MANPOWERGROUP

Beleid inzake giften, entertainment en sponsoring

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

ManpowerGroup®

Inhoudsopgave

I. Introductie

Dit beleid is bedoeld om u te helpen bij het bepalen of u giften, maaltijden en entertainment, gastvrijheid, sponsoring en reisvoordelen aan externe partijen aanbiedt, vooral wanneer er regeringsambtenaren bij betrokken zijn. Het geeft ook aan welke processen moeten worden gevolgd. Het moet worden gelezen en begrepen in samenhang met het beleid inzake anticorruptie van de ManpowerGroup. Dit beleid geldt voor alle werknemers, leidinggevenden, leden van de raad van bestuur en anderen die in naam van ManpowerGroup handelen.

Onder regeringsambtenaren vallen bijvoorbeeld:

- ✓ Staatshoofden, ministers, en andere benoemde politici;
- ✓ Ambtenaren;
- ✓ Andere fulltime of parttime werknemers van de overheid;
- ✓ Particuliere burgers die in een officiële hoedanigheid handelen;
- ✓ Veiligheidspersoneel (militairen, politie, inlichtingendiensten);
- ✓ Rechters en wetgevers;
- ✓ Ambtenaren en werknemers van staatsbedrijven of gecontroleerde ondernemingen (bijvoorbeeld een aardoliemaatschappij of een luchtvaartmaatschappij die in handen is van de staat); en
- ✓ Werknemers van andere openbare instellingen, inclusief universiteiten, laboratoria, ziekenhuizen, en dergelijke.

Het beleid inzake anticorruptie van ManpowerGroup verbiedt ten strengste elke vorm van omkoperij en corruptie in verband met de zaken van het bedrijf. Het aanbieden van giften, entertainment en overnachtingsmogelijkheden en het sponsoren van reizen of andere activiteiten kan een toegestaan onderdeel zijn van het zakendoen. Deze activiteiten kunnen in sommige omstandigheden echter ook als een corrupt voordeel worden beschouwd en kunnen leiden tot strafrechtelijke aansprakelijkheid voor de betrokkenen. Bovendien kunnen ze zijn gereglementeerd door de regering van de plaats of het land waar de voordelen worden aangeboden, of beperkt zijn door de organisatie van de ontvanger. Dit is met name waar wanneer de voordelen worden ontvangen door personen die volgens de desbetreffende wetten als regeringsambtenaren worden gezien. 'Regeringsambtenaren' is een ruim begrip dat ook ambtenaren kan omvatten van bedrijven die eigendom zijn van of gecontroleerd worden door de regering. In alle gevallen moet ManpowerGroup zorg dragen voor een goede interne controle en toereikende boeken en records met betrekking tot deze voordelen.

De regels en uitgavenlimieten in dit beleid bepalen uw handelingen met externe partijen, zoals klanten, verkopers en regeringsambtenaren. Interne uitgaven voor giften, maaltijden enentertainment, zoals voor uw collega's en teams, vallen niet onder dit algemene beleid. Er wordt van u echter verwacht dat u voor dergelijke activiteiten steeds uw gezond verstand gebruikt, en de plaatselijke goedkeuringsprocedure in acht neemt.

Elke werknemer die zich ervan bewust wordt, of vermoedt, dat dit beleid is geschonden, moet onmiddellijk:

Hun manager of leidinggevende op de hoogte stellen;

- ✓ De juridisch adviseur of de Global Ethics Compliance Officer op de hoogte brengen; of
- ✓ Melding maken van zorgen via de wereldwijde hotline voor ethische vragen bij ManpowerGroup

II. Algemene regels die van toepassing zijn op alle soorten voordelen

Giften, maaltijden, entertainment, overnachtingen en het aanbieden van sponsoring of andere voordelen, inclusief het sponsoren van reizen, worden in dit beleid 'Voordelen' genoemd.

De volgende regels zijn van toepassing:

1. Voordelen zijn **nooit** toegestaan wanneer ze aan regeringsambtenaren, zakenpartners, klanten of toekomstige klanten worden aangeboden om hun handelingen of beslissingen in hun officiële of zakelijke hoedanigheid te beïnvloeden.

2. Van de werknemers wordt verwacht dat ze hun gezond verstand gebruiken bij de beslissing om voordelen aan te bieden of te verstrekken, en ze moeten bereid zijn het legitieme zakelijke doel van de voordelen aan te geven. In de volgende specifieke secties vindt u enkele voorbeelden van legitieme activiteiten.

3. Alle voorschriften van de plaatselijke wetgeving en regels van de organisatie van de ontvanger moeten in acht worden genomen. Veel bedrijven beperken de geschenken of het entertainment die hun werknemers mogen accepteren, en contracten met klanten kunnen extra beperkingen opleggen. Voordat u voordelen aan een externe partij verstrekt, is het uw verantwoordelijkheid om alle vereiste goedkeuringen van ManpowerGroup te verkrijgen, en ook om te bevestigen dat de plaatselijke wetgeving, evenals het beleid van uw ontvanger, wordt nageleefd.

4. Dit beleid omvat algemene, geldelijke grenzen. **Uw land heeft misschien lagere bestedingslimieten vastgesteld om de plaatselijke gewoontes te weerspiegelen.** Het is uw verantwoordelijkheid om zowel de algemene als de landspecifieke vereisten te begrijpen en na te leven.

