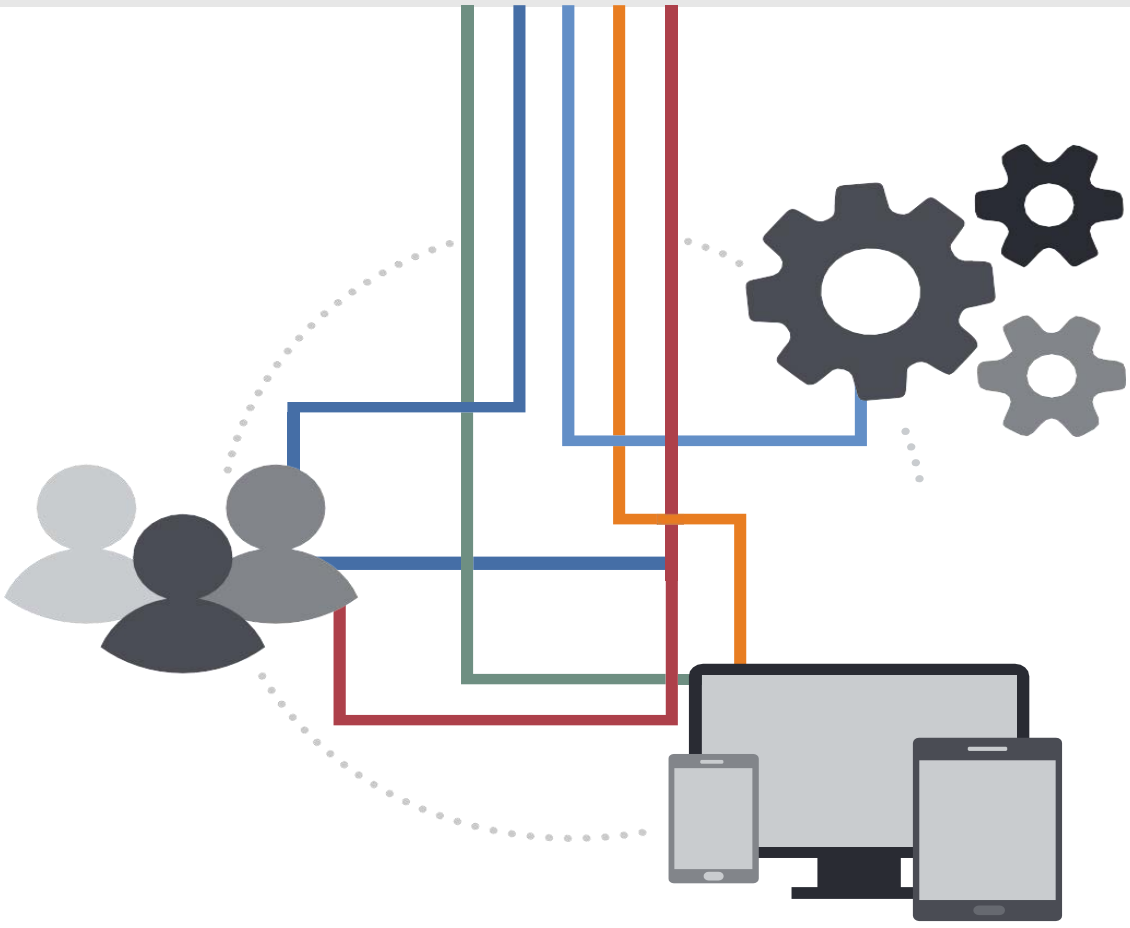
We protect from malicious code execution (Malware) through activities including:

- Confirming our security controls through regular audits
- Monitoring and recording systems and events
- Protecting information system logging facilities and log information against tampering and unauthorized access
- Subjecting all hardware and software to adhere to the vulnerability management program that includes anti-virus protection, security patches and industry-acknowledged practices for asset hardening and defense
- Requiring workstations and servers to install, configure and maintain end-point protection software
- Scanning public-facing web applications for vulnerabilities at least annually
- Implementing regular end-user education campaigns and communications
- Utilizing web and email technology to scan for malware prior to it entering our environment

Business Continuity

Our Business Continuity Program ensures resiliency for ManpowerGroup's business operations through a comprehensive Response and Recovery Framework that features:

- A formal Business Impact Analysis process that identifies critical processes and supporting IT enablers
- Risk assessments that identify and prioritize risks related to confidentiality, integrity, and availability
- A Business Continuity Plan (BCP) that is reviewed, updated and distributed regularly
- Comprehensive backup and recovery strategies that ensure operational Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Training, awareness, and testing



Contact Us

We appreciate your interest in our Information Security Policy and encourage you to become more involved with the protection of your data. If you have any questions about how ManpowerGroup protects its information as well as the information entrusted to us please contact me directly. If you would like to hear more about our program, please do not hesitate to request a meeting with us. On behalf of ManpowerGroup and the entire Security team, we look forward to working with you.