5. De voordelen moeten **altijd** een redelijk bedrag en van passende aard zijn.

6. Bepaalde soorten voordelen mogen nooit worden aangeboden. Dit omvat voordelen in cash, voordelen in verband met illegale activiteiten of activiteiten die de reputatie van het bedrijf kunnen schaden, zoals escortservices, amusementscentra voor volwassenen of gokken.

7. Er moet rekening gehouden worden met de reputatie. Voordelen die de meeste mensen als overdadig of extravagant zouden beschouwen, of die een persoonlijk karakter hebben (bijvoorbeeld juwelen of luxegoederen), kaartjes voor grote evenementen of uitstapjes naar vrijetijdsbestemmingen, mogen over het algemeen niet worden aangeboden.

8. Voordelen, zoals giften, die worden gegeven wanneer er met de ontvanger zakelijke of contractuele beslissingen worden behandeld die ManpowerGroup een voordeel zouden kunnen opleveren, kunnen ook problemen op het gebied van reputatie veroorzaken, en mogen in het algemeen niet worden gegeven.

9. De regelmaat van het aanbieden van voordelen aan bepaalde ontvangers moet worden gecontroleerd. Zelfs relatief bescheiden voordelen, zoals maaltijden, kunnen, wanneer ze regelmatig worden aangeboden, juridische problemen of problemen met de reputatie veroorzaken, en moeten worden vermeden.

10. De totale waarde van de voordelen aan bepaalde ontvangers moet ook in aanmerking worden genomen. Indien de totale waarde van de giften, maaltijden en entertainment die aan een bepaalde persoon in de loop van een jaar zijn aangeboden meer dan **USD 250** bedraagt, moet men voorzichtig zijn met het verstrekken van verdere voordelen aan deze persoon.

11. Het gebruik van persoonlijk geld om voordelen aan te bieden, is verboden.

12. Uitgaven in verband met voordelen moeten nauwkeurig en volledig zijn en naar behoren gedocumenteerd.
    Passende documentatie omvat betalingsbewijzen voor uitgaven, informatie over eventuele aanwezigen en begunstigden (inclusief naam en plaats van tewerkstelling), en een verklaring van het zakelijke doel.

13. Alle uitgaven voor voordelen moeten worden goedgekeurd zoals bepaald in sectie VII hieronder.

14. Bedrijven die menen dat de omstandigheden van hun bedrijf andere drempels of benaderingen vereisen dan wat in dit beleid wordt uiteengezet, moeten hun behoeften bespreken met de Global Ethics Compliance Officer.

III. Giften

Alle giften moeten passen bij de gelegenheid, een redelijk bedrag zijn en alleen als beleefdheid of blijk van hoogachting worden gegeven. Giften mogen niet worden gegeven om de keuze te beïnvloeden van een bedrijf wat betreft het aanbod van hun diensten of om een actie van een regeringsambtenaar of zakenpartner te beïnvloeden of teweeg te brengen. **ManpowerGroup heeft een algemeen limiet voor giften van USD 150**. U kunt deze algemene limiet niet overschrijden zonder voorafgaande schriftelijke toestemming. Om goedkeuring te krijgen, bekijkt u het diagram voor goedkeuringen in sectie VII. Naast de algemene limieten zijn er landspecifieke bestedingslimieten voor giften vastgesteld door elke landenmanager. Controleer uw landspecifieke limiet voordat u een gift aanbiedt.

Naast de richtlijnen in sectie II gelden de volgende richtlijnen voor **giften** die worden gegeven aan regeringsambtenaren, zakenpartners, klanten of potentiële klanten:

- ✓ Giften moeten openlijk en transparant worden aangeboden en in overeenstemming met de gelegenheid. Als u zich daar niet prettig bij voelt, is dat een teken van een mogelijk probleem.
- ✓ De plaatselijke gebruiken en praktijken kunnen in sommige plaatsen anders zijn en daar moet rekening mee worden gehouden.
- ✓ Geld en equivalenten daarvan, zoals cadeaubonnen, reischeques, opwaardeerkaarten voor mobiele telefoons, en cheques, zijn nooit toelaatbare geschenken.
- ✓ Giften aan kantoren of groepen die zijn bedoeld om met collega's te delen (bijvoorbeeld voedselmanden), hebben de voorkeur boven geschenken aan individuen.
- ✓ Bijzondere voorzichtigheid is geboden met giften aan ambtenaren die zich bezighouden met aanbestedingen of anderen die de bevoegdheid hebben om contracten aan de onderneming te gunnen. Giften die worden aangeboden wanneer de besluitvorming over het plaatsen van opdrachten gaande zijn, kunnen de schijn wekken van een ongepaste bedoeling om invloed uit te oefenen en moeten worden vermeden.
- ✓ Giften van items voor persoonlijk gebruik of voor familieleden of vrienden van regeringsambtenaren of zakenpartners zijn minder gepast dan promotieartikelen van het bedrijf, maar kunnen soms wel gepast zijn (bijvoorbeeld bloemen of een 'gift voor de gastvrouw/gastheer' wanneer u bij iemand thuis komt eten)

Zolang de gift redelijk is, zijn voorbeelden van passende giften onder meer:

- ✓ Giften om feestdagen te vieren die gewoonlijk met het geven van giften worden geassocieerd, zoals Kerstmis, Chinees Nieuwjaar en andere soortgelijke gebeurtenissen.
- ✓ Giften om specifieke gebeurtenissen te herdenken, zoals een bedrijfsjubileum, de afsluiting van een zakelijke transactie, pensionering, etc.
- ✓ Giften van promotieartikelen waarop het logo van het bedrijf staat gegraveerd, zoals glaswerk, kantoorartikelen, pennen, koffiemokken, shirts, hoeden, enz. zijn over het algemeen geschikte giften.

IV. Maaltijden en entertainment

Maaltijden en entertainment, zoals in deze sectie gebruikt, omvatten zowel traditionele restaurantmaaltijden, als culturele en sportevenementen, zowel persoonlijk als virtueel, waarbij we toegangsbewijzen en bijbehorend eten en dranken kunnen kopen. Let op: maaltijden of vermaak die deel uitmaken van gesponsorde reizen, vallen hieronder in sectie V, Reizen. **ManpowerGroup heeft een algemeen limiet voor maaltijden en entertainment van USD 200**. U kunt deze algemene limiet niet overschrijden zonder voorafgaande toestemming. Om goedkeuring te krijgen, bekijkt u het diagram voor goedkeuringen in sectie VII. Naast de algemene limieten zijn er landspecifieke bestedingslimieten voor maaltijden en entertainment vastgesteld door elke landenmanager. Controleer uw landspecifieke limieten voordat u maaltijden en entertainment aanbiedt.

Voorbeelden van legitieme vormen maaltijden en entertainment zijn:

- ✓ Lunch ter gelegenheid van een zakenbijeenkomst met een klant.
- ✓ Diner ter gelegenheid van de start van een nieuwe zakenrelatie.
- ✓ Een zakenpartner of klant uitnodigen om met een werknemer naar een voetbalwedstrijd te gaan. Let op: de totale uitgaven voor het evenement, met inbegrip van de kaartjes en eventueel aangeboden eten en/of drank, mogen de algemene limiet niet overschrijden.
- ✓ U hebt een tweedaagse vergadering met een klant of een potentiële klant. Op de tweede dag organiseert u een afsluitende cruise met een diner.

Naast de algemene richtlijnen in sectie II hierboven gelden de volgende richtlijnen voor **maaltijden en entertainment** die worden gegeven aan regeringsambtenaren, zakenpartners, klanten of potentiële klanten:

- ✓ Zakenmaaltijden moeten niet vaak voorkomen, in overeenstemming zijn met de normen van het land en de plaatselijke praktijken, en moeten nooit extravagant zijn.
- ✓ De werknemers van ManpowerGroup moeten plaatsen voor maaltijden en entertainment kiezen die binnen dit beleid vallen. Als u het aan de persoon van de andere partij overlaat om de plaats te kiezen, kunt u een situatie creëren waarin u niet aan dit beleid kunt voldoen. Plan van tevoren en vermijd moeilijke en gênante situaties!
- ✓ Familieleden of vrienden van een regeringssambtenaar, zakenpartner, klant of toekomstige klant mogen geen maaltijd, sportevenement of amusementsactiviteit bijwonen op kosten van het bedrijf, tenzij de echtgenoten of vrienden van de werknemers van ManpowerGroup ook aanwezig zijn, of als er vooraf toestemming is verkregen van de Global Ethics Compliance Officer.
- ✓ Entertainment kan deel uitmaken van een legitieme zakelijke bijeenkomst, mits het hoofddoel van de bijeenkomst het doen van zaken, of de bedrijfsontwikkeling is. Losstaande uitstapjes zonder verwant zakelijk doel, zoals een golfweekend, zijn over het algemeen geen gepast zakelijk entertainment en vereisen specifieke voorafgaande toestemming van de Global Ethics Compliance Officer.
- ✓ Een werknemer of vertegenwoordiger van het bedrijf moet sportevenementen of amusementsactiviteiten bijwonen met de regeringsambtenaar, zakenpartner, klant of toekomstige klant. Kaartjes voor een sportevenement zodat de persoon het evenement alleen of met gasten van zijn keuze kan bijwonen, zijn bijvoorbeeld over het algemeen niet gepast.
- ✓ Waar mogelijk moeten de betalingen voor maaltijden en entertainment door werknemers van ManpowerGroup rechtstreeks aan de dienstverleners worden gedaan.
- ✓ In de meer ongebruikelijke gevallen waarin een vergoeding voor maaltijden of entertainment aan een regeringsambtenaar of zakenpartner op zijn plaats is, moet de vergoeding worden onderbouwd met passende ontvangstbewijzen waaruit de aard en het bedrag van de te vergoeden uitgave blijkt.

V. Sponsoring van reizen

Over het algemeen wordt van regeringsambtenaren, zakenpartners, klanten of potentiële klanten verwacht dat ze de kosten van hun eigen reizen betalen. Er kunnen zich echter bepaalde omstandigheden voordoen waarin het bedrijf de reiskosten betaalt van een regeringsambtenaar, zakenpartner, klant of toekomstige klant voor een bezoek aan een bedrijfslocatie van het bedrijf, voor een gezamenlijke vergadering of voor een ander passend zakelijk doel. De kosten van het sponsoren van een reis kunnen betrekking hebben op vervoer, overnachtingen en maaltijden, en op andere bijkomende kosten. Sponsoring van reizen door het bedrijf kan aanzienlijke geldbedragen met zich meebrengen en moet worden goedgekeurd. Om goedkeuring te krijgen, bekijkt u het diagram voor goedkeuringen in sectie VII.