Randy L. Herold

Chief Information Security Officer

randy.herold@manpowergroup.com

Learn more about our Information Security Policy and Practices:
https://www.manpowergroup.com/sustainability/infosecprivacy

ManpowerGroup BeLux
PR/22/0/ENG – 01/08/2022

ManpowerGroup

MANPOWERGROUP

Supply Chain Business Partner Policy

ManpowerGroup BeLux
PR/15/0/ENG – 01/08/2022

ManpowerGroup®

Policy

It is ManpowerGroup policy to require that our supply chain business partners be committed to business principles, culture and values that align with our own commitments to social responsibility and sustainability, and that these business partners provide positive assurance as to their commitment to certain key practices as outlined in our Supplier Code of Conduct.

ManpowerGroup enjoys a reputation for conducting business with integrity and respect for all of those who are affected by our activities. This reputation is an asset for both ManpowerGroup and our business partners. We apply apply the standards of socially responsible and sustainable conduct globally and in each aspect of our day-to-day business. These principles include a commitment to establish mutually beneficial relationships with our suppliers. Further, our expectation is that our supplier business partners will adhere to business principles, culture and values that are consistent with our own standards of social responsibility and sustainability including the principles of the United Nations Global Compact to which we are committed.

This Policy is intended to support the Company as it strives to meet the increasing need for transparency with regard to how businesses manage their broad range of operational, social and environmental responsibilities.

What is Required

Supply chain business partners are required to provide the following as positive assurance of their commitment:

a. Confirm the intention to comply with the Supplier Code of Conduct either in the supplier's contract or through signing and returning the Supplier Affirmation Form (Attachment #2).
b. Expressly notify ManpowerGroup should any of the key principles cause specific concerns.
c. Provide ManpowerGroup with specific, internal company policies, procedures, published reports and/or other information that show further positive assurance as to adherence to the key practices, upon request.

Non-Compliance

ManpowerGroup's intention is to establish a compatibility of standards and to incorporate the above practices in the supplier approval processes of ManpowerGroup's businesses. The expectation is that, where there are differences, ManpowerGroup and the supplier will agree on an acceptable level of consistency and that the supplier will actively work toward achieving the desired level of performance. As a last resort, ManpowerGroup is prepared to terminate business with any supplier that does not demonstrate progress towards meeting ManpowerGroup's Supplier Code.

ManpowerGroup's business partners are encouraged to report any concerns directly to their primary contact or via the ManpowerGroup Business Ethics Hotline.

Entity Compliance Process

✓ Entities must confirm their adherence to this Policy on the quarterly Internal Control Checklist.

✓ Audit Advisory Services will also confirm compliance with this Policy as in-country or desk audit procedures are performed.

Supplier Code of Conduct

Obeying the Law

1. Compliance with all applicable laws and regulations of the jurisdiction where operations are undertaken.

Business Integrity

2. No offer or attempt at improper advantage, including the payment or acceptance of bribes, to secure delivery of goods or services.

Employees

3. Provision of safe and healthy working conditions for all employees.
4. Zero tolerance of human trafficking.
5. No use of any form of forced or compulsory labor and freedom of employees to leave employment after reasonable notice.
6. No use of child labor and compliance with relevant International Labor Organization standards.
7. No discrimination due to race, color, religion, national origin, cultural background, gender, age, disability, sexual orientation, or gender identity, or any other protected status in the jurisdiction where operations are undertaken.
8. Wages and working hours complying, at a minimum with applicable laws, rules and regulations regarding employment, including minimum wage, overtime and maximum hours in the jurisdiction concerned.
9. Respect for the right of employees to freedom of association and collective bargaining.
10. Ensure the privacy and protection of personal and sensitive information and data.
11. Provide training and learning opportunities.