Voorbeelden waarbij het bedrijf de reiskosten kan betalen, zijn:

- ✓ Een bestuursvergadering van een joint venture waarvan de partner van het bedrijf een staatsbedrijf is.
- ✓ Voor een contract met een klant moet u de reiskosten van het personeel voor trainingsdoeleinden betalen.
- ✓ Een potentiële klant wil zien hoe de diensten op een bepaalde plaats worden verleend.
- ✓ Een bezoek aan het hoofdkantoor van het bedrijf om de mogelijkheden van ManpowerGroup te begrijpen.

Naast de algemene vereisten in sectie II hierboven gelden de volgende richtlijnen voor **het sponsoren van reizen** die wordt aangeboden aan regeringsambtenaren, zakenpartners, klanten of potentiële klanten:

- ✓ Alle gesponsorde reizen moeten een legitiem zakelijk doel hebben. De sponsoring van reizen die alleen voor ontspanning of entertainment zijn, worden niet goedgekeurd.
- ✓ Betalingen in de vorm van een dagvergoeding voor personen van wie de reis wordt gesponsord, bijv. contante betalingen of 'zakgeld', worden in het algemeen niet goedgekeurd.
- ✓ Indien mogelijk, moet de betaling van sponsoringkosten voor reizen direct aan de dienstverlener worden gedaan, bijv. luchtvaartmaatschappij, hotel, restaurant.
- ✓ Indien de vergoeding van gesponsorde reiskosten op zijn plaats is, moet de vergoeding worden onderbouwd met passende betalingsbewijzen waaruit de aard en het bedrag van de uitgaven blijken
- ✓ Over het algemeen moet het bedrijf, de instelling of de organisatie van de gesponsorde personen, en niet ManpowerGroup, de specifieke personen kiezen waarvan de reis wordt gesponsord.
- ✓ Gesponsorde personen moeten kunnen aantonen dat ze alle interne goedkeuringen hebben gekregen om te kunnen reizen.
- ✓ Familieleden of vrienden mogen de regeringsambtenaar, zakenpartner, klant of toekomstige klant niet vergezellen op de reis op kosten van het bedrijf, tenzij de familie en/of vrienden in aanmerking komen om op eigen kosten een dergelijke ontvangst te krijgen.

VI. Sponsoring van evenementen

Sponsoring van evenementen kan verschillende vormen aannemen, bijvoorbeeld het sponsoren van een tentoonstelling, activiteit, programma of iets dergelijks door het bedrijf. Sponsoring van evenementen geeft het bedrijf normaal gesproken de mogelijkheid zijn diensten te promoten of zichtbaarheid en goodwill te verwerven. Evenementen die nauw zijn verbonden met regeringsambtenaren, zakenpartners, klanten of toekomstige klanten (bijvoorbeeld, de sponsoring is aangevraagd door een regeringsambtenaar, of het is bekend dat de te sponsoren organisatie banden heeft met een regeringsambtenaar of een naast familielid van de ambtenaar), leveren speciale problemen op, evenals sponsoring in het kader van een lopend contract. Om in een dergelijke situatie goedkeuring te krijgen, bekijkt u het diagram voor goedkeuringen in sectie VII.

Naast de algemene vereisten in Sectie II hierboven, zijn de volgende richtlijnen van toepassing op **evenementsponsoring** ten gunste van regeringsambtenaren of zakenpartners:

- ✓ Sponsoring van evenementen moet als hoofddoel hebben de diensten van het bedrijf te promoten, goed gedrag van het bedrijf, of een andere legitieme zakelijke rechtvaardiging.
- ✓ De bedrijfseenheid die het evenement wil sponsoren, moet het nodige onderzoek doen naar de organisatoren van evenementen en de personen die het bedrijf willen sponsoren, en de resultaten moeten worden gedocumenteerd en bewaard. Indien mogelijk moet de betaling rechtstreeks aan de organisator van het evenement worden overgemaakt. Sponsoring mag niet in cash worden betaald.
- ✓ Werknemers van het bedrijf moeten stappen ondernemen om te verifiëren dat het sponsorgeld wordt gebruikt voor het beoogde doel, en dat het bedrijf de overeengekomen voordelen ontvangt in ruil voor de sponsoring.
- ✓ Alle reizen in verband met de sponsoring van evenementen moeten voldoen aan de vereisten van de sectie Reizen van dit beleid, dat wordt uiteengezet in sectie V.
- ✓ Giften die worden aangeboden in verband met de sponsoring van evenementen moeten voldoen aan de vereisten van de sectie Giften van dit beleid, dat wordt uiteengezet in sectie III.

VII. Autorisaties en goedkeuringen

De onderstaande tabel geeft een overzicht van de goedkeuringsvereisten op grond van deze algemene beleidslijn. Vergeet niet u te houden aan eventuele plaatselijke beperkingen of goedkeuringsvoorschriften.

Goedkeuringen van giften, entertainment en sponsoring

Soort aangeboden voordeel	Goedkeuring is vereist voor:
Giften	Geschenken van meer dan **USD 150** per ontvanger.
Maaltijden en entertainment	Maaltijden en entertainment van meer dan **USD 200** per ontvanger.
Losstaande uitstapjes zonder gerelateerd zakelijk doel	Alle uitstapjes.
Sponsoring van reizen	Alle sponsoring van reizen.
Sponsoring van evenementen die nauw verbonden zijn met regeringsambtenaren, zakenpartners, klanten of toekomstige zakenpartners of klanten	Alle evenementen.

Goedkeuringsproces

Alle verzoeken om goedkeuring moeten worden gemaild naar:

giftsandentertainment.authorization@manpowergroup.com.

Vermeld details betreffende de voorgestelde uitgaven, inclusief de naam, de titel en de band van de voorgestelde deelnemers, het budget en de dienstverleners. U moet ook het zakelijke doel vermelden.

De Global Ethics Compliance Officer neemt uw verzoek in overweging. Alle goedkeuringen worden schriftelijk gegeven. Als een goedgekeurde uitgave wezenlijk verandert ten opzichte van het ingediende voorstel (bijv. als de werkelijke begroting aanzienlijk hoger uitvalt dan de voorgestelde begroting, of als de aanwezigen veranderen) is een nieuwe goedkeuring vereist.

Records bijhouden

U moet gegevens over de uitgaven bewaren. In alle ingediende onkostendeclaraties moeten de namen, titels en banden van de aanwezigen en het zakelijke doel van de uitgaven schriftelijk worden vermeld.

VIII. Administratie en onderzoeken

De juridisch adviseur **Richard Buchband** houdt toezicht op de naleving van dit beleid en het anticorruptieprogramma van het bedrijf. Onder zijn leiding behandelen **Shannon Kobylarczyk**, Global Ethics Compliance Officer, ede vragen en goedkeuringen.

Als u vragen hebt, neem dan contact op met Shannon op via **414.906.7024**, of stuur een bericht aan ons team via ethics.training@manpowergroup.com of generalcounsel@manpowergroup.com.

ManpowerGroup

ESG/DUURZAAMHEID

MILIEU

MILIEUBELEID

“Nu is het tijd om te handelen voor het klimaat.”

#TheChangeStartsWithYouAndMe

ONZE VERBINTENIS

ManpowerGroup zet zich in voor de strijd tegen de opwarming van de aarde. In 2021 hebben we onze klimaatdoelstellingen laten valideren door de organisatie Science Based Targets (SBTi), de toonaangevende autoriteit op het gebied van klimaat autoriteit op het gebied van klimaatactie in de bedrijfswereld.

Onze ambitie is om het doel van nul netto emissies uiterlijk tegen 2045 te bereiken.

Hier zijn onze doelstellingen tegen 2030:

- **de uitstoot van zijn operationele activiteiten met 60% verminderen** (Doelstelling 1 & 2 – energie- en elektriciteitsverbruik in gebouwen, bedrijfswagens, enz.);
- **de uitstoot in de toeleveringsketen met 30% verminderen** (Doelstelling 3 – afvalbeheer, reizen, mobiliteit, leveranciers).

Ons actieplan richt zich op de domeinen met de grootste impact op het klimaat en we meten en we meten jaarlijks onze vooruitgang aan de hand van gegevens die zijn verzameld met behulp van een strenge methodologie.

ManpowerGroup Belgium deelt dezelfde ambitie.
Om onze globale strategie te realiseren, hebben we de volgende doelstellingen vastgelegd:

ENERGIE

- 100% hernieuwbare energie voor onze kantoren tegen 2030.
- Geleidelijke overgang van ons kantoornetwerk naar koolstofarme gebouwen.
- Ons energieverbruik verminderen.

MOBILITEIT

- Nul CO_2-uitstoot van onze bedrijfswagens tegen 2030.
- Implementatie van acties om de impact van de woon-werkverkeer op het milieu te verminderen onze reizen (mobiliteitsplan, flexibele werktijden, hybride e werkmethoden, beperken van zakenreizen).

NUL PAPIER/NUL AFVAL/ RECYCLING

- 95% van onze externe documenten in elektronische vorm tegen 2025 en vermindering van het printen van onze interne documenten op weg naar «nul papier».
- 100% sorteren en recyclen: procedures in kracht om optimale vermindering en sortering van intern afval, alsmede recycling van materialen (kantoormeubilair, IT-apparatuur, elektrische apparatuur, printercartridges, enz.)

DUURZAME AANKOOP

- Gebruik van duurzame producten in de dagelijkse werking van het bedrijf (kantoorbenodigdheden, tassen, promotiemateriaal, bekers, enz.)

Wij sensibiliseren ons personeel en alle stakeholders met betrekking tot de klimaatuitdagingen.

Alle medewerkers van ManpowerGroup zijn betrokken bij het bereiken van onze klimaatdoelstellingen door dagelijks gedrag aan te nemen milieuverantwoord gedrag aan te nemen gedrag op dagelijkse basis.

'The Change Starts With You And Me'

ManpowerGroup BeLux

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

ManpowerGroup

ESG/DUURZAAMHEID

SOCIALE DIALOOG

BELEID SOCIALE DIALOOG

"We zijn ervan overtuigd dat een gezond economisch klimaat niet mogelijk is zonder een gezond sociaal klimaat."

Daarom streven we naar relaties met de sociale partners die steunen op vertrouwen en respecteren we de wettelijke rol en opdracht van de vakbondsorganisaties.

In nauwe samenwerking met de verantwoordelijken van de sociale relaties en de juridische afdeling, verzorgt de Directie Human Resources van ManpowerGroup BeLux het beheer en de uitvoering van de zakelijke, syndicale en institutionele relaties van ManpowerGroup.

Zo steunen en sturen ze:

- het beheer van de sociale kalender en de vergaderingen met de werknemersorganen;
- de onderhandelingen met de representatieve vakbondsorganisaties;
- het individueel en collectief beheer van de personeelsvertegenwoordigers;
- de sociale verkiezingen.