Clients and Customers

12. Delivery of services which consistently meet specified quality, safety and data privacy and other relevant criteria.

Communities

13. Giving back to the community.

Environment

14. Management of the business in an environmentally sound manner, including compliance with all relevant legislation of the jurisdiction where operations are undertaken.

ATTACHMENT 1 – MANPOWERGROUP'S REQUEST FOR BUSINESS PARTNERS TO ACKNOWLEDGE COMPLIANCE WITH OUR SUPPLIER CODE OF CONDUCT

ManpowerGroup OR < Local Country Letterhead Paper >

< date >

Dear Sir or Madame:

RE: Corporate Social Responsibility and ManpowerGroup's Supply Chain Business Partners

ManpowerGroup enjoys a reputation for conducting business with integrity and respect for those our activities will affect. This reputation is an asset for both ManpowerGroup and our business partners. Attached, for your information, is the website link to ManpowerGroup's Code of Business Conduct and Ethics. ManpowerGroup applies these standards of conduct globally and in each aspect of our day-to-day business. These principles include a commitment to establish mutually beneficial relationships with our suppliers. Further, our expectation is that our supplier business partners will adhere to business principles, culture and values that are consistent with an attitude of social responsibility.

There is an increasing need for transparency with regard to how businesses manage their broad range of operational, social and environmental responsibilities. We require our supply chain business partners to provide positive assurance that they intend to operate in accordance with the key business practices outlined in ManpowerGroup's Supplier Code of Conduct.

As a first step, we ask you to provide a response on the attached form:

a. Acknowledge receipt of this letter and confirm your intention, in principle, of complying with the key practices outlined in ManpowerGroup's Supplier Code of Conduct.
b. Provide feedback to ManpowerGroup should any of the key practices cause specific concerns. Our expectation is that, where there are differences, we will agree on an acceptable level of consistency and that you will actively work toward achieving the desired level of performance.
c. Provide ManpowerGroup with specific, internal company policies, procedures, published reports and/or other information that show further positive assurance.

We hope you share the sense of importance we attach to the key business practices in the Supplier Code. We believe these policies are central to the sustainability of our business and imperative to the industry in which we jointly participate.

If you have any questions, please contact the ManpowerGroup representative noted below.

Thank you.

Yours sincerely,

On behalf of ManpowerGroup (your local company name)
XXX (Local Country Lead Name here)

ATTACHMENT 2 – SUPPLIER AFFIRMATION FORM

RE: Affirmation of Adherence to ManpowerGroup's Supplier Code of Conduct

On behalf of my Company, its subsidiaries and sister companies, I acknowledge receipt of ManpowerGroup's Supplier Code of Conduct. We affirm that we operate in accordance with the key practices concerning; Obeying the Law, Employees, Clients & Candidates, Communities, the Environment and Business Integrity. We will notify ManpowerGroup immediately should any of the practices in the Supplier Code cause concern, and agree to work toward achieving a mutually agreed upon level of performance. We understand that non-compliance or lack of progress toward compliance may be cause for ManpowerGroup to terminate the business relationship.

Organization Name:	
Geographic Locations Covered: (global, regions, or countries)	
Comments (if applicable):	
Name of Person Signing:	
Title:	
Date:	
Signature:	

Please return the original signed and dated form to ManpowerGroup's address below, along with any specifically requested information about your internal company policies and/or published reports that provide further positive assurance for your company's practices. Additionally, all responses justifying a company decision not to follow or incorporate the key practices defined in the Supplier Code should also be sent to the contact below.

XXX (Local Country Lead/Contact Name here)
XXX (Local Country Lead/Contact Title here)

ManpowerGroup
XXX (Local Country Corporate Headquarters address here)
XXX (Local Country Contact Details)

ManpowerGroup

POLITIQUES ESG & DÉVELOPPEMENT DURABLE

Plus d'informations sur la stratégie de développement durable de ManpowerGroup

> Au niveau mondial : manpowergroup.com

> Au niveau belge : manpowergroup.be

ManpowerGroup BeLux
PR/10/3/FR – 01/10/2025
For external use.

ManpowerGroup | Manpower | Experis ManpowerGroup | Talent Solutions ManpowerGroup | Jefferson Wells ManpowerGroup