ManpowerGroup BeLux

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

MANPOWERGROUP'S INFORMATION SECURITY POLICY

TODAY'S CONTEXT: RAPID DIGITAL TRANSFORMATION

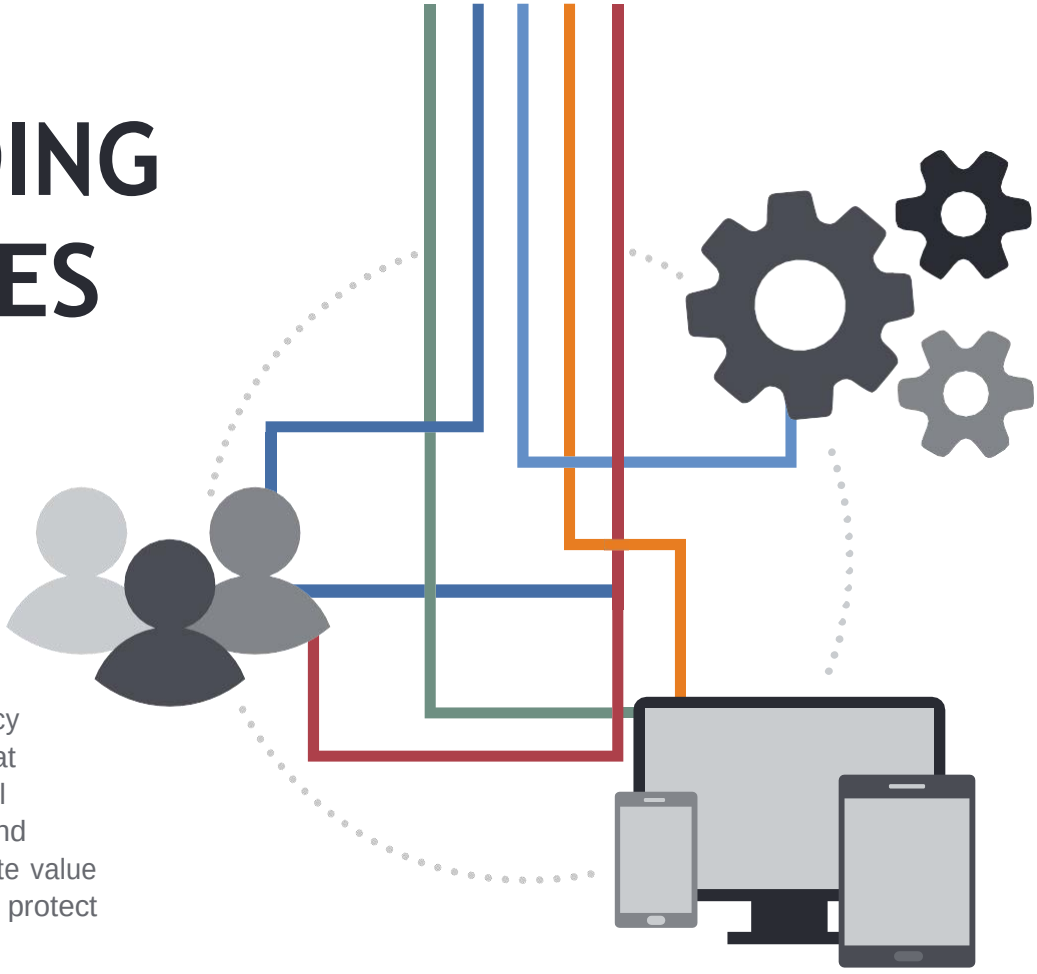
The severity, frequency and impact of cyber-crime has been on the rise for a number of years. Now, with the acceleration of remote working and rapid digitization organizations will require even greater prioritization of information security capabilities. Business and security leaders are being challenged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

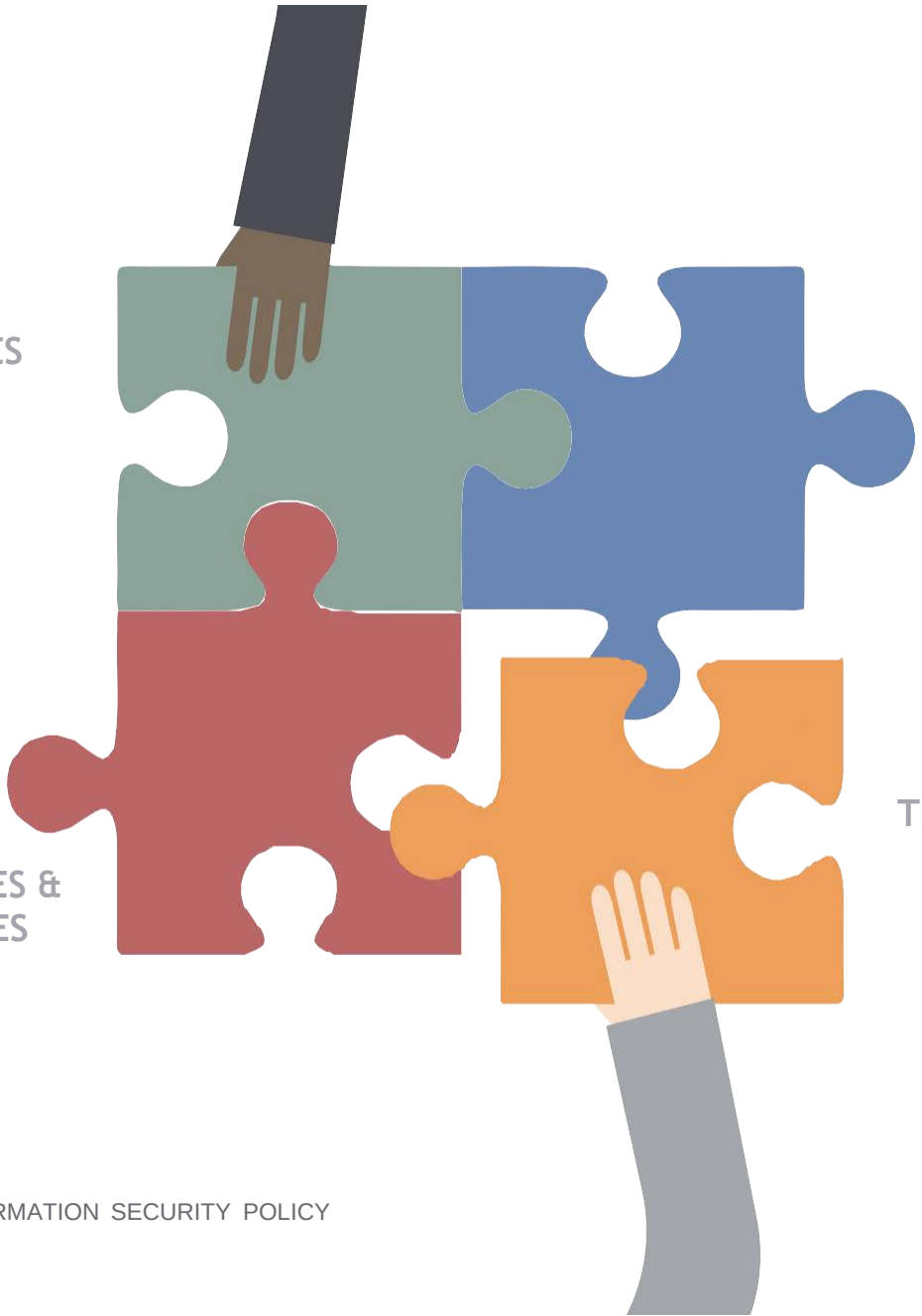
TECHNOLOGY

- 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.

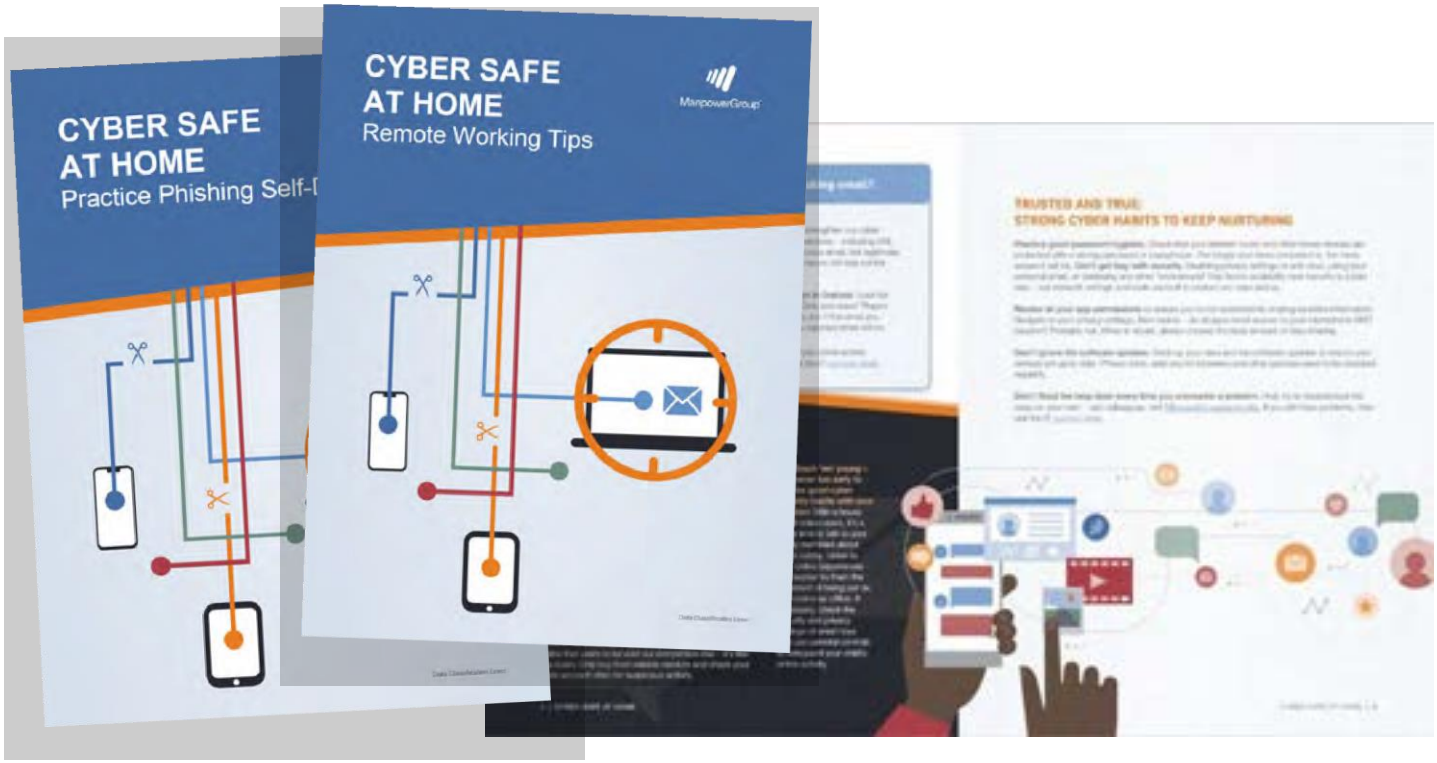
Our talented team dedicated to information security and data privacy has increased in size significantly over recent years. Our people are strategically positioned at the global, regional and local market levels to provide consistent policies, processes and technology solutions. Our highly trained staff 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.

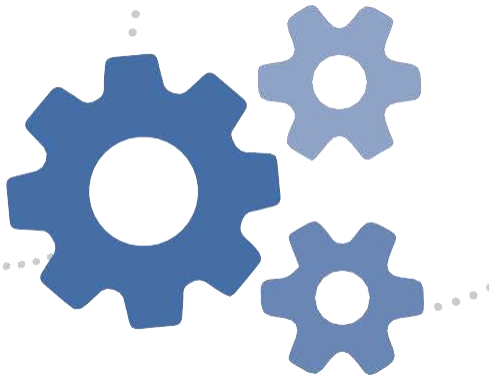


Embedding Security into our People & Culture Practices

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

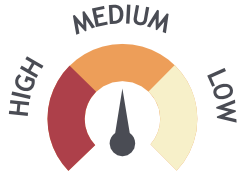
Analyzing Risks

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

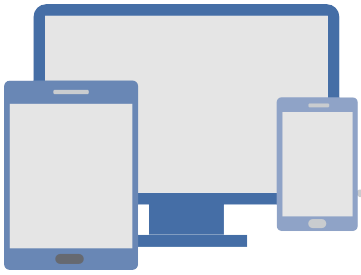
To safeguard our information assets, access is limited to authorized, business-justified entities with a “need to know.” We have taken thorough measures to prevent the inappropriate use of access credentials:

- 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

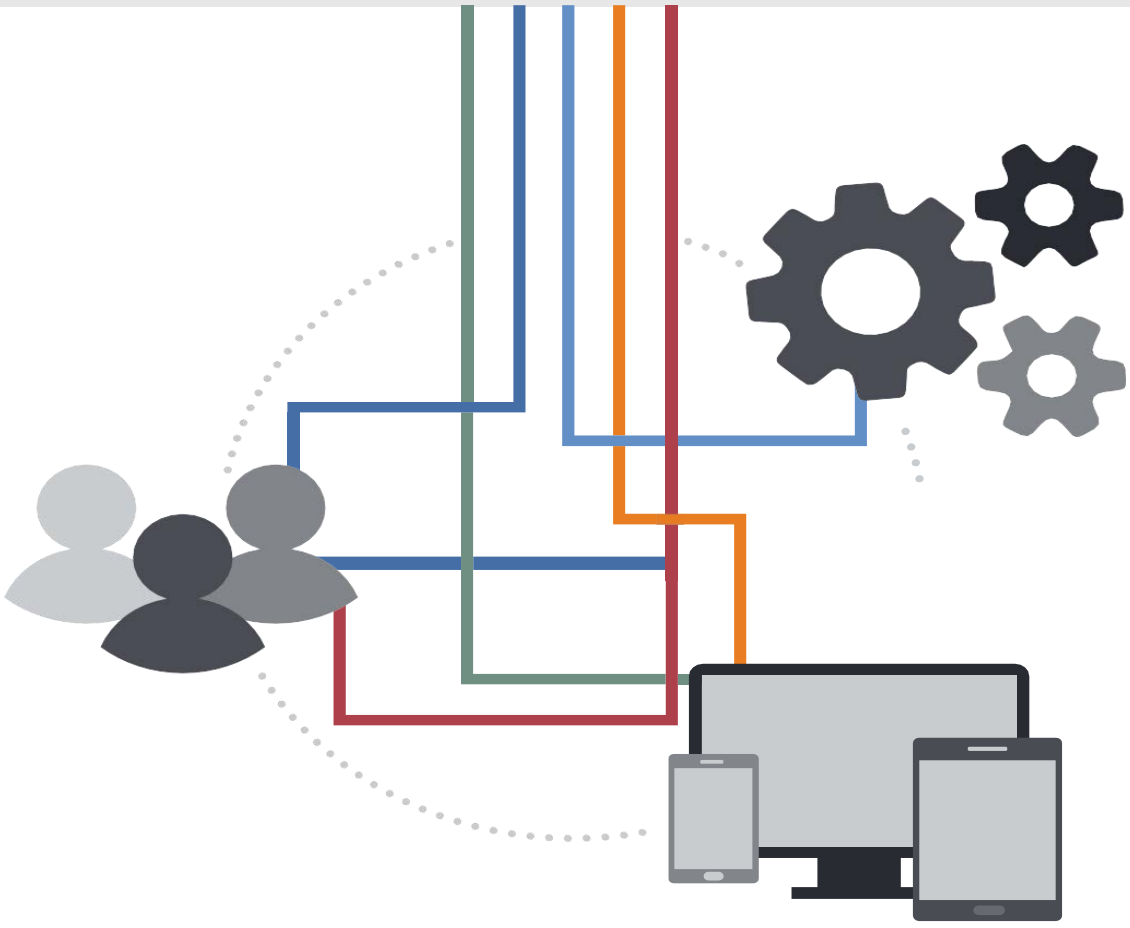
We protect from malicious code execution (Malware) through activities including:

- 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

BELEIDEN INZAKE ESG & DUURZAAMHEID

Meer informatie over de duurzaamheidsstrategie van ManpowerGroup:

> Wereldwijd: manpowergroup.com

> Op Belgisch niveau: manpowergroup.be

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

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